RECENT DEVELOPMENTS IN PRIVACY PROTECTIONS FOR CONSUMERS

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

OCTOBER 11, 2000

Serial No. 106–160

Printed for the use of the Committee on Commerce

U.S. GOVERNMENT PRINTING OFFICE
67–635CC WASHINGTON : 2000

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
TOM SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California

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
TOM SAWYER, Ohio
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

RECENT DEVELOPMENTS IN PRIVACY PROTECTIONS FOR CONSUMERS

WEDNESDAY, OCTOBER 11, 2000

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

The subcommittee met, pursuant to notice, at 10:15 a.m., in room 2123, Rayburn House Office Building, Hon. W.J. "Billy" Tauzin (chairman) presiding.

Members present: Representatives Tauzin, Gillmor, Cox, Shimkus, Ehrlich, Markey, Boucher, Wynn, Luther, Sawyer, Green, and McCarthy.

Staff present: Paul Scolese, majority professional staff; Anthony Habib, legislative clerk; and Andy Levin, minority counsel.

Mr. TAUZIN. The subcommittee will please come to order.

Today the subcommittee will hold the hearing on the important developments in the efforts to the protect privacy of American consumers. Few issues in this industry generate such strong emotions as how to deal with the enormous amounts of personal information that are collected, distributed, stored every day via the Internet.

Later this morning, we will hear from two of our colleagues, Representative Clay Shaw and Representative Bob Goodlatte. Representative Shaw will explain to this subcommittee his legislation H.R. 4857, the Privacy and Identity Protection Act of 2000, which has been reported out of the Ways and Means Subcommittee on Social Security and is currently awaiting action in this subcommittee.

In addition the subcommittee will hear from Representative Goodlatte about the Lansdowne Privacy Summit which the National Chamber Foundation hosted for House Republicans in May of this year and what has come from that. I understand that the foundation also scheduled a similar session with the House Democrats, and unfortunately it got canceled, I believe.

Representative Goodlatte cohosted, along with my colleagues, Chairman Bliley, Representative Ehrlich and myself, this privacy summit; and I personally want to thank him for his efforts in this endeavor. I also want to thank both of our colleagues for coming this morning, for sharing their views with us. The subcommittee has been a keen observer for many years of this debate, holding hearings on this issue both in 1998, 1999 and again in 2000.

Over the last year, we have seen consumer concerns over privacy heightened and, as a result, specific Federal responses. Congress has adopted two Federal laws to deal with specific areas of concern,

the Gramm-Leach-Bliley law in which financial privacy laws are written, and the Children's Online Privacy Protection Act. In addition, Americans have witnessed the development of a new private-sector technology and, in fact, many technologies to help consumers, as well as voluntary standards by industry to self-police, and educate consumers.

In certain areas, the Federal Government and commercial entities have come together to achieve cooperative standards to govern their online conduct. Privacy was not created with the advent of the Internet. In fact, we have been passing privacy laws, I believe, for the past 30 years, but the Internet adds a level of dissemination beyond what Americans had ever thought possible in many circumstances beyond which they feel comfortable.

While the Internet is still relatively new, the issue of privacy, of course, is not. Prior to the adoption of the GLB and the COPPA laws, Congress had enacted privacy protections in a dozen other circumstances, indeed over that past 30 years, with the Fair Credit Reporting Act in 1970 starting that process. Sharing personal information did not begin when the Internet was established. Many people remember party-line telephones and can recall door-to-door salesmen plying their wares, using neighborhood directories. Businesses for decades have bought and sold their business assets, including their valuable information data bases about their customers. Nothing new in that.

As I have said many times before, personal information has value to both consumers and an information economy. We live in an Internet Information Age and obviously information is the lifeblood of that system. A consumer's purchasing patterns, online behavior, is indeed valuable information to marketers. But at the same time, I believe consumers should have the ability to control that information or at least to be potentially compensated for giving away personal information if it indeed is a valuable asset.

One of my witnesses who will testify later this morning has a business model that operates on consumers being compensated for sharing their personal information.

The issue as we move forward in the coming years are these: Has industry done enough to protect consumer privacy, or should government step in to establish minimum standards to protect against the bad player? And if there are standards that work for private industry, should they also be applied to government's collection of personal information? After all, I can choose whether to give information to a private company, but in many government agencies I don't have a choice. I am obliged to provide them with personal information. Does the government have a higher standard in play here to protect the privacy of my information?

Well, hopefully this morning will shed some light on these matters. While the tremendous amount of attention over the past year has been paid to the privacy of consumers in dealing with private industry, very little has been paid to the Federal Government's collection of personal information. Last time I checked, very few consumers indeed were providing information to the IRS, strictly voluntarily. Consumers indeed can vote with their feet in the private sector and go to another business if they don't want to share private information with them; but can you refuse to do business with

the IRS or the EPA or the Medicare program for that matter? And if you do, can you refuse to provide them with information they require of you in order to do business with them?

Earlier this year, Representative Dick Armey and I asked the GAO to conduct a survey of the privacy policies of Federal web sites and then compare it to the fair information practices recommended by the FTC for commercial web sites. In short, we wanted to see if Federal web sites would fare any better than the commercial web sites if they were held to the exact same standards that the FTC has held the commercial web sites in their reviews. Was the Federal Government ready to practice what it has preached?

Well, from the results of the survey which we will discuss today, it appears that the Federal Government does not practice what it preaches. Our report is not the only GAO report that has produced failing grades for government web sites and data bases. The Horn report on data base security and the Lieberman report on OMB privacy requirements have also both shown that the government is not doing an adequate job of protecting America's personal information.

On just two issues in recent weeks, the government has flunked. On the placement of cookies on government web sites the results are troubling. Despite OMB memoranda in 1999 and in June of 2000 prohibiting the placement of cookies on Federal web sites, the practice continues today at the IRS and possibly at other government web sites. In fact, we learned in the GAO report, I think, that 14 percent of the web sites surveyed potentially permit cookies on their Federal web sites. And just last Friday, the AP reported that the White House web site itself violates COPPA by collecting personal information from children.

While government web sites can hide behind different standards, in these two instances they certainly do not live up to the spirit of the laws that apply in the commercial world.

Chairman Pitofsky of the Federal Trade Commission has graciously agreed to testify today about the many FTC reports and activities in the past year dealing with privacy. We will also hear from private-sector witnesses who will discuss online profiling, the Children's Online Privacy Protection Act, and the use of technology in protecting privacy, and we will hear from one entrepreneur with an interesting take on privacy. In short, we will be looking at both the government sector and the private sector today, and we will examine just how well we stack up.

In short, while there is no obvious time this year for this committee to engage in legislation in the remaining days of this session, this hearing will be preparatory to activities next year in which we will continue our efforts to guarantee that both the Federal Government and the private sector respect the privacy of American citizens.

I want to close by inviting you—I understand the web site is down this morning, but to visit the EPA web site. Our staff visited the EPA web site, I believe yesterday, and discovered that there is on the EPA web site a section called Explorers Club which invites children to give information about themselves to the EPA. Nowhere on this web site is there a disclosure that children should first get

permission of their parents before sharing their private information with a government agency. There is something wrong when Federal agencies can't obey the law that we impose on private citizens.

The Chair yields back his time and the Chair recognizes the gentleman from Virginia, Mr. Boucher, for an opening statement.

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

PREPARED STATEMENT OF HON. W.J. "BILLY" TAUZIN, CHAIRMAN, SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE AND CONSUMER PROTECTION

Today this subcommittee will hold a hearing on important developments in the efforts to protect the privacy of American consumers. Few issues in this industry generate such strong emotions as how to deal with the enormous amounts of personal information that are collected, distributed and stored everyday via the Internet.

This morning we will hear from two of our colleagues Rep. Claw Shaw and Rep. Bob Goodlatte. Rep. Shaw will explain to the Subcommittee his legislation, H.R. 4857 the Privacy and Identity Protection Act of 2000 which has been reported out of the Ways & Means Subcommittee on Social Security and is currently awaiting action in this Subcommittee.

In addition, the Subcommittee will hear from Rep. Goodlatte about the Lansdowne Privacy Summit which the National Chamber Foundation hosted for House Republicans in May of this year and what has come from that. Rep. Goodlatte co-hosted along with my colleagues Chairman Bliley, Rep. Ehrlich and myself, the Privacy Summit and I personally want to thank him for his efforts in this endeavor.

I want to thank both of our colleagues for coming this morning and sharing their views with us.

This Subcommittee has been a keen observer of the debate for many years—holding hearings on this issue in 1998 and 1999. Over the last year we have seen consumer concerns over privacy heightened and as a result specific federal responses. This past year we have adopted two federal laws to deal with specific areas of concern—the Gramm-Leach-Bliley law and the Children's On-Line Privacy Protection Act. In addition, consumers have witnessed the development of new private sector technologies to help consumers as well as voluntary standards by industry to self-police and educate consumers. In certain areas, the federal government and commercial entities have come together to achieve cooperative standards to govern their on-line conduct.

Privacy was not created with the advent of the Internet, but it does add a level of dissemination beyond what Americans had ever thought possible and in many circumstances are comfortable with.

While the Internet is still relatively new, the issue of privacy is not. Prior to the adoption of the GLB and COPPA laws, Congress had enacted privacy protections in a dozen other circumstances over the past thirty years starting with the Fair Credit Reporting Act in 1970. The sharing of personal information did not begin when the Internet was established—how many people remember party line telephones and can recall door to door salesmen plying their wares using neighborhood directories. Businesses for decades have bought and sold their business assets *including* the valuable information databases about their customers.

As I have said many times before, personal information has value to both consumers and to our economy. We live in an Internet and information economy and information is the lifeblood that makes our Internet engine run. A consumer's purchasing patterns and online behavior is valuable information to marketers, and I believe that consumers should have the night to control that information or be compensated for giving such personal information to business. One of our witnesses who will testify later this morning has a business model that operates on consumers being compensated for their private information.

The issue as we move forward in this debate in coming years is this: Has industry done enough to protect consumer privacy or should government step in an establish minimum standards? There are no simple answers. Hopefully this hearing will help shed some light on these matters.

While a tremendous amount of attention over the past year has been paid to the privacy of consumers in their dealings with private industry, very little has been paid to the federal government's collection of personal information.

Last time I checked, very few consumers have the option of not providing a government agency with their personal information. In the private sector, consumers can vote with their feet and go to someone else if they do not like the privacy policy

of a business. Americans must deal with the IRS, EPA and the Medicare program and cannot refuse to provide personal information.

Earlier this year, Rep. Dick Armey and I asked the GAO to conduct a survey of the privacy policies of Federal websites and compare it to the fair information practices recommended by the FTC for commercial websites.

We wanted to see how Federal websites would fare if they were held to the same standards as commercial websites.

Was the Federal government practicing what it preached?

From the results of the survey, which we will discuss today, it appears that the Federal government does not. But our report is not the only GAO report that has produced failing grades for government websites and databases. The HORN report on database security and the LIEBERMAN report on OMB privacy requirements have shown that government is not doing an adequate job in protecting American's personal information.

On just two issues in recent weeks the government has flunked. On the placement of cookies on government websites the results are troubling. Despite OMB Memoranda in 1999 and June 2000 prohibiting the placement of cookies, that practice continues today at the IRS and possibly at other government websites. And just last Friday the AP reported that the White House website itself violates COPPA by collecting personal information from children.

While government websites can hide behind different standards, in these two instances they certainly do not live up to the spirit of the laws that apply in the commercial world.

Chairman Pitofsky of the Federal Trade Commission has graciously agreed to testify today about the many FTC reports and activities this past year dealing with privacy.

We will also hear from private sector witnesses who will discuss online profiling, the Childrens' Online Privacy Protection Act, the use of technology in protecting privacy and we will hear from one entrepreneur with an interesting take on privacy.

In closing I want to thank all of the witnesses for their attendance today.

Mr. BOUCHER. Thank you, Mr. Chairman. I want to begin by complimenting you on your handling of the delicate and complex matter of establishing a Federal privacy policy respecting the practices of web sites that collect information from the Internet-using public. The chairman has properly taken a cautious and deliberative approach toward the development of legislation in this sensitive area. In my view, the time for legislation has now arrived.

With the hearing today, I urge the subcommittee to begin the process of developing a federally assured baseline set of guarantees for personal privacy with respect to the information collected by web sites through the use of cookies placed on the hard drives of web site visitors. The requirements which Congress should enact are straightforward and would be in the nature of minimum guarantees that would be applicable to all web sites. I suggest that our legislation contain the following five elements: First, each web site should provide a clear notice of what information is collected from the Internet-using public and how that information is used. If the information is used internally within the web site, that fact should be stated. If there are circumstances under which the information is transferred to third parties, that fact should also be stated and those circumstances listed.

Second, after reviewing the policy, the web site visitors should be able to limit the information about them which is collected, and in practical terms that may mean that he would depart the web site with no information being collected, a practice that we commonly would refer to as an opt-out.

Third, the Federal Trade Commission should be directed by statute to create a mechanism to assure compliance with these basic privacy guarantees.

Fourth, the legislation should declare that the policy is the national policy and preempt any State requirements that are more onerous or inconsistent or in conflict with the national guarantees as assured in the statute.

And, fifth, the Federal Trade Commission should be instructed to review web site practices on an ongoing basis and recommend any additional legislative steps that may be appropriate.

I would suggest that a number of benefits would flow from the passage of this set of minimum statutory guarantees. First, it would assure that all web sites, whether privately operated or operated by a government agency, respect privacy. The larger commercial sites are presently members of self-regulatory organizations and generally respect the privacy policies announced by the SROs. Smaller web sites in large numbers do not belong to SROs, and government agencies have observed a privacy policy in a truly voluntary way, which has been somewhat inconsistent, as the chairman has suggested. In our view, all sites should be covered by a minimum Federal guarantee.

Second, the legislation would establish only a minimum set of guarantees and web sites could then offer higher levels of privacy protection and market that enhanced privacy as a competitive difference, and so offering greater levels of privacy would then become a competitive asset in the marketplace.

Third, this basic privacy guarantee would encourage the growth and development of the Internet by creating the confidence in Internet users that their privacy is being protected.

And, forth, we can assure that the law is efficient and workable by prevent a patchwork of inconsistent or conflicting State requirements from arising.

The Federal Trade Commission has called on the Congress to act and it is time for the Congress to accept that invitation. And I believe that we can do so with a large consensus of support from the private sector. Over the course of the last several months, I have watched that consensus grow, and it is in support of the kinds of steps that I am recommending that we take this morning.

I want to welcome to the subcommittee today my friend and Virginia colleague, Bob Goodlatte, with whom I have the privilege of cochairing the House Internet Caucus. Eighteen months ago, Mr. Goodlatte and I put forward legislation which closely resembles the recommendations that I have made this morning. Our Internet Caucus has also been active over the course of the last year. We have conducted a technology demonstration to demonstrate various technical means of protecting personal privacy for Internet users. We have also conducted two widely attended workshops on the question of protecting Internet user privacy. And now we are planning to take our activities to the next level.

During the coming days we intend to establish a working group of interested Members of the House and Senate, primarily composed, I suppose, of Members of the Internet Caucus, but anyone is certainly welcome to participate. And our goal in establishing this working group will be to help in developing a broad consensus in support of the elements that should comprise our privacy legislation during the course of the next Congress. It is our hope that the consensus-building process will include consultation with the in-

dustry and with the Federal Trade Commission, and we hope to achieve the consensus that we are seeking within a matter of just several months so that by January, recommendations can be in hand that enjoy the support of a broad consensus within the stakeholder community and among Members of Congress.

I look forward to working with the interested members of this subcommittee and with my friend, Mr. Goodlatte, and the members of the Internet Caucus as we consider the best means of enhancing privacy protections for the Internet-using public.

Mr. Chairman, I want to commend you for this timely hearing. I frankly wish it was a little bit better attended because it truly is an important subject. And I want to commend you also for the careful and thoughtful way in which you have addressed it, and I look forward to working with you as we seek to assure that the Internet-using public, truly has its privacy protected. Thank you.

Mr. TAUZIN. I thank the gentleman and, believe me, I feel very similar about the gentleman's involvement. I pledge to him that, as I did privately, we are going to work very closely over the next several months in preparing for some very serious work on this issue next session. I thank the gentleman.

The Chair recognizes the gentleman from Illinois, Mr. Shimkus, for an opening statement.

Mr. SHIMKUS. Thank you, Mr. Chairman. I will be brief. I do believe, as many of us do, the big issue of the new millennium will be privacy, and it is a great issue because it really brings the political spectrum of the far left and the far right together as teammates really trying to address the concerns of the good government types that want to create new efficiencies for government to provide services with the possibility of accepting and storing personal data.

So this is a great time to have this hearing. I am concerned about the policies and statements that we enact as the Federal law, but I am more concerned that we follow those policies and statements which it seems—because those of us who are not that technology expert, you know, unfortunately we are a very trustful Nation, we trust everybody. And so if an agency says this information is not going to be used and they ask for information, well, we think oh, good for them. But the information is still being gathered and stored.

I hope that this debate stirs up the whole issues that I think our Founding Fathers would be very proud of: the debate of personal privacy, actually privacy rights which would be similar to property rights, in that there are some—they are part of the fabric of our national culture—that I think we have lost through the technology age and information age that we need to get back to some privacy rights issues.

Again, I think the Founding Fathers would be pleased about this debate, and we have a lot of work to do. I appreciate this hearing and I look forward to being engaged with my friends from Virginia and members of this committee as we move forward in the next Congress. I yield back my time.

Mr. TAUZIN. The Chair recognizes the gentleman from Ohio, Mr. Sawyer.

Mr. SAWYER. Thank you, Mr. Chairman. I can't help but think our Founding Fathers would be proud but flabbergasted by this debate. I want to join with my colleagues in thanking the chairman for this hearing today. As he suggested, many businesses and many other kinds of entities have long collected information about Americans for a variety of purposes, but today the users of individual reference services and lockup services operate computerized data bases on personalized information that have expanded the concept beyond what most Americans have ever really seriously thought about, but they will be thinking about them a great deal more in the future.

Most of us are familiar with the story Thomas Friedman likes to tell. The New York columnist checked into a hotel with his wife and children and, as children are wont, they wanted to go to the hotel pool right away. So they jumped into their swimsuits, went downstairs and got in the pool. When it came time to get out of the pool and go back to their rooms, they discovered that he had left the hotel key in the room. And so, dripping wet, with little more than a bathing suit and a towel, he went up to the front desk and asked the check-in clerk if he could get an extra room key. And the clerk said, "I am sorry; if you don't have any identification with you, we can't do that."

Then he said, "I will call my manager." And the manager came out and said, "Mr. Friedman, I really could not do that in good conscience. Plus you wouldn't want me to give your key to someone who simply came up in a bathing suit and said that he was you."

In the meantime he is standing there, he is working with the computer. The manager said, "But wait, can tell you what room you are in." He said, "When are your kids birthdays?" He said, "Here's your key." Friedman said, "Why did you do that?" The manager said, "Because you stayed here 9 months ago and we have all of this information and a whole lot more about you." And he said, "Thank you very much."

Friedman was gratified, but he was dumbfounded by the level of information and the depth of knowledge they had about him as a product of simply having checked into the hotel on a previous occasion.

That is chilling information, and it is a remarkable example of why the hearing that we are having today is important. I appreciate the comments about the relationship between information gathered by Federal agencies and those gathered by businesses over the course of the last couple of days, Mr. Chairman.

Ironically, I have rejoined a discussion that I have been involved in for the last dozen years about data sharing across government agencies. Those are efforts over the last 210 years to gain access to private individual information gathered as a product of the Census that has never been violated in the 210-year history of this Nation.

If we are looking for principal examples of the fundamental ideas behind which we might seek to guard information, we could do no better than to turn to the kind of repeated efforts that have been made to penetrate the Census, and the efforts that the census has made to guard against that. Even as we learned last spring, in times of war when efforts were made to individually identify Japa-

nese Americans living in the United States, United States citizens, and that effort was directly resisted as a product of the work of the census.

Personal information is our single most valued possession and the work that we are doing here today could not be more important. I thank you for that and yield back the balance of my time.

Mr. TAUZIN. By the way, that hotel has new personal data on Mr. Friedman: the fact that he loses his key.

The gentleman from Maryland, Mr. Ehrlich.

Mr. EHRLICH. Real briefly, real brief. Everyone said really what I can say. This is a timely issue. It is an emerging issue. It has always been a second-tier issue, now rapidly becoming a first-tier issue in American politics. If there is any doubt for anybody in this room that this issue is very important to them, let me assure you that there should be no doubts, because the chairman and I regularly have conversations about this. We have already had one conference, to be followed by many more conferences and hearings, and hopefully a good piece of legislation. And I yield back.

Mr. TAUZIN. I thank my friend and also thank him for cohosting the conference with Chairman Bliley and Mr. Goodlatte and I. And, as you know, we will hear about that conference a little later, but again I want to thank the gentleman for his personal involvement because it is going to take a lot of members' involvement for us to unravel all these issues by next year.

The Chair welcomes and recognizes Mr. Luther for an opening statement.

Mr. LUTHER. Thank you, Mr. Chairman. Thank you for holding this important final subcommittee hearing.

I want to thank you and Mr. Markey and Mr. Boucher for your leadership on this subcommittee and on this issue, and I am pleased to hear you say that this hearing will only be the beginning on this issue and that hopefully in the next Congress we can deal very substantively with this particular issue for the benefit of America's consumers.

Last November I was pleased to join Representative Markey in introducing H.R. 3321, the Electronic Privacy Bill of Rights, which would require web site operators to comply with the so-called Fair Information Practice Principles.

I would also be remiss if I didn't mention this morning the great work of my colleague and friend, Congressman Bruce Vento of Minnesota, who passed away yesterday morning. Bruce introduced two online privacy bills, and I want to recognize him for his hard work on behalf of the American consumer on this issue and on so many other issues through his lifetime.

Mr. TAUZIN. Would the gentleman yield? I wonder, Mr. Luther, if we might ask all our friends for a moment of silence in memory of Mr. Vento. He was indeed a dear friend of many of us, and his passing is very hard on many of us. We ask you all now to join us in a moment of silence.

[Moment of silence.]

Mr. TAUZIN. Thank you. Mr. Luther.

Mr. LUTHER. Thank you, Mr. Chairman.

In light of both the FTC and GAO studies that report that an unacceptably low percentage of web sites comply with the fair infor-

mation practices, I look forward to hearing our panelists' opinions. Hopefully their testimony will provide insight as to what we as a committee and as a Congress can do to protect the American consumer from this wholesale collection and distribution of personal information.

Thank you, Mr. Chairman and I yield back.

Mr. TAUZIN. Thank you, Mr. Luther.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. PAUL E. GILLMOR, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Mr. Chairman, I want to thank you for calling this important hearing today on the matter of protecting consumer privacy. Public opinion is strongly behind the need to safeguard personal information. I believe this issue is important and I am pleased that our committee is spending some time to look into this issue.

During our committee's most recent foray into the issue of privacy, during the Gramm-Leach-Bliley financial services law, we learned just how complex an issue this is. I was pleased to be one of the active members of this panel on the privacy issue and think our work in this arena has just begun.

Privacy laws, in themselves, are not new things. However, with emerging Internet technologies, I believe it is crucial that Internet users and consumers can feel safe that the information that they are transmitting is being protected from others. I like to draw the parallel on this subject from Federal wire-tapping laws that our nation passed to protect telephone customers from unwanted parties. In the same way, we must ensure the integrity of the lines carrying Internet conversations.

I come from the perspective that a person's information is his or her own. And, that when a person decides to give up some of their individual data, it is for a specific and intended purpose. I do not believe it is up to the merchant to decide how and when a person's information should be used, especially if it falls outside of the initial transaction that precipitated the need for the person's data.

I look forward to the testimony of our witnesses. I am especially interested in listening to the Government Accounting Office's assessment of the present situation, as well as the thoughts of the Federal Trade Commission. As most members of the panel know, while the FTC lacks the authority to regulate operators of commercial websites, it has been busy looking into this matter and issuing reports a direction it believes is the most appropriate from containing unwarranted releases of personal information. I believe this will be a good starting point for our most recent discussions.

Again, Mr. Chairman, I want to thank you for calling this hearing and your diligent work on this matter. I pledge my support and help to you in working on future legislation to ensure the privacy rights of all Americans.

PREPARED STATEMENT OF HON. TOM BLILEY, CHAIRMAN, COMMITTEE ON COMMERCE

Good morning and thank you Mr. Tauzin for holding this hearing today.

Two and one half years ago, when this subcommittee held its first hearing on Internet privacy, many of us in Washington were just starting to learn what the issue of online privacy was all about.

Consumers were just learning how companies collected information from them and how the companies used it.

Businesses were just starting to become aware how important an issue privacy was to their consumers and finally government was starting to understand the public policy issues surrounding online privacy and electronic commerce.

Looking back all those months, I think we have made great progress. Consumers are more aware of how to protect their privacy as they go online—whether through the use of new privacy protecting software or by knowing what to look for in a privacy policy.

Businesses also understand how important it is for their customers to feel safe, secure and private while online.

Industry groups like the Online Privacy Alliance have been working on tough industry guidelines and they have made excellent progress toward effective self-regulation.

But this said, there is still more for industry to do such as: ensuring that consumers do have the choice to "opt-out" of providing personal information and work-

ing with outside auditors to ensure privacy policies are being adhered to and the consumers have recourse if they believe their privacy has been violated.

I have said throughout this debate that I believe self-regulation is a better approach than government regulation. Government regulation by its nature is slower to respond than the marketplace and much less flexible and could place a serious competitive burden on the dynamic Internet economy.

Before I close, I would like to leave some advice for the future Congresses that discuss and debate this issue.

My policy toward the Internet economy has been simple—"First do no harm." It is a policy I hope that will continue in Congress and in this Committee.

Privacy is a complex issue and Congress should not act hastily but rather carefully and deliberately on this issue. Over-regulation of the engine of growth of our economy would be foolhardy and imposing rigid regulations that don't take into account new privacy protection technology would be short sighted.

On that note, it is important to keep in mind that slightly altering the current privacy restrictions can have a dramatic impact on the business plans of Internet companies. Today, much of the information on web sites is free, driven by advertising. Putting burdensome privacy restrictions could fundamentally change this structure and move us towards a pay-site world. We must be cautious. We must know the effects of any changes that are proposed—not just on privacy but also on Internet functionality and operations.

Thank you Mr. Tauzin and I yield back the balance of my time.

PREPARED STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. Chairman: I want to thank you for holding this important hearing on consumer privacy issues.

Mr. Chairman, as American consumers venture onto the Internet to browse for information or to purchase one of the millions of products available online, they do so with a belief that their time on the Internet will be anonymous.

Unfortunately, that is not necessarily the case.

Sophisticated computer programs have been developed that allow companies to track consumers as they surf the Internet.

What I find most disturbing about this practice is that the level of detail that can be acquired about a consumer's personal habits and preferences is staggering.

Fortunately, most of this data is still anonymous and is being collected without the detailed personal information that would allow direct marketers to bombard you at home with advertisements for products you viewed while on the Internet.

However, the technology already exists to tie your name, address, social security number, and other personal information traits to you while you are online and that is where the true privacy battle must be joined.

The Internet is a tool of convenience, but to use that tool consumers should not be forced to relinquish their right to privacy.

I will introduce legislation today that allows e-businesses to collect and compile customer information acquired through normal business transactions so long as it is for internal use only.

This legislation will explicitly prohibit the anonymous tracking and merging of personal data with site the individual has visited online.

While I do not believe we can make shopping online as anonymous as buying something at the mall with cash, that should be our goal.

I believe the fastest way to hurt the growth of the Internet is to have American consumers lose faith in their ability to control their personal information.

The FTC has taken a step in the right direction in outlining what commercial Internet sites should consider having as a boilerplate privacy policy.

The four FTC principals of notice, consent, access, and security each are important components to ensuring online privacy.

It is my hope that in the next Congress we will begin to outline the basic protections that all consumers can expect when they transact business or just surf the Internet.

I commend the many e-businesses that have understood the need to develop and update their privacy policies. These e-businesses are responding to the concerns of their customers and are in turn safeguarding their future business.

Mr. Chairman, I look forward to hearing from the witnesses and I yield back the balance of my time.

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

Thank you Chairman Tauzin and Ranking Member Markey for holding this important hearing on recent developments in privacy protections for consumers. It is vital that we address issues of consumer protection and privacy in the information age to ensure that we are providing the public with the security it needs and desires to deal comfortably in the Internet marketplace.

Research done over the last several years indicates that consumers are frustrated by the increase by website operators in gathering and disseminating personal information, often without an individual's knowledge. Technologies such as cookies and click streaming enable website operators to collect personal information about visitors to websites, then sell information regarding an individual's Internet research. My constituents do not want their personal data collected by either commercial or government websites.

I hope the panelists address what level of privacy individuals and organizations can reasonably expect in our digital world. Consumers want to be able to surf the Internet without having their viewing and purchasing habits tracked. Marketers seek to better tailor their advertisements as well as provide consumers with more personally tailored products and services. We need to determine how to assure privacy in a medium where incredible amounts of data reside.

I am looking forward to the testimony of witnesses today. I would like to hear from all of them on what they believe the best way is to strike a balance between the privacy desires of consumers and the marketing desires of commercial website operators. Do all of the witnesses believe that government must step in to establish minimum protections as the Federal Trade Commission has suggested? Can industry self-regulate itself? What do we do about bad actors in the system? Should government websites be held to the same standard as commercial websites?

It is my hope that both industry and government can reach a consensus on what the best policies are to provide consumers with the privacy protections they desire while giving online businesses the ability to better tailor their marketing.

I am also interested to hear from the witnesses on the implementation process for the Children's Online Privacy Protection Act. Does the Federal Trade Commission need to revise some its rules pertaining to the Children's Online Privacy Protection Act? Are the concerns of children's website operators regarding their ability to comply with the Act legitimate? Should Congress amend the law to subject federal websites to the provisions of the Act?

Thank you Mr. Chairman. I yield back the balance of my time.

Mr. TAUZIN. The Chair is now pleased to welcome our first witness, indeed our good friend from the Judiciary Committee who I think spends more time here than he does with his own committee, the honorable gentleman from Virginia, Mr. Bob Goodlatte. Bob, I spoke last night at midnight with your Chairman, Mr. Hyde, and he was kind enough to get on the phone with his staff last night and work out the final details of the Firestone recall bill that we passed last night, and I again wanted to thank all of you members of the Judiciary Committee for the excellent cooperation your committee provided our committee in resolving the technical areas of common concern in the bill and for waiving referral to the Judiciary Committee.

Again, if you will extend my thanks on behalf of the Commerce Committee to other members of the Judiciary Committee, I would deeply appreciate it. As you know, the bill passed last night and is now on the way to the Senate. Again, we are very grateful for the work of our good friend Mr. Goodlatte on the Judiciary Committee. You are recognized sir.

STATEMENT OF HON. BOB GOODLATTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA

Mr. GOODLATTE. Thank you, Mr. Chairman. I want to thank you and other members of the Commerce Committee for similar cooperation and coordination of legislation that these committees

share on many occasions, and you've been very helpful to us. We very much appreciate that, and I will pass your remarks to Chairman Hyde on to my colleagues on the Judiciary Committee.

I also want to thank you for allow me to testify today. I do want to know how many appearances are required before I can get a guest member status, but I do very much appreciate the opportunity to testify on this very important issue, which I must also thank you for your leadership on this. You were very instrumental in organizing the retreat which you have referenced which Congressman Ehrlich, Chairman Bliley and myself were privileged to cohost with you. I felt that it was a very, very productive retreat for Republican Members, and while this hearing is bipartisan in nature and we intend to work with our Democratic friends on this issue as well, that retreat which heard from experts in industry, academia and various think tanks on this increasingly important issue, yielded I think some very substantive results. I can say with confidence that it was a success and I think members learned a great deal about the issues. We discussed what the main privacy concerns of our constituents are, including unsolicited direct mail marketing, the collection of personal information on the Internet, the disclosure of personal financial information by financial institutions and identity theft and other criminal uses of personal information for fraudulent purposes.

We also learned about the complexities of how information is used by commercial entities and that any privacy legislation needs to permit the beneficial uses of the information as well as address consumer concerns. And finally, we learned that we need to use a combination of tools to address privacy: 1) targeted legislation that specifically identifies the harm we are trying to regulate; 2) education to ensure consumers know what their rights are and how to commercialize those rights; 3) technological tools on the Internet to allow consumers to control their information better; and 4) policies that encourage and reward businesses for self-regulation and protect consumer privacy at the same time that they extend enormous new benefits to consumers by making valuable information available to them. We also have to be careful not to increase identity theft and fraud by making information unavailable to businesses and law enforcement to detect and stop crime.

I also want to recognize and thank my colleague from Virginia, Congressman Boucher, for his dedicated hard work on this issue. We are, as you well know, the cochairs of the Congressional Internet Caucus, and with the hard work of Congressman Boucher the Caucus has sponsored a number of privacy-related activities and events in recent years, including several public policy forums, a technology demonstration of the latest privacy technologies, and a briefing book for Members that outlines various positions on the issues of online privacy.

As my colleague mentioned, the Caucus will continue to be active on this issue after we adjourn this year. Earlier this year I had the opportunity to lead a congressional delegation along with Congressman Boucher that was attended by several members of the Commerce Committee, including Congressman Gordon, Congressman Stearns, and Congressman Pickering, in which we had the oppor-

tunity to testify before the European Parliament on the issue of privacy as relates to electronic commerce.

As a part of that testimony, we promoted the efforts to coordinate privacy policy with the European Union, something that, as you know, is vitally important and something that hasn't been mentioned thus far today but is also important looking toward our States as well. We have a great concern that if we have 50 different State privacy policies enacted by our State legislatures, many of which are very active on this issue today, as well as differing privacy policies around the world, we will have an unworkable situation on the Internet. And so the effort to promote the safe harbor that allows U.S. companies to do business in Europe by meeting certain standards, while not requiring the United States to pass legislation that may be contrary to our interest and the intent of the majority of the Members of Congress, is vitally important.

It is also important to recognize the contribution that industry has made because substantial progress has been made in the area of self-regulation. At this time, the vast majority of Internet sites of major businesses have good, solid privacy policies that are enforced by those companies, and that progress which would indicate that, for example, of the top 100 web sites in the country, they have improved from 71 percent having a privacy policy to now better than 95 percent is progress, but obviously more work needs to be done in this area.

Mr. Chairman, you have noted the substantial progress we have already made in a number of targeted areas dealing with children's privacy, financial privacy, and medical privacy. I think that is the type of approach that we should continue to pursue, not a shotgun approach, but a targeted approach to where the problems exist. We believe that through private initiative and this targeted Federal action, we have been making and will continue to make substantial progress toward achieving balance, toward ensuring adequate consumer protection, encouraging the development of electronic commerce.

As we look ahead, obviously bipartisan support is vital. And I am pleased to hear so many Members on each side of the aisle commit to that, because that is exactly what is called for. There have been several legislative proposals introduced and considered in the Congress this year, and it is unlikely they will see any of them enacted into a general online privacy law this year. That is a good thing, that is not a bad thing. And I know there have been those who have been pushing for us to take action before we adjourn this year, but quite frankly the Congress must approach the issue of comprehensive online privacy information in a careful and deliberate manner, and that is exactly what we are doing with your leadership here today.

Last, I want to say a little bit more about what Congressman Boucher mentioned, and that is the desire of the Internet Caucus to work with you and other Members of the Congress as we brainstorm, if you will, for ideas on this work in this direction. And I do think Congressman Boucher has outlined the shape of a very good potential piece of legislation, very similar to what came out of the privacy retreat which we host, and we are moving toward

that kind of consensus; but during the time between now and when the Congress reconvenes in January, there is much work to be done, and the Internet Caucus intends to be a part of that by coordinating a working group of Caucus members and others to develop a statement of principles on Internet privacy.

This working group will consist of any member of the Caucus or others who are interested in the issue of online privacy, will work informally from now until the new Congress convenes in January to outline those areas the Caucus deems important to address in any legislative initiative. And Members who have been leaders on privacy issues from both sides of he aisle and both sides of the Hill, from Congressman Asa Hutchinson to Senator Ron Wyden we hope will be actively involved in the working group. And we are also hopeful that by working in a bipartisan manner, we can contribute to the process which will begin in your committee, and to ensure that all Members of the House, including new Members who are still looking for information, are prepared to act on any legislation that is considered in the early part of this year. I thank you again for the opportunity to testify today and look forward to continuing to work with you.

Mr. TAUZIN. Thank you, Mr. Goodlatte.

Let me first of all—you mentioned Asa Hutchinson. I wanted to state publicly our concern about Asa's bill to create a commission, which many members of this committee voted against, was not, of course, that we don't do an awful lot of work done on this issue and, as you pointed out, perhaps even some legislation next year, but it was our concern that this work ought to be done by Members of Congress rather than some commission. And Asa and I have had many discussions about that. Our opposition was simply that it was a job we had to do and we needed to get about doing it.

Second, I think you will recommend to our good friends on this side of the aisle the experiences of the Lansdowne conference. I know the Chamber Foundation has agreed to conduct a similar treatment for Members of the Democratic Conference or Caucus.

Let us talk about the Lansdowne conference quickly, Bob. First of all, it rained all weekend, so everybody had to listen to each other, which was pretty good after all the meetings, all the panels, which included, as you pointed out, members of industry, academia, think tanks, consumer representatives. After everybody had a chance to listen to one another, wasn't there a major shift in the conference opinion by the time we left the early morning sessions on the first day until the last session, and didn't that shift represent a sort of major redefining of our mission bearing on privacy?

Mr. GOODLATTE. I think there was definitely a coming together of ideas. And speaking about Asa again, one of the reasons why I also did not vote for his legislation was, in addition to the fact that Congress needs to address this, I think the speed with which we need to address it is upon us; and therefore, some might take the establishment of a commission that would last for some lengthy period of time as a putting off of addressing this, and I don't think we should do that. And I think that one of the things that came out of that conference was that we need to act in a comprehensive manner and we need to do it in such a way that sets a minimum

baseline. There is an opportunity for legislation here that promotes self-regulation.

Mr. TAUZIN. Let us talk about some of the issues the conference highlighted. One of them was harmonizing various privacy laws. The conference—I noted the fact that in some of the State legislatures of our land, there were as many as 200 bills filed. I know most of them didn't pass, but there is a lot of activity going on in State legislatures to establish privacy rights that may be very different from one another and may create some very different laws, all set on top of an Internet interstate-international commerce question, and would you address that quickly for us?

Mr. GOODLATTE. Well, I think we have an international problem here. We have to start by having our own house in order in the United States.

And the chairman is absolutely right. One of the things that I mentioned earlier that came out of the conference was the need to have Federal legislation. To avoid having 50 different States have 50 different privacy policies that are inevitably going to conflict with each other in a company attempting to do business in interstate commerce on the Internet is going to have to have a consistent policy. I mean, you can't have a web site which has two conflicting requirements on it, much less perhaps 50 different States with a multitude of different components of regulation that could collectively make it a totally unworkable proposition, particularly for a small business that wants to do something to supplement their bricks-and-mortar business with some Internet business and suddenly find that they have an enormously impossible task of complying with regulations. So we need to come up with something simple and understandable and comprehensive that everyone can comply with and avoid this problem.

Mr. TAUZIN. We also ran into the question of various Federal agencies adopting privacy policies that may or may not be in conflict with one another or in conflict with those State laws and businesses that have to comply with more than one agency privacy policy that may be different from one another. And the question was, do we need to focus on harmonizing the Federal standards as it applies to private businesses doing business with the Federal Government?

Mr. GOODLATTE. Well, I think that is absolutely correct. And we have to make sure the Federal Government itself, as you noted earlier, is setting the example of protecting the privacy of consumers and not abusing already existing laws much less.

Mr. TAUZIN. Finally, we are going to hear from the GAO about the various tests by which web sites are judged or rated, and we will hear from the FTC about how well privacy is being protected in the private commercial sites of America and we will learn that there are always going to be some bad actors, some bad players. Can we trust on privacy to be totally protected by private sort of self-policing organizations, or will we need some minimum standard by which—or something that applies to those sites that refuse to be members of self-policing organizations?

Mr. GOODLATTE. We are always going to have, of the millions of commercial web sites, some that are going to, either through neglect or through deliberate desire to misuse consumers' privacy,

abuse this process in very unacceptable ways that are going to harm consumer confidence in the entire Internet. And therefore it seems to me that legislation should include a baseline standard to go after those outliers who are not going to meet that standard.

When we do that we have to be very, very careful that we don't get into the idea that we should dictate the minutia of how businesses protect privacy of consumers when we have, in fact, a long history, as you cited, of useful information being made available to consumers through businesses.

Mr. TAUZIN. Finally, Bob, I want to ask one thing of you, the Internet Caucus. If you don't mind, I would very much appreciate if before we get to this matter next year, if you would perhaps cohost with us a technology demonstration for all Members of the Congress to see the new technology in privacy. At the Lansdowne conference we saw some new software, some new hardware, some new IP systems by which consumers can and will be able to protect themselves from sites that might be negligent or intentionally damaging to their privacy, and I think a demonstration of all those new technologies would probably help us understand what needs to be done in law and what can be taken care of in technology and self-policing.

So I would ask of you that consideration of perhaps some sort of technology demonstration for our committee, perhaps in union with the Internet Caucus perhaps next year.

Mr. GOODLATTE. We would be delighted to work with you to do just that. We have hosted some similar demonstrations and, you know, it is a hard time reaching so many Members of Congress who have such busy schedules, so continuing to do that and perhaps in conjunction with the committee here, tap a committee room or something.

Mr. TAUZIN. They could come or we threaten to release their private information.

Mr. Boucher is recognized.

Mr. BOUCHER. Well thank you, Mr. Chairman. And let me echo the comments of Mr. Goodlatte about our willingness through the Internet Caucus to integrate our activities more closely with those of this subcommittee, both in terms of conducting demonstrations and perhaps also in terms of having panel discussions that are apart from the formal hearing process and through other ways collaborating in the development of good policy.

I want to commend Mr. Goodlatte on his superb statement here this morning, I will note in passing that I am not a particular fan of partisan retreats, so you will not be surprised if the Democrats do not accept the invitation to have a purely partisan retreat. I tend to think that the best policy is made in a bipartisan fashion, but I am very pleased that tremendous pub members gained education from the retreat that they had.

Mr. TAUZIN. Would the gentleman yield?

Mr. BOUCHER. I will be pleased to yield.

Mr. TAUZIN. Did I notice sarcasm there?

Mr. BOUCHER. Oh, no, Mr. Chairman there was no sarcasm; the statement speaks for itself.

Mr. Goodlatte, I enjoy very much the visit that we paid to the European Parliament in February of this year and I am glad that

you mentioned that. I thought it was an informative exchange on both sides. We did have, as Mr. Goodlatte indicated, the opportunity to testify before the European Parliament on the concerns that we have on this side of the ocean about privacy protection.

At that time we strongly encouraged the formation of a safe harbor agreement which subsequently was negotiated. I am not sure we can claim much credit for, but we certainly endorsed the concept, and I was pleased to hear Mr. Goodlatte mention this morning that that safe harbor arrangement between the United States and the European Union is in the nature of a foundation. It is a minimum set of guarantees; it is in the nature of a floor. And it is anticipated that the privacy understandings between the U.S. and the European Union evolve over time.

And I would ask Mr. Goodlatte if he agrees that adopting a set of guarantees as national policy here in the United States that would assure the privacy protection of those who are using the Internet and visiting web sites, whether commercial or governmental, would be in keeping with the spirit of the safe harbor agreement between the U.S. and the European Union and would serve to strengthen that agreement to the mutual benefit of U.S. citizens and European citizens alike.

Mr. GOODLATTE. Well, I say that the legislation that you and I introduced earlier and which is a shorter form of legislation that I know that the chairman and others have been formulating in their thinking process would provide such a baseline standard of guarantees. But we have to be careful that we don't try to, I think, micromanage that as the Europeans have done. I think that the purpose of that safe harbor is to allow us to take our course of action and to continue to promote privacy in a way very different than the way that the European Union has taken that approach of basically an opt-in policy, in fact, and opt in each time somebody wants to use information. And I would say that that would be the wrong direction to head.

If I might give an analogy to other areas: If I go into a men's clothing store that I frequent every year in Roanoke Virginia—the gentleman is probably familiar with it—and they were to remember that I wear a size 40 suit and I like a particular brand of suit and so on—I am giving away a lot of privacy information—and he happens to remember that either in his head or by writing it down on a little card and keeping it in the back room, so when I come in again, he tells me about a special sale they have on this particular type of suit and pulls out the size 40 or goes directly to size 40 to see what they have in that stock, I am not in the least bit offended by that.

And I am also not offended if I go online to Amazon.com or BarnesandNoble.com and the first screen pops up and says, "Welcome, Mr. Goodlatte. We know that you are interested in biographies and we have a new biography that we think that you might be interested in." That to me is a value to consumers, in fact, in some areas like purchasing airline tickets, you are also notified of a potential reduced rate on a particular hotel room notary public in the city that you are going to. I think most consumers would appreciate having that information and they should have the opportunity to opt-out if they don't like that. But I don't think we should

get into the business of cutting people off from that, and I think that is the effect of the policy in Europe that we need to steer away from.

Mr. BOUCHER. Well Mr. Goodlatte, thank you very much. In the interest of time, I am going to stop with this. But I do want to thank you once again for being here this morning. We always enjoy having you before this subcommittee and hope that you will return.

Thank you, Mr. Chairman.

Mr. TAUZIN. The Chair asks unanimous consent, by the way, that all members' written statements be made a part of the record, including those of our witnesses. Is there any objection? Without objection so ordered.

The gentleman from Maryland first, Mr. Ehrlich.

Mr. EHRLICH. I yield my time, Mr. Chairman.

Mr. TAUZIN. The gentleman from California, Mr. Cox.

Mr. COX. Thank you. I just want to welcome my colleague, Mr. Goodlatte, and likewise thank you for your informed statement on this and all of the hard work and study that you are putting into this subject. I would like to ask you because of your role also as a member of the Judiciary Committee, whether or not you think that it would be possible to improve choices for consumers and protections for consumers by using property rights in personal information as the means by which we regulate as individuals the information sharing that goes on both over the Internet and in other forms of commerce.

I want to stress, too, that I hope we can think about this in nontechnologically bound terms, because while the Internet is certainly today's medium, the Internet wasn't around a few years ago and it may not be around in recognizable form some years from now. Catalog sellers have collected financial information long before there was an Amazon.com. Direct marketers have bought lists of names and mailing addresses long before there was e-mail. Americans have used the white pages to look up people's names and phone numbers long before search engines like People Finder were around. So in that sense, what the Internet has done is simply to improve vastly the efficiency and reduce the expense of this kind of data collection and dissemination, and that development has brought into sharp attention the longstanding tension between the desire for privacy on the one hand and the benefits of dissemination of information on the other.

So my question is whether or not as a consumer I shouldn't have the opportunity to take advantage, as you have said, of the opportunities to benefit, in many cases, from sharing my personal information. But if I am a consumer who just disagrees with you and, you know, what suit size I wear is nobody's business but my own, and that may be good for Goodlatte, may be good for Cox, but it is not good for me, the consumer, you know, should I have that choice? And can we do this, therefore, on market basis, on an individual basis, and give people property rights in the form of laws that we might pass here that would permit them in essence to license this information, sometimes for free or nominal cost, sometimes just for the benefits of whatever it is that they would be getting over the Internet, as a means of implementing this because—but I will just leave it to you to think about it and answer it—be-

cause I so fundamentally agree with what you said about the need for some predictability and uniformity. In the sense that we don't want to have all of these different privacy regimes in place and so some uniformity with a national rule might be useful, isn't it true that if you had a one-size-fits-all policy, that the downside of that is that it might not satisfy consumers, that the consumers come in a lot of different shapes and sizes, that is what markets are all about; what you really want are neutral rules of universal application that permit the maximum amount of flexibility so we can all have our own privacy policies. And the Cox privacy policy might be different from the Goodlatte privacy policy, which might be different from the privacy policy of every member of the panel, but what is the same is the law that gives us the right to choose and to enforce our choice in a legally binding way so that everybody leaves a market-based transaction happy because they chose the result, and so that we avoid the problems with government mandates which are almost impossible for everyone to leave happy because it is forced on everyone whether they like it or not.

Mr. GOODLATTE. Well, I think you make a very interesting observation. In fact, I think everyone does have their own privacy policy. If I don't like the fact that the fellow remembers my suit size and so on, I will go to another store the next time around. And similarly with other types of information. If I don't want to be listed in the phone book, I will asked to be deleted. And if there is an abuse of that information, I think we do need to set the policy to give the consumer that right so that, for example, when you go into a store or go to visit a web site, and that web site has information about me that they might want to use to give me more information, that is different than if that web site takes that information and sells it to somebody else. I need to have the opportunity to know that and make a decision about whether or not I want to deal with somebody who is going to turn around and share that information with somebody I may not want to have it shared with.

Now, there are lots of new technologies that are enabling people to establish that personal privacy policy and fine-tune it to their own preferences. P3P for example is a new technology that is growing in its use on the Internet that allows you to set your computer so that when you visit a web site it will tell you whether or not that web site has met certain privacy policies based upon your own criteria that you devise at the outset and will warn you that this site does not meet all of those criteria and therefore you can leave the site if you don't want to participate in the standard that they have, or you can let them know you don't agree with their standard and negotiate with them to change that policy as they deal with you.

But I think that should be a part of the opportunity not only of each consumer but each business to negotiate as a part of their doing business with you. But when they take that to the next step of taking that information beyond their own usage of it because, after all, the transaction that took place in the past between you and them is information that both you and they share in ownership, but if they even attempt to turn around and sell that to somebody else or give it to somebody else for whatever reason, I think

you need to have the opportunity to avoid that if you don't want to.

Mr. COX. Can I ask you to comment just briefly on the other part of that question, which is whether it is possible to use property rights as the basis for enforcing this regime of privacy protection and information sharing and apply it across all technologies, pen and ink, typewriter, telephone, U.S. mail, the Internet, whatever it is going to be; we write a law that says you have these protections, you have these rights, businesses also have rights and ways to conduct themselves, they are all clear in advance and aren't dependent upon the Internet?

Mr. GOODLATTE. Well, framing it as a property right, I think we have laws that do that to a certain extent today, but in limited areas like intellectual property and so on. Whether you can take that beyond that is a good thinking tool, I guess, as we move forward to address this. But it would be, I think, a major change in policy to try to write every use of every piece of information about anybody that cannot be known; there are lots of things we pick up by looking around this room.

Mr. COX. To the contrary, what I would have in mind is simply by clarifying that people can do whatever they want, you would have the maximum freedom to exchange information, but also individuals would have the maximum opportunity if they chose not to participate in that regime to pick something else.

Mr. GOODLATTE. I think that is the direction we are headed in an opt-out policy here.

Mr. COX. Can you extend that to life on the planet as opposed to just the Internet?

Mr. GOODLATTE. Well, we I think should certainly consider that as we move forward, if it is necessary and appropriate, to make sure that we are not singling out the Internet.

Mr. COX. I think if we could do that, that would be ideal, because I worry about law, however well intended, will end up discriminating against the Internet. We need to recognize that some of this transcends the technology and a lot of these things have been going on for an awfully long time.

Mr. GOODLATTE. We also have some laws in those other areas that in a new technology we need to make sure that those same protections exist there. I think our objective is the same, but also important is how we achieve it——

Mr. COX. Thank you, Mr. Chairman.

Mr. TAUZIN. The Chair recognizes Mr. Sawyer for a round of questions.

Mr. SAWYER. Thank you, Mr. Chairman. I am grateful for the work that both of the gentlemen from Virginia have done, not only within this Congress but internationally. I think the work that you have done internationally may be even more important than the work that has taken place here, as important as it may have been.

I was interested in your tailor analogy. My tailor has gone one step beyond yours. He has been able to project trend lines. I came in when I was in the legislature at 38 and then when I was mayor it was 40, and now as a Member of Congress it is 42. I am stunned by his ability to anticipate such things.

Mr. TAUZIN. He has an inflated view of your potential.

Mr. SAWYER. I was out of the room for a moment.

Am I correct in hearing the tail end of your comment to the gentleman from California, you believe that there ought to be a distinction between information gathered for the internal use of a vendor of a service and that which is subsequently offered for sale for profit to others?

Mr. GOODLATTE. I think that there needs to be a standard set that allows people to know if that information is going to be used for other purposes to give them the opportunity to opt out. That is one of the things that Congressman Boucher outlined in potential legislation that I think would promote the Internet, at the same time make sure that consumers are aware of some of the risk and misuse of their information.

Mr. SAWYER. Might that be an important point of distinction between opt-out and opt-in?

Mr. GOODLATTE. It is the opportunity to find out whether the information is going to be used for those purposes and choose not to do business with that company or have the company agree that in dealing with you they will not use the information for that purpose.

Mr. SAWYER. Let me touch on the subject that you and Mr. Boucher talked about in terms of the work which has been done with the European Union. Clearly that is only one arena where this kind of problem will arise in a global market. To what degree do you believe this has served as a template for broader negotiations, and how would you propose to go about doing it?

Mr. GOODLATTE. We have such widely divergent approaches to consumer privacy on the Internet that it only works in the intermediate term, if you will.

Mr. SAWYER. You are rather answering my second question.

Mr. GOODLATTE. Let me say——

Mr. SAWYER. There are huge cultural differences between the United States and Europe in terms of their government-business relationship.

Mr. GOODLATTE. There are, and the Internet is probably the greatest challenge to the sovereignty of states and nations to insist on a particular format or standard. I think we need to continue to work with parts of the world that have taken the lead in addressing this issue, like the European Union, with whom we may have substantial disagreement, and attempt to forge a workable solution to that, and also show more leadership in the United States as we continue to evolve this policy so that then as other countries in the world begin to address this, we can have some influence over that process. Again, we will have the same problem with 150 nations around the world as we do with 50 States in the United States attempting to have different privacy policies.

Mr. SAWYER. Or 18 members of the European Union. I yield back the balance of my time.

Mr. TAUZIN. I thank the gentleman. The gentleman, Mr. Luther, is recognized.

Mr. LUTHER. Mr. Chairman, thank you. I will pass.

Mr. TAUZIN. Ms. McCarthy.

Ms. MCCARTHY. I thank both gentlemen from Virginia for their efforts to raise and resolve this very important issue; and, Mr.

Chairman, I would like to reserve my questions for the panelists who are coming.

Mr. TAUZIN. Thank you. Mr. Green from Texas.

Mr. GREEN. Thank you, Mr. Chairman. I have one question that I would like to ask our colleague. I know that you mentioned beneficial uses earlier and data collection and I want to echo your comments. I think we in Congress must be careful not to restrict legitimate business practices.

One of the concerns that I have on data collection, do you believe that Congress should prevent third parties from trying to collect an individual's anonymous web site visits with that individual's personal information? Now we are hearing new technology like this being developed every day. One time it was cookies, you didn't accept that, but now there is other technology that the individual user may not know. Again, it is hard to write laws to stop this type of practice when technology can change from day to day and week to week. I would appreciate a comment on third parties tracking someone who may not have a business relationship with that entity.

Mr. GOODLATTE. I think that is a very great concern and we have in our Constitution protections against governments doing that in our Fourth Amendment, and we certainly should have protections against other individuals who are not engaged in a transaction with you using some technological device to track your activities and gather information about you without your knowledge or approval. I think that is a serious problem.

I think quite frankly that some existing laws and regulations enforced by the FTC give some protection in that area, but we need to continue to look at that. We also need to have the kind of spotlight on that activity that has, I think, been effective thus far in pointing out some entities that have stepped over the line on the Internet, and there has been an outcry, and if they are a reputable business they have backed away from some of these things. That is good and important.

So in addition to disclosure to individuals, we also have to have prohibitions in any law that we write that say if you are gathering information about somebody without their knowledge and not disclosing that to them, that there is a consequence to doing that.

Mr. TAUZIN. I thank the gentleman. The Chair again wishes to thank our friend for his patience and again we pledge to work with him in the next Congress where we can continue this dialog and eventually a resolution on some of these issues.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. TAUZIN. We welcome our second panel. I want to preface the second panel with an explanation that the second panel will discuss with us findings of several reports, the Horn report, the Lieberman report and the recent GAO report done at the request of Mr. Armey and myself insofar as it covers the Federal web sites and the status of the Federal web sites.

In prefacing this panel, I want to read the results of that GAO report in brief. As of July 2000, all of the 65 web sites in our survey conducted by GAO, collected personal identifying information from their visitors. 85 percent of the sites posted a privacy notice. That means 15 percent did not. The majority of these Federal sites,

69 percent, also met the FTC's criteria for notice, which implies that 31 percent did not. However, a much smaller number of sites implemented the three remaining principles of the FTC: Choice, 45 percent; access, 17 percent; and security, 23 percent. Few of the Federal sites, 3 percent, implemented elements of all four of the FTC's fair information principles. Three percent implemented elements of all four of the FTC's fair information principles. Finally, a small number of sites, 22 percent, disclosed that they may allow third party cookies. Fourteen percent actually allowed their placement. That is 14 percent of the sites surveyed by GAO indicated that they allowed placement of cookies on the Federal web sites.

In fact, we learned in the news today that the White House itself discovered that it permitted the collection of information through a cookie system and has ordered it to be dismantled. Where is that notice? I want to refer to it so that everybody can see that this is a real problem. This is a story on the web today, White House on cookies, dah. Cookie dough, I guess. After being chastised by watchdog groups, the White House has issued an order to all Federal departments and agencies, no more cookies. The White House was embarrassed last week by the revelation that it used cookies, bits of consumer code, that track and record users' movement across web sites, on some of its web sites, violating its own privacy policies, and possibly violating Federal privacy laws. Check it out on the web entitled White House on cookies, dough, Wired News report.

I am pleased to welcome Linda Koontz, Director, Information Management Issues, U.S. General Accounting Office, Ms. Sally Katzen, Deputy Director for Management, OMB; and Mr. Roger Baker, Chief Information Officer, Department of Commerce, who chairs a privacy subcommittee of the Chief Information Officers Council.

We welcome our first witness, Linda Koontz. Remember, your written statements are a part of our record. Please summarize your comments and then open yourself up to a dialog with us on some of the issues that we have discussed today.

Let me thank the GAO on behalf of Mr. Armey and myself and this subcommittee for conducting the survey. That information combined with the Lieberman and Horn reports is again the basis of this panel's discussion. We will begin with Linda Koontz.

STATEMENTS OF LINDA D. KOONTZ, DIRECTOR, INFORMATION MANAGEMENT ISSUES, U.S. GENERAL ACCOUNTING OFFICE; SALLY KATZEN, DEPUTY DIRECTOR FOR MANAGEMENT, OFFICE OF MANAGEMENT AND BUDGET; AND ROGER W. BAKER, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF COMMERCE

Ms. KOONTZ. Mr. Chairman, thank you for inviting us to discuss online privacy, a subject which has emerged as one of the key and most contentious issues surrounding evolution of the Internet. My testimony today will discuss the findings in our recent report on Internet privacy, which is based on the survey of Federal web sites that we conducted at your request in July 2000.

Specifically, you asked us to determine how Federal web sites would fare when measured against the FTC's fair information prin-

ciples for commercial web sites. These principles are: Notice. Data collectors must disclose their information practices before collecting personal information from consumers.

Choice. Consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those which the information was provided.

Access. Consumers should be able to view and contest the accuracy and completeness of data collected about them.

And security. Data collectors must take reasonable steps to ensure that information collected from consumers is both accurate and protected from unauthorized use.

Using the methodology that the FTC developed to evaluate commercial web site privacy disclosures, we analyzed a sample of 65 Federal web sites to determine whether they collected personal information such as name, address, e-mail; and if so, whether the sites included disclosures to indicate that they met the fair information principles. We did not try to determine whether the web sites actually followed their stated policies.

I should note that Federal agencies are not required to follow FTC's fair information principles, but instead are subject to the requirements of law such as the Privacy Act and guidance issued by the Office of Management and Budget. In addition, FTC staff expressed concern about our use of the methodology stating that there are fundamental differences between Federal and commercial web sites which in their view make the methodology inappropriate for use in evaluating Federal web site privacy policies.

You have already summarized very accurately what our findings were in this report, so I will conclude my statement here and I will be happy to answer any questions that you have at the end of the panel.

[The prepared statement of Linda D. Koontz follows:]

PREPARED STATEMENT OF LINDA D. KOONTZ, DIRECTOR, INFORMATION MANAGEMENT ISSUES, GAO

Mr. Chairman and Members of the Subcommittee: Thank you for inviting us to discuss the privacy policies of selected federal web sites and their conformity with the Federal Trade Commission's four fair information principles—Notice, Choice, Access, and Security. After providing brief background information including an overview of the laws and guidance governing on-line privacy of federal web sites, my testimony today will discuss the findings in our recent report on Internet privacy which is based on the review we conducted at your request in July and August 2000.[1]

As you know, on-line privacy has emerged as one of the key—and most contentious—issues surrounding the continued evolution of the Internet. The World Wide Web requires the collection of certain data from individuals who visit web sites—such as Internet address—in order for the site to operate properly. However, collection of even this most basic data can be controversial because of the public's apprehension about what information is collected and how it could be used.

You asked us to determine how federal web sites would fare when measured against FTC's fair information principles for commercial web sites. In applying FTC's methodology, we analyzed a sample of 65 federal web sites to determine whether they collected personal identifying information, and if so, whether the sites included disclosures to indicate that they met the fair information principles of Notice, Choice, Access, and Security. We also determined the extent to which these

[1] *Internet Privacy: Comparison of Federal Agency Practices With FTC's Fair Information Principles* (GAO/AIMD-00-296R).

sites allowed the placement of third-party cookies [2] and disclosed to individuals that they may allow the placement of these cookies. We did not, however, verify whether the web sites follow their stated privacy policies.

I should note that FTC staff expressed concern about this use of their methodology, stating that there are fundamental differences between federal and commercial web sites which, in their view, make FTC's methodology inappropriate for use in evaluating federal web site privacy policies. For example, an agency's failure to provide for Access or Choice on its privacy policy may reflect the needs of law enforcement or the dictates of the Privacy Act or other federal statutes that do not apply to sites collecting information for commercial purposes.

As of July 2000, all of the 65 web sites in our survey collected personal identifying information [3] from their visitors; 85 percent of the sites also posted a privacy notice. A majority of these federal sites (69 percent) met FTC's criteria for Notice. However, we found that a much smaller number of sites implemented the three remaining principles—Choice (45 percent), Access (17 percent), and Security (23 percent). Few of the federal sites—3 percent—implemented elements of all four of FTC's fair information principles. Finally, a small number of sites (22 percent) disclosed that they may allow third-party cookies; 14 percent actually allowed their placement.

BACKGROUND

Concerned about the capacity of the on-line industry to collect, store, and analyze vast amounts of data about consumers visiting commercial web sites, the FTC reported in May 2000 on its most recent privacy survey of commercial web sites. The survey's objective was to assess the on-line industry's progress in implementing four fair information principles which FTC believes are widely accepted.

- *Notice.* Data collectors must disclose their information practices before collecting personal information from consumers.
- *Choice.* Consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided.
- *Access.* Consumers should be able to view and contest the accuracy and completeness of data collected about them.
- *Security.* Data collectors must take reasonable steps to ensure that information collected from consumers is accurate and secure from unauthorized use.

In addition, the survey looked at the use of third-party cookies by commercial web sites. Although FTC noted improvement over previous surveys, it nonetheless concluded that the on-line industry's self-regulatory initiatives were falling short. As a result, a majority of the FTC commissioners, based on a 3 to 2 vote, recommended legislation to require commercial web sites not already covered by the Children's Online Privacy Protection Act (COPPA) [4] to implement the four fair information principles.

While the FTC's fair information principles address Internet privacy issues in the commercial sector, federal web sites are governed by specific laws designed to protect individuals' privacy when agencies collect personal information. The Privacy Act of 1974 is the primary law regulating the federal collection and maintenance of personal information maintained in a federal agency's systems of records.[5] The act provides, for example, that (1) agencies cannot disclose such records without the consent of the individual except as authorized by law, (2) under certain conditions, individuals can gain access to their own records and request corrections, and (3) agencies must protect records against disclosure and loss. While these requirements are generally consistent with FTC's fair information principles, the act's specific provisions limit the application of these principles to the federal government. Specifically, the Privacy Act applies these principles only to information maintained in a system of records and contains exceptions that allow, under various circumstances, the dis-

---

[2] A cookie is a small text file placed on a consumer's computer hard drive by a web server. The cookie transmits information back to the server that placed it, and, in general, can be read only by that server. A third-party cookie is placed on a consumer's computer hard drive by a web server other than the one being visited by the consumer—often without the consumer's knowledge.

[3] Information used to identify or locate an individual, e.g., name, address, e-mail address, credit card number, Social Security number, etc.

[4] 15 U.S.C. 6501 et seq. The provisions of COPPA govern the collection of information from children under the age of 13 at web sites, or portions of web sites, directed to children or which have actual knowledge that a user from which they seek personal information is a child under 13 years old. These provisions took effect April 21, 2000.

[5] A system of records means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

closure and use of information without the consent of the individual. On June 2, 1999, OMB provided additional guidance on Internet privacy issues in Memorandum M-99-18, directing agencies to post on principal federal web sites privacy policies that disclose what information is collected, why it is collected, and how it will be used. In a separate report issued earlier,[6] we evaluated selected federal web sites' privacy policies against certain aspects of applicable laws and guidance, and included a comparison of the Fair Information Principles and the Privacy Act. We also have ongoing work—which we intend to report on later this year—addressing in greater depth the use of cookies on federal web sites.

SCOPE AND METHODOLOGY

As you requested, we used FTC's methodology to provide a snapshot of the privacy practices of two groups of web sites operated by executive branch agencies compared to the fair information principles. We reviewed a total of 65 sites during July 2000. One group consisted of web sites operated by 32 high-impact agencies, which handle the majority of the government's contact with the public.[7] A second group consisted of web sites randomly selected from the General Services Administration's (GSA) government domain registration database.[8] This group consisted mostly of web sites operated by small agencies, commissions, or programs. Finally, at your request, we assessed the FTC web site itself. (For the purpose of our analysis, the FTC site was added to the sites operated by the 32 high-impact agencies.)

In conducting our survey we generally followed the FTC methodology, including the selection of similar groups of web sites and the use of its data-collection forms and analytical techniques. We requested—and received—training from FTC similar to that provided to staff who collected and analyzed its survey information. Our staff underwent 2 half-days of training by FTC staff on its methodology and content analysis procedures for commercial web sites.

We visited the web sites in our samples from July 12 through July 21, 2000. We reviewed the web pages within the site—for up to a time limit of 15 minutes—to determine whether the site (1) collected any personal or personal identifying information, (2) posted a privacy statement, information practice statement, or disclosure notice, (3) provided individual access to and choice regarding use of the information, and (4) provided security over the information. We also looked for the placement and disclosure of third-party cookies.

FEDERAL WEB SITES SURVEYED COLLECT PERSONAL DATA BUT VARY IN DEGREE OF CONFORMITY TO FTC PRINCIPLES

We found that all of the 65 web sites surveyed collected personal identifying information from their visitors. Most sites—85 percent—posted a privacy notice. However, they varied in the extent to which they provided Notice to consumers, allowed consumers Choice and Access regarding their information, disclosed that they provided Security for the information provided, and allowed and disclosed the placement of third-party cookies.

Using the same scoring methodology that FTC used for commercial sites, our survey showed that only 6 percent of the federal high-impact agencies and 3 percent of the randomly sampled sites federal web sites implemented, at least in part, each of the four fair information principles. The following explains how we scored the sites to determine conformance with each principle and describes how the federal web sites in our survey fared in conforming with each of the principles.

Notice

The Notice principle is a prerequisite to implementing the other principles. We concluded that a site provided Notice if it met all of the following criteria: (1) posted a privacy policy, (2) stated anything about what specific personal information it collects, (3) stated anything about how the site may use personal information internally, and (4) stated anything about whether it discloses personal information to third parties. Our survey showed that 69 percent of all sites visited met FTC's criteria for Notice.

Choice

Under the Choice principle, web sites collecting personal identifying information must afford consumers an opportunity to consent to secondary uses of their personal

---

[6] *Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy* (GAO/GGD-00-191, September 5, 2000.

[7] According to the National Partnership for Reinventing Government, these agencies handle 90 percent of the federal government's contact with the public.

[8] Our random sample was not large enough to project to the universe of federal web sites.

information, such as the placement of consumers' names on a list for marketing additional products or the transfer of personal information to entities other than the data collector. Consistent with such consumer concerns, FTC's survey included questions about whether sites provided choice with respect to their internal use of personal information to send communications back to consumers (other than those related to processing an order) and whether they provided choice with respect to their disclosure of personal identifying information to other entities, defined as third-party choice.

We concluded that a site provided Choice if both internal choice with respect to at least one type of communication with the consumer and third-party choice with respect to at least one type of information were given to individuals. Our survey showed that 45 percent of all sites met FTC's criteria for Choice.

Access

Access refers to an individual's ability both to access data about himself or herself—to view the data in the web site's files—and to contest that data's accuracy and completeness. Access is essential to improving the accuracy of data collected, which benefits both data collectors who rely on such data and consumers who might otherwise be harmed by adverse decisions based on incorrect data. FTC's survey asked three questions about Access: whether the site stated that it allows consumers to (1) review at least some personal information about them, (2) have inaccuracies in at least some personal information about themselves corrected, and (3) have at least some personal information deleted.

We concluded that a site provided Access if it provided any one of these disclosures. Our survey showed that 17 percent of all sites met the FTC criteria for Access.

Security

Security refers to the protection of personal information against unauthorized access, use, or disclosure, and against loss or destruction. Security involves both management and technical measures to provide such protections. FTC's survey asked whether sites disclose that they (1) take any steps to provide security, and if so, whether they (2) take any steps to provide security for information during transmission, or (3) take any steps to provide security for information after receipt.

We concluded that a site provided Security if it made any disclosure regarding security.

Our survey showed that 23 percent of all sites met FTC's criteria for Security.

Third-Party Cookies

FTC defines a third-party cookie as a cookie placed on a consumer's computer by any domain other than the site being surveyed. Typically, in the commercial environment, the third party is an on-line marketing organization or an on-line service that tracks and tabulates web-site traffic. However, some federal web sites also allow placement of third-party cookies. Our survey showed that 22 percent of all sites disclosed that they may allow third-party cookies and 14 percent allowed their placement.

Mr. Chairman, this concludes my statement. I would be happy to respond to any questions that you or other members of the Subcommittee may have at this time.

Contact and Acknowledgements

For information about this testimony, please contact Linda D. Koontz at (202) 512-6240 or by e-mail at koontzl.aimd@gao.gov. Individuals making key contributors to this testimony include Ronald B. Bageant, Scott A. Binder, Mirko J. Dolak, Michael P. Fruitman, Pamlutricia Greenleaf, William N. Isrin, Michael W. Jarvis, Kenneth A. Johnson, Glenn R. Nichols, David F. Plocher, Jamie M. Pressman, and Warren Smith.

Mr. TAUZIN. Thank you. We will now hear from Ms. Katzen, Deputy Director of the Office of Management and Budget.

STATEMENT OF SALLY KATZEN

Ms. KATZEN. Thank you, Mr. Chairman. I congratulate you on having this hearing on this very important issue and I appreciate your inviting me to testify on privacy on government web sites.

As the members of this panel know, protecting the privacy of American citizens is a very high priority for this administration. We have worked hard to ensure that fundamental privacy protec-

tions are properly safeguarded as our government, indeed society at large, moves into the Digital Age. Nowhere is this task more important than in the Federal Government's obligation to continue to protect the privacy and confidentiality of the personal information that it maintains and to protect the privacy of individuals in their interactions with the government over the Internet.

Today the Federal Government is increasingly becoming an electronic government full of new opportunities to provide information easily and quickly to the public. But as everyone has noted today, we must be vigilant to ensure that personal privacy protections remain constant or improved in the process of this transformation. I am proud to be able to testify here today about the success of this administration in meeting this challenge and in taking major steps to boost the level of privacy afforded to American citizens when they access the government electronically. Without doubt we have more to learn as the government in this time of rapid change in technology and information flows; all organizations do, no matter their size. But I am confident that we are achieving significant progress and clearly heading in the right direction.

Now to understand the GAO reports on privacy practices, it is important to put them in proper context and history, and I would begin with the Privacy Act of 1974, as you did, Mr. Chairman, in your opening comments. For over a quarter of a century, it has afforded Americans strong legal protections for personal information stored in government systems of records, no matter whether they exist in papers or in electronic form. This is not voluntary. This is mandatory. It is the law of the land. These protections include notice, prohibitions on the unauthorized release of personal information, ability to access your records and change errors that may appear, and security safeguards as well.

I would just note that Representative Horn's grades on security, which you have mentioned a couple of times now, was the subject of another hearing that I participated in, and there is grave concern about the methodology that he used and the grades that he gave. That is not an uncontested system that he established. We believe that the security of the government web sites is indeed very strong and will remain so.

Now, while the Privacy Act provides the bedrock privacy protections for Americans in their relationship with government, the changes in technologies have produced a different world than existed in 1974. And as has been noted, to keep current with meaningful privacy protections, the Office of Management and Budget has augmented the Privacy Act provisions with policy guidance. The agencies' response to that guidance has been outstanding.

For example, in April 1999 a study revealed that just over a third of the Federal agencies had privacy policies posted on their main web pages. In June, 2 months later, OMB Director Jack Lew issued a memo to all agency heads directing them to post clearly written privacy policies on their web sites by September 1, 1999. Director Lew, echoing the sentiments of Mr. Boucher, said we cannot realize the full potential of the web until people are confident we protect their privacy when they visit our sites.

The message was received by the Federal agencies, and the GAO confirmed this result, in what you have referred to as the

Lieberman study. This was a study conducted in April 2000 and released on September 5, 2000. I call it the first GAO study.

Now the chairman suggested that GAO found the privacy policies to be wanting. In fact, this study found that 69 of 70 principal agency web sites had a privacy policy posted on their sites and all 70 did within days of release of that report. Equally impressive, the GAO identified 2,692 major points of entry to six Federal Government agencies. These are sites where the largest number of people interact with the Federal Government. And of the sites they reviewed, GAO found only 9 lacked privacy policies. This record is impressive, and I believe is an accurate picture of Federal privacy policies online.

In view of this, it is, I think, fair to ask why GAO reached the conclusions that it did about Federal agencies' compliance with the fair information practices written by the Federal Trade Commission for commercial web sites, which is the second GAO report. The answer, I believe, has more to do with the questions that were asked than the practices reported.

Specifically, the administration pointed out to GAO staff in the course of that study that the study was misdirected and the answers to the study's questions would likely be misleading. GAO has also reported that the FTC independently expressed concern that its methodology was "inappropriate for use in evaluating Federal web site privacy policies."

Why is this, you might ask. Let me explain. A central premise of the study that was done was that the FTC formulation of fair information practices for commercial sites could appropriately be used to measure the privacy protections of government web sites. We think it cannot because the FTC practices were designed for the private sector, where the Privacy Act and OMB guidance do not apply. This is a very important distinction between commercial companies and Federal agencies.

The fact that there is no law establishing privacy protection for individuals in the commercial arena led the FTC to stress the need for a statement about policies, because absent a statement, the companies cannot be held accountable. That is, you must have a representation of what you will do and not do to be enforceable by the FTC. Government web sites by contrast do not have to make any representations to be held accountable. The Privacy Act establishes in the most public way possible the standards to which citizens can hold Federal agencies accountable and exactly how they can hold those agencies accountable.

Thus, the test of whether a Federal web site provides privacy protection is not whether it includes a statement that makes it comparable with commercial practices, but rather whether good privacy protections are in fact in place. And the first GAO report, the Lieberman report, showed that the major Federal web sites inform citizens of how their data are used at their web sites, and I would refer you specifically to page 25 of that report, which takes each of the fair information practices and documents that they are covered either by OMB policy or by the Privacy Act. It is against that which the first study measured the Federal web sites and it is against that standard that they did as well as they have done.

Now, we recognize that in this Information Age it is critical that the Federal Government continue to use technology to keep the public informed and provide services to the public and stay on the cutting edge of technology. The launch on September 22 of firstgov.gov was a major step to enable us to continue providing information and resources to the American people. In this and many other ways, the need for privacy protection online and the need for public confidence in the Federal Government's online privacy standards is expected to only increase in the years ahead. It would be most unfortunate if any misleading conclusions as to the state of privacy on Federal web sites interfered with our common goal of achieving electronic government without full participation of the public. I thank you for holding this hearing and giving me an opportunity to testify.

[The prepared statement of Sally Katzen follows:]

PREPARED STATEMENT OF SALLY KATZEN, DEPUTY DIRECTOR FOR MANAGEMENT, OFFICE OF MANAGEMENT AND BUDGET

Mr. Chairman and members of the Committee, I thank you for inviting me here today to discuss the important topic of privacy on government web-sites. As you know, protecting the privacy of American citizens is a very high priority for this Administration. We have worked hard to ensure that fundamental privacy protections are properly safeguarded as our government, and society at large, moves into the Digital Age. Nowhere is this task more important than in the federal government's obligation to continue to protect the privacy and confidentiality of the personal information that it maintains, and, now, to protect the privacy of individuals in their interactions with the government over the Internet.

Today the federal government is increasingly becoming an electronic government, full of new opportunities to provide services and information to the public quickly, easily, and when the public wants them. But as you, Mr. Chairman, and so many others here have noted, we must be vigilant to ensure that personal privacy protections remain constant or are improved in the process of this transformation. I am proud to be able to testify today about the success of this Administration in meeting this challenge—in taking major steps to boost the level of privacy afforded to American citizens when they access the government electronically. Without doubt, we have more to learn as a government. In this time of revolutionary changes in technology and information flows, all organizations do, no matter their size. But I am confident that we have achieved significant progress, and are clearly heading in the right direction in this critical area.

To understand the recent General Accounting Office reports on the privacy practices of federal agencies on-line, it is helpful to put them in their proper context and history. First, there is the Privacy Act of 1974, which for over a quarter of a century has afforded Americans strong legal protections for personal information stored in government systems of records—no matter if they exist in paper or electronic form. These protections include notice, prohibitions on the unauthorized release of your personal information, the ability to access your own records, the ability to change errors in your records, and security safeguards, among other protections.

While this Act provides the bedrock privacy protections for Americans in their relations with the government, changes in technology—most notably the dramatic increase in Internet-access to the government—have produced a different world than existed in 1974. To keep current with meaningful privacy protections, the Office of Management and Budget has augmented the Privacy Act provisions with policy guidance, and the agencies' response, I believe, has been outstanding.

For example, in April 1999, a study revealed that just over one-third of federal agencies had privacy policies clearly posted on their main web pages. In June 1999, OMB Director Jacob J. Lew issued a memorandum to all agency heads directing them to post clearly labeled and clearly written privacy policies on their web-sites by September 1, 1999. Director Lew told agencies then, "We cannot realize the full potential of the web until people are confident we protect their privacy when they visit our sites."

The message was received by federal agencies. The General Accounting Office confirmed this result in a review conducted in April of 2000 and released on September 5, 2000 ("the first GAO report"). This GAO study found that 69 of 70 principal agen-

cy web-sites had a privacy policy posted on their sites—and all 70 did within days of the report's release. Even more impressive, the GAO identified 2,692 major Web-site points of entry to six federal government agencies. These are sites where the largest number of citizens interact with the Federal government. Of the sites they reviewed, GAO found that only nine lacked privacy policies.

This record of progress is impressive, and, I believe, it is an accurate picture of the state of Federal privacy policies on-line. It is a story of working rapidly, across the expansive federal government and across thousands of web-pages, to ensure that citizens' privacy is protected when they choose to visit the federal government over the Internet.

As part of our continuing efforts in the area, OMB Director Lew issued another memorandum this June to further enhance privacy protections on federal web-sites. Director Lew directed that cookies will not be used on Federal web-sites, except under very limited conditions. He also made clear, as a matter of Federal policy, that agencies are to comply with the standards of the Children's Online Privacy Protection Act, even though Congress did not include the Federal Government within the scope of that law. In addition, he directed each agency to describe its privacy practices and the steps taken to comply with Administration privacy policies in its budget submissions this fall to OMB. In this way, good privacy protection gets built into the budget process, emphasizing to everyone in the Government the importance of assuring citizen privacy.

These efforts to boost privacy safeguards have extended to areas beyond the federal government's practices on-line, as the Administration has supported strengthening citizens' legal privacy protections in such areas as medical information, financial records, genetic information, and Social Security numbers. These are categories of sensitive data that require protection in both the public and private sectors.

In light of this record of significant achievement, you may well ask why GAO reached the conclusions that it did about the Federal agencies' compliance with the fair information practices written by the Federal Trade Commission for commercial web-sites (the second GAO report). The answer, I believe, has more to do with the questions that were asked than the practices reported. Specifically, the Administration pointed out to GAO staff in the course of that study that the study was misdirected and that the answers to the study's questions would be misleading. GAO also has reported that the FTC independently expressed concern that its methodology was "inappropriate for use in evaluating federal web site privacy policies."

The central premise of this particular study was apparently that the FTC formulation of fair information practices for commercial web-sites could appropriately be used to measure the privacy protections of government web-sites. We think it cannot. As noted, the FTC practices were designed for the private sector, where the Privacy Act and OMB policy do not apply. This is an important difference between commercial companies and federal agencies, even though both the government and businesses often use web-sites for the same core purposes: to provide information to consumers and to provide services to the public. The fact that there is no law establishing privacy protections for individuals in the commercial arena led the FTC to stress the need for those web-sites to make clear statements as to their privacy protections. The FTC does the same—that is, require clear statements—about commercial web-site policies with respect to access and security practices. It is through these statements that these companies can be held accountable.

Government web-sites, by contrast, do not have to make any representations to be held accountable. The Privacy Act establishes—in the most public way possible—the standards to which citizens can hold federal agencies accountable and exactly how they can hold agencies accountable. Thus, the test of whether a federal web-site provides privacy protection is not whether it includes statements that make it compatible with commercial practices, but rather whether good privacy protections are in place. The first GAO report confirmed that they are: When government web-sites were measured against government privacy standards, the results were impressive.

In this Information Age, it is critical that the federal government continues to use technology to keep the public informed and to provide services for the public. The launch of the Federal government's FirstGov web-site on September 22 was a major step to enable easy access to government resources on-line. In this and many other ways, the need for privacy protection on-line—and the need for public confidence in the Federal government's on-line privacy standards—is expected to only increase in the years ahead. It would be most unfortunate if any misleading conclusions as to the state of privacy on federal web-sites interfered with our common goal of achieving an electronic government with full public participation.

As I said before, the federal government can, and should, continue to improve in its protection of the privacy of those individuals who access government web-sites.

The first GAO report pointed out that we could do a better job of posting privacy policies at specific Federal web pages where a substantial amount of personal information is collected. That report also made recommendations about how OMB might provide clearer guidance to agencies, and we are working with the Federal CIO Council to respond to those recommendations. Beyond that, I think that we will learn much from the privacy materials included with the agency FY 2002 budget submissions to OMB. At the same time, I would again emphasize that the Administration's record on privacy protection in this area is strong, with a resolute commitment to safeguard personal privacy.

I thank you, Mr. Chairman, for holding this hearing today and for inviting me to testify. I look forward to continuing to work with you and the other members of this committee in making the federal government a model of good privacy practices.

Mr. TAUZIN. Mr. Roger Baker, Chief Information Officer of the U.S. Department of Commerce.

STATEMENT OF ROGER W. BAKER

Mr. BAKER. Thank you, Mr. Chairman. Thank you for inviting me to testify before the committee today. I am testifying as the Chairman of the Chief Information Officers Council Subcommittee on Privacy. However, as a practicing Chief Information Officer for an agency, my testimony also includes some anecdotal information from the Department of Commerce.

I would like to make three points: First, privacy is an important issue for Chief Information Officers throughout the government and the Federal CIO Council. Second, our fundamental guidance on privacy inside the Federal Government comes from the Privacy Act, other applicable Federal laws and OMB policy, and that in the past 2 years we have made substantial progress in both the quality and quantity of the privacy policies posted on Federal web sites and significantly raised the awareness of privacy issues within the Federal information technology community.

First, privacy is an important issue for the Federal CIO Council. By creating a Subcommittee on Privacy, the Federal CIO Council signaled to all Federal information technology workers that protecting the personal privacy of the public is one of the key issues facing us today.

The American public provides government agencies with the most sensitive of personal information. It is our duty as Federal employees to protect this information to the best of our ability. This means that our information systems must be secure from intrusion and the systems must work in accordance with applicable Federal laws. The CIO Council keeps this issue at the forefront of IT discussions by making it a key part of our annual strategic plan, by including privacy in the conferences we support and the speeches we make, and providing agencies with best practices or examples of how to improve the privacy and security aspects of their information systems.

There are many examples of these best practices for privacy and security on the CIO Council web site at www.cio.gov.

I would like to submit with my testimony the privacy impact assessment best practices developed by the IRS and recommended by the Security, Privacy and Critical Infrastructure Committee for use by all Federal agencies. The CIO continues to work with OMB and others to identify further best practices and other useful guidance to be provided to agencies to help them in their efforts to protect personal privacy on the Internet and other information systems.

Second, our fundamental guidance on privacy inside the Federal Government comes from the Privacy Act and other applicable Federal laws. Federal information systems, including Internet web site servers, are subject to the provisions of the Privacy Act. OMB has issued policy directives regarding privacy protections on Federal web sites that focus on a number of issues. First, that all major entry points and all points where personal information is collected should have easily accessible privacy policies posted; second, that those privacy policies be clearly written and reflect actual agency policy with regard to the collected information; third, those policies are in accordance with the Privacy Act and other laws and guidance that may be applicable to specific agencies; and, fourth, that there is a presumption against the use of technologies that allow the tracking of activities over time and across different web sites; for example, persistent cookies as differentiated from session cookies, unless a high level of approval is obtained.

The CIO Council has worked closely with OMB to support the development and implementation of these directives. As a result of an example of this work, I would like to submit the privacy policy posted on the main page of the Census Bureau's Internet web site, www.census.gov. While admittedly somewhat long, this privacy policy clearly conveys the types of information that may be collected, how used and the specific legal protections provided that information. I used the Census privacy policy as an example because it involves both the Privacy Act and Title 13 protections.

Mr. Chairman, I believe the following points were made in the GAO report, but they are so important I will quickly make them again.

Federal records are covered by specific laws that give individuals specific rights and the remedies if their private information is disclosed. These laws apply whether or not a privacy policy is posted on a Federal web site. There are no equivalent laws covering nongovernmental systems. The FTC rules regarding privacy policies for private sector web sites are meant to establish a legal basis under which a private sector web site operator can be held responsible for the protection of private information collected on a web site. Once posted, the privacy policy falls under the jurisdiction of the FTC, which uses existing laws to hold companies to the promises they make to the consumers.

In short, if a private sector web site does not post a privacy policy, there is no ready legal recourse available to an individual whose privacy has been violated. In contrast, the Privacy Act and other laws apply even if a Federal web site does not post a privacy notice. We can and should do a better job of communicating the protections that the Privacy Act and other Federal laws provide users on Federal web sites, but we should continue to use existing Federal laws or guidance in these areas instead of the FTC policies clearly intended to achieve a different purpose.

In the past 2 years we have made substantial progress in both the quantity and quality of privacy policies posted on Federal web sites. In 1999, the secretary of commerce called on private sector web site operators to improve their privacy practices, placing special emphasis on the need for: One, posting privacy policies; and,second, that policies include the fair information practices of

notice, choice, access and security. We quickly recognized that we also needed to make major improvements in our own web site privacy policies, both at the Department of Commerce and throughout the Federal Government. Working with OMB, we raised the profile of the privacy issues with both agency and technical management and made substantial strides in both the quality and quantity of privacy practices posted on Federal web sites. And I won't go through the GAO reports again, since you have that information.

Clearly we made a major improvement, and I believe this is evidenced by the examples from the Census Bureau. The overall qualities of these privacy policies have seen substantial improvement as well.

In closing, I would like to reiterate my main points. Privacy is a very important issue for agency CIOs and the Federal CIO Council. Our fundamental guidance on privacy inside the Federal Government comes from the Privacy Act and other applicable laws and OMB guidance, and in the past 2 years I believe we have made substantial progress in quality and quantity of privacy policies posed on Federal web sites.

Thank you for your time and I look forward to any questions you may have.

[The prepared statement of Roger W. Baker follows:]

PREPARED STATEMENT OF ROGER W. BAKER, CHIEF INFORMATION OFFICER, UNITED STATES DEPARTMENT OF COMMERCE

Mr. Chairman and members of the Committee: Thank you for inviting me to testify before the committee today. I am testifying in my role as the Chairman of the Federal Chief Information Officer's Council subcommittee on Privacy. However, as a practicing CIO, I will also include some anecdotal information from my agency, the Department of Commerce.

In my testimony today, I would like to make three points.

- Privacy is an important issue for agency CIOs and the Federal CIO Council.
- Our fundamental guidance on privacy inside the federal government comes from the Privacy Act, other applicable federal laws, and OMB policy.
- In the past two years, we have made substantial progress in both the quantity and quality of privacy policies posted on federal web sites, and significantly raised the awareness of privacy issues within the federal IT community.

Privacy is an important issue for CIOs and the Federal CIO Council.

By creating a subcommittee on privacy, the Federal CIO Council signaled to all federal information technology workers that protecting the personal privacy of the public is one of the key issues facing us today. The American public provides government agencies with the most sensitive of personal information. It is our duty, as federal employees, to protect this information to the best of our ability. This means that our information systems must be secure from intrusion, and that these systems must work in accordance with applicable federal laws.

The CIO Council keeps this issue at the forefront of IT discussions by making it a key part of our strategic plan, by including privacy in the conferences we support and speeches we make, and by providing agencies with "best practices" to provide them with examples of how to improve the privacy and security aspects of their information systems.

There are many examples of these "best practices" for privacy and security on the CIO council web site at www.cio.gov. I would like to submit with my testimony the PRIVACY IMPACT ASSESSMENT best practice developed by the Internal Revenue Service and recommended by the Security, Privacy, and Critical Infrastructure Committee for use by all federal agencies. The Privacy Impact Assessment best practice provides agencies with a template for evaluating and certifying that an information system has been implemented in accordance with applicable agency policies and federal laws on privacy.

The CIO Council will continue to work with OMB and others to identify further best practices and other useful guidance that can be provided to agencies to help

them in their efforts to protect personal privacy on the Internet and other information systems.

Our fundamental guidance on privacy inside the federal government comes from the Privacy Act and other applicable federal laws.

Federal information systems, including Internet web servers, are subject to the provisions of the Privacy Act. In addition, OMB has issued policy directives regarding privacy protections on federal web sites that focus on a number of issues. **First,** that all major entry points and all points where substantial personal information is collected should have easily accessible privacy policies posted. **Second,** that those privacy policies be clearly written and reflect actual agency policies with regard to the collected information. **Third,** that those policies are in accordance with the Privacy Act and other laws and guidance that may be applicable to specific agencies. And **fourth,** there is a presumption against the use of technologies that allow the tracking of the activities of users over time and across different web sites (for example, persistent cookies) unless high-level approval is obtained. The CIO Council has worked closely with OMB to support the development and implementation of these directives.

As an example of the results of this work, I would like to submit into the record the privacy policy posted on the main page of the Census Bureau's Internet web site, www.census.gov. While somewhat long, this privacy policy clearly conveys the types of information that may be collected, how that information will be used, and the specific legal protections provided that information. I use the Census privacy policy as an example because it involves both the Privacy Act and Title 13 protections.

Mr. Chairman, I believe the following points were made in the GAO report, but they are so important that I will quickly make them again. Federal systems of records are covered by specific laws that give individuals specific rights and remedies if their private information is disclosed. These laws apply whether or not a privacy policy is posted on a federal web site. There are no equivalent laws covering non-governmental systems. The FTC rules regarding privacy policies for private sector web sites are meant to establish a legal basis under which a private sector web site operator can be held responsible for the protection of private information collected on a web site. Once posted, the privacy policy falls under the jurisdiction of the FTC, which uses existing laws to hold companies to the promises they make to consumers.

In short, if a private sector web site does not post a privacy notice, there is no ready legal recourse available to an individual whose privacy has been violated. In contrast, the Privacy Act and other laws apply even if a federal web site does not post a privacy notice.

We can and should do a better job of communicating the protections that the Privacy Act and other federal laws provide users on federal web sites. But I believe we should continue to use existing federal law as our guidance in this area, instead of FTC policies clearly intended to achieve a different purpose.

In the past two years, we have made substantial progress in both the quantity and quality of Privacy Policies posted on federal web sites.

In 1999 the Secretary of Commerce called on private sector web site operators to improve their privacy practices, placing special emphasis on the need for (1) posting privacy policies and (2) policies include the fair information practices of notice, choice, access, and security. We quickly recognized that we, also, needed to make major improvements in our own web site privacy policies, both at Commerce and throughout the federal government. Working with OMB, we raised the profile of the privacy issue with both agency and technical management, and made substantial strides in both the quantity and quality of privacy policies posted on federal web sites. A recent GAO report concluded that 69 out of 70 agency main pages had privacy policies clearly posted. Further, GAO identified 2692 major points of entry to six federal agencies. Of the sites they reviewed, GAO found that only 9 lacked privacy policies. This, clearly, is a major improvement. And, as is evidenced by the example from the Census Bureau, the overall quality of these privacy policies has seen substantial improvement as well.

Closing

Mr. Chairman, in closing I would like to reiterate my main points.

- Privacy is an important issue for agency CIOs and the Federal CIO Council.
- Our fundamental guidance on privacy inside the federal government comes from the Privacy Act, other applicable federal laws, and OMB guidance.

- In the past two years, we have made substantial progress in both the quantity and quality of Privacy Policies posted on federal web sites.

Thank you for your time. I look forward to any questions you may have.

Mr. TAUZIN. Thank you, Mr. Baker. The Chair recognizes himself for 5 minutes. There is another story on the web on Yahoo News that is quite relevant, Ms. Katzen. It is entitled "FTC to Apply Law to Web Sites," and it leads, "Contrary to Federal directive, major government web sites, including the one operated by the White House, are not adhering to a law that requires companies to obtain parental consent before soliciting personal information from children. The web site invites children to submit personal information along with e-mail messages to the President and First Family, and there is no warning that children first get parental consent before sharing this information."

Is the White House violating the Federal law?

Ms. KATZEN. No, it is not. COPPA, the Children's Online Privacy Protection Act, does not apply to the Federal Government.

Mr. TAUZIN. Isn't that wonderful?

Ms. KATZEN. Excuse me, if I may explain the practices, because this is a statement that has been made time and again in the press.

By law we are not covered by COPPA. However, we have taken every step that we can, consistent with our being a unique place, to meet the spirit of COPPA. COPPA was to protect children from marketers who would seek to exploit them——

Mr. TAUZIN. I want to ask you: Does not the June memorandum state that all Federal web sites and contractors when operating on behalf of agencies shall comply with the standards set forth in the Children's Online Privacy Protection Act?

Ms. KATZEN. Yes, but one of the conditions of COPPA is if you are going to get personal information for a one-time contact, you must destroy the record. The Presidential Records Act does not allow us to destroy records.

Mr. TAUZIN. Does not COPPA require the advice to children to get parental consent?

Ms. KATZEN. Yes. And on five different——

Mr. TAUZIN. And is the White House complying with COPPA today?

Ms. KATZEN. It is not required to comply with——

Mr. TAUZIN. Does the memorandum require it to?

Ms. KATZEN. The memorandum says do what we can, and we are working on systems to enable us not to destroy records. The Presidential Records Act, the security that attends the White House, and other considerations make the White House very different from what COPPA was designed to do.

Mr. TAUZIN. I am going to run out of time. I want to go to some other witnesses.

Mr. COX. Mr. Chairman, if you would yield on this point. Having served in the White House Counsel's Office, I am well aware of the Presidential Records Act, which has not been followed by this administration in any case. But why do you need to collect the information from the kids in the first place? Then you would not have a record to destroy.

Ms. KATZEN. Children do not have to provide any information to send a letter to the White House. If you want a response, you need to provide an e-mail address or a regular address. That is the information which COPPA says we would have to destroy if we obtained it from the child in the first instance. It is for that reason that on the White House Home Pages, which are here, it says on at least five occasions, make sure that it is okay with your parents. We cannot respond to your message without your address, but you can write us and tell us what you think without any information from you coming in.

Mr. TAUZIN. Reclaiming my time, does EPA require that? Does EPA advise——

Ms. KATZEN. Yes, and the site you were talking about has been taken down.

Mr. TAUZIN. Taken down today?

Ms. KATZEN. No, it was taken down on Friday.

Mr. TAUZIN. Right before this hearing.

Ms. KATZEN. It was taken down as soon as it was brought to our attention that there was a violation. When we learned——

Mr. TAUZIN. I have to control my time. Let me ask the other witnesses, you keep referring to the fact that Federal agencies don't need to post their privacy policies and say what they are collecting and how they are collecting it and who they are sharing it with because Federal agencies are covered by the Privacy Act. We have information on the Privacy Act. The Privacy Act provides 12 different exceptions, 12 exceptions provided by law for information collected by the Federal Government to be shared with other people. They include, for example, for routine uses defined in the act, to other offices and employees of the agency, to a recipient who has provided the agency with an adequate advance written assurance that the record will be used solely for statistical research. It allows the sharing of private information to persons pursuant to showing of compelling circumstances of health, to Members of Congress, to the Controller General, by an order of court, to a consumer reporting agency, 12 different exceptions by which consumer information can be shared with other people, and Federal agencies only say that we are complying with the Privacy Act.

How do consumers know without getting a lawyer and getting a lawyer to explain what is in fact happening to his private information under this Privacy Act?

Mr. BAKER. I certainly wouldn't want to imply that I don't believe agencies should have privacy policies. I have worked hard to get agencies to have privacy policies.

Mr. TAUZIN. Shouldn't Federal agencies post their privacy policies just like people in the commercial sector so consumers know without getting a lawyer what is going to be shared with whom?

Mr. BAKER. Federal agencies should post a privacy policy which should reflect the Federal law which applies to them, and I certainly as Chief Information Officer would not advise anyone working for me to not comply.

Mr. TAUZIN. You are saying that it is our fault we wrote a law that lets these agencies share information so consumers be damned? Or should the Federal Government—let me pose a question to you as clearly as I can.

If the FTC and, for that matter, Members of Congress are harping on the private sector to do more about informing consumers what information is being collected about them, how it is being shared and to whom it is being sent, should not Federal agencies live by the same standard, particularly where information is being shared with Federal agencies in a nonvoluntary situation?

Ms. KATZEN. They are, and they should be.

Mr. TAUZIN. I am asking Mr. Baker.

Mr. BAKER. I'm sorry?

Mr. TAUZIN. Let me ask it again as carefully as I can. If the FTC is setting up standards by which it is going to judge private sector web sites on the basis of whether or not they adequately inform consumers what information is being gathered and how it is being used and to whom it is being shared so that consumers can be warned, should not the Federal agencies by which consumers and constituents interact with information that is not necessarily voluntarily presented to the government, in many cases mandatorily provided to the government, shouldn't the Federal agencies be under a higher standard to do that, to inform consumers precisely about what information is being gathered, what it is being used for and to whom it is going to be shared with instead of hiding behind a law that has 12 exceptions that the consumer doesn't even know about?

Mr. BAKER. I think Federal agencies should be as clear as they can. Again the Census Bureau example, I believe it is pretty clear about what the protections are. The Privacy Act is there and that is what we have used as our guidance.

Mr. TAUZIN. Ms. Koontz, did the IRS in fact have a cookie on its web site?

Ms. KOONTZ. Using the FTC methodology, we identified a third party cookie in use at the IRS. In fairness to everyone here, the cookie that we identified was one that is placed on the visitors' hard drive when they are in the process of leaving the IRS site. The reason we picked this up——

Mr. TAUZIN. Wait. I want to understand that. We have a Federal policy discouraging—the memorandum discourages cookies on Federal web sites. But there are exceptions and cookies are allowed if the head of the agency allows a cookie on the Federal web site. Are you telling me in your investigation, in your survey, you did discover that the IRS had a cookie on its web site that visitors could click onto and have information shared with third parties?

Ms. KOONTZ. When you were clicking onto a link that led you to another web site, the receiving web site was placing a cookie on your hard drive as you were exiting.

Mr. TAUZIN. Was that authorized by the head of the agency?

Ms. KOONTZ. I didn't ask them.

Mr. TAUZIN. How many web sites had cookies?

Ms. KOONTZ. There were eight web sites that had cookies.

Mr. TAUZIN. Out of the 65 that you surveyed, there were eight Federal web sites that had cookies by which third parties could gather information about citizens who visited those web sites?

Ms. KOONTZ. Yes. I want to be clear. This is third party cookies identified using FTC's methodology.

Mr. TAUZIN. I understand. The gentleman from Virginia, Mr. Boucher.

Mr. BOUCHER. Thank you. Let me ask our witnesses this morning if there is any reason why we shouldn't simply extend the protections of COPPA, which essentially require before any information is collected from children, that the permission of parents be obtained, to the Federal Government? Why should we not do that?

Ms. KATZEN. I don't have any problem with that. As the chairman noted, we have a memorandum from OMB instructing the agencies that they should comply, and if the law were expanded to cover Federal sites, it would be fine.

It may mean that when children write to the White House and ask for a picture of the President, they want a glossy picture, we could not respond unless they wrote their request on paper and provided a postal address for return mail. But aside from the inhibition on incoming requests for pictures or papers from the White House, there is no reason why the law should not be expanded. We believe strongly in COPPA and have supported it. Whenever we find that someone is not complying, we take down that site.

Mr. BOUCHER. Do either of the other witnesses have anything to add to that?

Ms. Katzen, you were attempting to provide an answer about current White House web site practices with respect to the Children's Online Privacy Protection Act. I think you did not get a full opportunity to answer that question, and I would like to afford that to you if you would like to do that.

Ms. KATZEN. Thank you very much, Mr. Boucher. We had originally had a White House kids page, which got a lot of requests from children and we knew that it would be covered within the spirit, if not the letter, of COPPA.

At the time we had asked for the child's name, the address, the e-mail address, the school, what grade they were in, a lot of different questions. Because of COPPA, we stripped that down to the bare essentials, the minimization principle, which is so prevalent in privacy discussions, and we only asked for that information if they wanted us to respond to them, not if they were simply communicating one way to us.

Also, we placed throughout the site in a number of places warnings that children should be talking to their parents, that they should be involving their parents in this. Finally, we have been negotiating with NARA, the National Archives, to see whether we could get an exception from the Presidential Records Act, as we have for bulk mail, for example, or if we could put these children's addresses, just to send them a picture of the President or Socks or Buddy, if we could put those addresses in a separate file or folder and/or destroy them so we don't retain that kind of information. Our objection is to protect children's privacy and to engage parents. We think COPPA is good law.

Mr. BOUCHER. And you would not object to having it extended to Federal Government sites generally?

Ms. KATZEN. Correct.

Mr. BOUCHER. Good. Let me hear your response to suggestions that I made earlier, that the time has now come for Congress to accept the invitation of the FTC and legislate a set of minimum

guarantees for the privacy protection of visitors to web sites, including the requirement that web sites post a notice of what information they collect and how it is used, and then provide an opt-out opportunity.

Is there any reason why we should not extend that set of guarantees not only to the practices of commercial web sites but also government web sites?

Ms. KATZEN. For the most part the actual substance of what you want to provide exists now in the law. In terms of legislation, this administration has taken the position that the most sensitive information should be protected first and foremost, so we have worked on financial records, we have worked on medical records. These are areas where we think that it is essential to provide adequate protection because they are so sensitive. If we could have those types of procedures in place for the very sensitive information, we would very much want to work toward the next step, which is to extend the scope of protecting privacy.

There are difficult questions, as Mr. Goodlatte and you have discussed—the balancing between giving out information and restricting the use of that information. But we have repeatedly called for more stringent protections, for financial, for medical, for genetic information and for Social Security numbers. There is a vast area that are specific problems have occurred.

Mr. BOUCHER. I gather the answer to the question is you are not sure and perhaps we need to consider further whether to extend that minimum set of guarantees not only to commercial web sites, but to government web sites as well?

Ms. KATZEN. I think it is an important step, but I think the other steps are more important and should take priority in any legislative proposal.

Mr. BOUCHER. May I have unanimous consent to proceed for 1 additional minute?

Mr. TAUZIN. Without objection, so ordered.

Mr. BOUCHER. Ms. Katzen, do you believe there are any statutory provisions that need to be adopted beyond what we have heard this morning? Do you have any recommendations for additional statutory provisions which would aid privacy of Internet users?

Ms. KATZEN. Yes, sir. The administration has a proposal to plug the loophole in Gramm-Leach-Bliley on financial records, which would enable consumers to know when information is being shared with affiliates of the organization. That bill in before the Congress. Mr. Markey has been active on that issue as well, I believe.

Medical health is another area. We have for 2 years requested Congress to move forward on medical health records. This is an area which is terribly important to people, whether it be sensitive matters like mental health records or HIV testing, or commonplace like mammograms. There is a story on NPR this morning about a woman who was fired after information about breast cancer became available.

The administration also has a Social Security bill to protect the sale and profiteering from selling Social Security numbers.

Genetic discrimination has been in committee for a long time. Ms. Slaughter's bill has been one that we have been supporting

and hoping Congress would pass. These are things that touch the lives of American people in a real way, not——

Mr. BOUCHER. Thank you.

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

Mr. BOUCHER. Thank you.

Mr. TAUZIN. The Chair recognizes the gentleman from Illinois.

Mr. SHIMKUS. Mr. Chairman, I yield my time to the gentleman from California. My brother-in-law was testifying before another committee, on the Government Reform Committee on anthrax. I got a chance to introduce him, and because of that I wasn't here to hear all of the testimony. In lieu of my being able to fully listen, I am going to yield my time to the gentleman from California.

Mr. TAUZIN. Mr. Cox from California.

Mr. COX. Thank you, and I will proceed out of order in that case. We begin with the GAO report telling us that most of our Federal agencies are not complying with the rules that we apply throughout the private sector when it comes to privacy. In fact, only 3 percent of agencies are implementing all or at least part of all of the FTC's requirements; and in particular the most disturbing, to me at least, finding is that so many agencies are placing cookies on the computers of people who log on.

I don't understand why the Office of Management and Budget in its latest guidance continues to permit the use of cookies by Federal agencies, continues to authorize the placement of cookies on citizens' computers, and I wonder if from OMB's perspective there is a good reason that we should have such vague rules about cookies. OMB doesn't differentiate between temporary and permanent cookies in its guidance. It is very, very brief, just a few paragraphs. Director Lew says that agency heads can approve putting cookies onsites. We have agencies then who are quoted in this article from Wired News saying that they are quite sure that their agency heads will approve this and continue to use the cookies.

The National Endowment for the Humanities says that they will continue to use cookies. The agency head was on vacation, that is what they told the reporter, but they were sure that the agency head would approve the gathering of information from citizens who log onto that site.

The Federal Energy Regulatory Commission actually says we generally do not use cookies; but according to Wired, anyone who stops by the FERC home page will receive a cookie and it will not expire until December of 2010.

The Department of Transportation has placed cookies on citizens' computers logging onto it that will last 34 years, and these are persistent cookies. They track your web activity after you leave the site.

So from the standpoint of OMB, why shouldn't we just say no cookies? Why are you putting cookies on people's computers? If you are investigating, I understand it. If somebody is not under investigation, why do we put a cookie on their computer, and why would that cookie track their activity when they left the site?

Ms. KATZEN. I think you raise a very important question to which my bottom line answer is that we shouldn't, and that is why the OMB policy was written. I think it is important to note that GAO did its study in July of 2000. We had issued the Lew memo-

randum, no cookies on this—presumption of no cookies in late June. So it has taken some time——

Mr. COX. But the Lew memorandum doesn't say no cookies.

Ms. KATZEN. It says there should be a presumption against cookies. Incidentally, there is a clarification on the session cookies point. There is a letter to Roger Baker from John Spotilla, who is the Administrator of the Office of Information and Regulatory Affairs, that says when you are logging on for a single session and you want to make a purchase order at the Mint, for example, and you have put in your name and address, and because you can't remember which things you wanted to buy, you want to open up another window and come back to the order form, having the session cookie there means that you can complete that one transaction. That cookie disappears when you have finished the transaction and log off, and that is the clarification of September 5 to Roger Baker.

There are other reasons, whether they be national security——

Mr. TAUZIN. Can we have a copy of that clarification for the record, Mr. Baker?

Ms. KATZEN. I have one here.

[The following was received for the record:]

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
September 5, 2000

ROGER BAKER
Chief Information Officer
U.S. Department of Commerce
Room 5033
14th & Constitution Avenue, NW
Washington, DC 20230

DEAR ROGER: Thank you for your letter of July 28, 2000, regarding OMB Memorandum 00-13 on "Privacy Policies and Data Collection on Federal Web Sites." We appreciate the CIO Council's strong support for protecting the personal information of citizens who visit federal web sites. We also stand ready to assist agencies as needed in implementing this guidance.

The President and the Vice President are strongly committed to the protection of privacy rights. They believe that the federal government should serve as a model of good privacy practices. Agencies need to be particularly careful before launching any effort to gather information on the activities of citizens who visit federal web sites. As we work to promote customer service, we must keep privacy concerns in mind.

In this spirit, OMB issued Memorandum 00-13, which aims specifically at the tracking of "the activities of users over time and across different web sites." As you correctly point out, a principal example of such is the use of persistent cookies. In accord with the Memorandum, federal web sites should not use persistent cookies unless four conditions are met:

- The site gives clear and conspicuous notice;
- There is a compelling need to gather the data on the site;
- Appropriate and publicly disclosed privacy safeguards exist for handling any information derived from the cookies; and
- The agency head gives personal approval for the use.

We are concerned about persistent cookies even if they do not themselves contain personally identifiable information. Such cookies can often be linked to a person after the fact, even where that was not the original intent of the web site operator. For instance, a person using the computer later may give his or her name or e-mail address to the agency. It may then be technically easy for the agency to learn the complete history of the browsing previously done by users of that computer, raising privacy concerns even when the agency did not originally know the names of the users.

We recognize that agency web sites can also seek information from visitors in ways that do not raise privacy concerns. Specifically, they may retain the information only during the session or for the purpose of completing a particular online

transaction, without any capacity to track users over time and across different web sites. When used only for a single session or transaction, such information can assist web users in their electronic interactions with government, without threatening their privacy. One example of such an approach that supports electronic government would be the use of a shopping cart to purchase a number of items online from the U.S. Mint. Another example would be the current technology that assists users in filling out applications that require accessing multiple web pages on the Department of Education's Direct Consolidation Loan site. We do not regard such activities as falling within the scope of Memorandum 00-13.

In your letter, you also inquired whether we should extend the policy guidance in Memorandum 00-13 to agency intranet sites as well as agency external internet web sites. The guidance, of course, focuses on internet traffic between the government and citizens. You raise an important issue, however, and we look forward to working with the CIO Council to review our policies regarding agency intranets.

Thank you again for sharing your insights and those of our CIO Council colleagues. Your creativity and support are indispensable to our electronic government efforts.

Sincerely,

JOHN T. SPOTILA

Mr. COX. What is the national security reason that we want to track the usage of the web by American citizens?

Ms. KATZEN. I cannot tell you that there is one.

Mr. COX. You just did.

Ms. KATZEN. I was interrupted when I was saying that if the agency head is presented with a compelling case for why this is crucial to the agency's mission or otherwise endangers some facet of their operation, then the agency head is to consider that information and make a decision. They are then to report that to OMB, where we will have a chance to review that. We will be getting information about this kind of situation and we will be monitoring it. I don't know offhand the kinds of situations that will be presented. We are talking about changes in technology that are happening very rapidly and practices that are changing very rapidly. And for us to try to set policy that says no way, no how, never, never, never, I think is to fly in the face of what we have seen.

Mr. COX. We are so far away from that with the Lew memorandum. The Lew memorandum, far from saying never, ever, ever, puts it at the discretion of every agency head.

Ms. KATZEN. It is not unbridled discretion because you have to have privacy policies in place. You have to have other kinds of——

Mr. COX. As I just quoted from the Wired News article, the agency heads or the people who work at these agencies have concluded, for whatever reason, for statistical purposes, collecting information about the use of their site, they can continue to put cookies onto people's computers, notwithstanding the Lew memorandum. That article was written after the Lew memorandum went out. Obviously people are not taking this as an instruction no longer to put cookies onto people's sites.

Last, with respect to COPPA, this business about the Presidential Records Act and now being able to respond to someone is relevant only if you are trying to end run the law because, as you know, the law, the basic provision of the law that the whole rest of the country is complying with is that you get parental consent. Verifiable parental consent is the touchstone of the law. If the White House were willing to live by the same rules as everyone else in America was living by, they would get parental consent and respond to kids in that way. The only reason that it becomes rel-

evant that you destroy the information is if you were trying to do an end run around that requirement. There is an exception where consent is not required in narrow circumstances and you are trying to exploit that provision by importing the Presidential Records Act as the reason that you can't get it done. Why can't you just comply with the law?

Ms. KATZEN. The exception that you note is the one-time contact and that is the situation that I am talking about. If you write in and say I want a picture of the President, it is only a one time contact. We are not trying to build a track record or a long-term relationship with the child. That is not an end run around the statute. It is recognizing, as Congress did, that if you are not going to build a long-term relationship, you don't need verifiable consent. Verifiable consent on a one-time contract only doesn't make a whole lot of sense. To have a child say I want a picture of Socks, and we respond: have your parent fill out a form and fax it in and when we get that, we will send the picture is a little bizarre. That is why that exception has that built in.

Mr. TAUZIN. The Chair recognizes the gentlewoman from Missouri, Ms. McCarthy.

Ms. MCCARTHY. I have no questions at this time.

Mr. TAUZIN. The Chair recognizes the gentleman from Texas, Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman. Ms. Katzen, the chairman outlined loopholes in the Privacy Act of 1974 and do you believe that the Privacy Act of 1974 is outdated and may allow the distribution of personal information cited by the Federal Government?

Ms. KATZEN. I think the Privacy Act has served us well for the last quarter century. I am always open to relooking at it to see whether in an age where we act faster with faxes and Internet, instead of more leisurely types of communication, some different language has to be included.

But if GAO asks us, or Congress in its oversight function asks us, for information, we are going to provide it, and I think citizens know that is the case. Those are the kinds of exceptions that are in there.

Routine use—to establish a routine use that the chairman mentioned, the agency has to publish a description of what it is they want to do—for example, they are going to take your information and share it with this bureau or that bureau for this purpose or that purpose. It is written in the Federal Register. Comments can be filed. It is a very public process.

So my instinct is that for the last quarter century we have been well served, but I would not be opposed to looking again at the language to see if it could be tightened. We believe in privacy.

Mr. GREEN. Are Americans providing information to Federal agencies vulnerable to having that information used in some inappropriate way, whether the IRS, whether it be HUD or somewhere else? Do you know of any examples where information that someone provided was used inappropriately?

Ms. KATZEN. I will not sit here and tell you that there is no misuse of information.

I can tell you that we have taken all reasonable steps to minimize that and to ensure that when we hear about something, there is a remedy.

I thought the first GAO study that identified where privacy policies could be more clearly stated, or better placed, was a good thing because the agencies saw that and they want to protect privacy, and they therefore have begun to take remedial steps from these kinds of reports. We have worked very closely with GAO to ensure that we know what is happening. I can't tell you there has never been an instance, and I won't do that.

Mr. GREEN. I don't expect that. We have remedies, but generally the American people ought to feel comfortable in contacting or providing information that it is not going to be shared.

Ms. KATZEN. Absolutely.

Mr. GREEN. And there are punishments for inappropriate use of that information.

Ms. KATZEN. Absolutely. Under the Privacy Act, if you feel that something has been done, you can bring suit.

Mr. GREEN. I want to make sure that there is an appropriate response that the U.S. Government can do to someone that is ilegally using this information.

Ms. KATZEN. There are civil and criminal statutes involved.

Mr. GREEN. Let me ask you about the Federal web placement of third party cookies, and the report that we have shows that 22 percent of all sites disclose that they may allow third party cookies, 14 percent allowed their placement. What would be the reason why we would allow placement of a third party cookie on our web site?

Ms. KATZEN. I don't know. I did not understand the GAO statement that agencies "may allow," and I did not understand that they "do allow" other than as people are leaving the site, the site to which they are going places the cookie. I think the witness from GAO was trying to explain it.

I should add that cookies are used for site management. They are very, very popular in the private sector. Everybody uses them in the private sector.

Mr. GREEN. Fourteen percent of a third party, I don't know if that is nongovernment. Mr. Baker, Ms. Koontz, do you know why we would have a third party involved in placing cookies on Federal web sites?

Ms. KOONTZ. In the survey that we did, we identified eight web sites where we picked up the concept of a third party cookie. In the vast majority of those, those were cases where a visitor might be clicking on a link to go someplace else, and the new site was placing the cookie before you left.

That is not something that is typically thought of as a third party cookie, but it was a concern because there was no clear warning that you were leaving, that you were subject to a new privacy policy or that a cookie was being placed. In one case, there was a Federal agency that did allow the placement of a cookie by a third party who collects information. This was done, I believe, as a way of the third party collecting usage information about that particular Federal site.

Mr. GREEN. It seems like we would want to have some kind of restrictions on third party cookies, whether it is inadvertent, and maybe that is something that should be looked at.

Thank you.

Mr. TAUZIN. I would like for the committee's edification, Ms. Katzen, if you would submit to the committee clarification of what conditions could an agency head permit the use of either session or persistent cookies under OMB policy.

Ms. KATZEN. Yes, sir.

[The following was received for the record:]

As discussed during the hearing, OMB Director Lew announced in June that, as a matter of federal policy, cookies that can track the "activities of users over time and across different web sites" will not be used on agency sites, except in very limited cases. When we issued this policy, we did not know and could not have known what mission-related uses of cookies might exist or be desired in the future. For this reason, we specified a process whereby only the agency head could give approval for the use of persistent cookies after balancing the importance of the use of cookies to the agency with the important privacy interests at stake. In addition, the agency head may give approval only where there is clear and conspicuous notice, a compelling need to gather the data, and appropriate and publicly disclosed privacy safeguards for the data gathered.

I am advised that there have been authorizations for the use of persistent cookies in a number of circumstances that on review I find appropriate and beneficial to the public. One example is the Department of Interior's Alaska Fire Service. Its site is targeted to fire managers around the state (although the site is public and can be accessed by anyone). It allows the managers to view time-critical weather data from more than one hundred weather stations around the state. Fire managers use cookies to create the right group of weather stations for each geographic area, and optimize their ability to determine local potential fire hazards. Other uses of persistent cookies include allowing users to return to a set of previously supplied transactional information. For instance, individuals can check their reservations with the National Park Service and purchasers can more conveniently purchase from a General Services Administration wireless store (generally after consent to the use of the cookie). We cannot anticipate at this time what other types of uses of cookies may prove worthwhile, and so leave the question open on a case-by-case basis.

Mr. TAUZIN. The Chair recognizes the gentleman from Maryland, Mr. Wynn, for a round of questions. I'm sorry, Mr. Sawyer is first. Mr. Sawyer from Ohio.

Mr. SAWYER. Thank you, Mr. Chairman. The irony of this is beyond belief. I have been going back and forth between Congress and Census with regard to a question which goes directly to this sort of thing. I am not going to go into that here, but I would hope that we could look at the mirror image of the concern that all of us up here share, and from what I am hearing you all share, about the assurance of privacy.

Could you talk to us for a moment, each of the three of you in turn, about how we make it possible for agencies of government to share information that they need in order to illuminate and inform sound policymaking here in a way that all of us would support without compromising the privacy of the information with which they have been entrusted?

Ms. KATZEN. Mr. Sawyer, that is a subject that is near and dear to my heart. That is something that I have worked on for the last 5 or 6 years. GAO sometimes refers to this issue in some of its studies. We have identified this as one of our priority management objectives this year, and have been working on it to do a number of things. One is to enable agencies to share information—to test eligibility, to ensure that the right person is getting the right ben-

efit, the right amount of the right benefit, and you do that by sometimes needing access to tax information, sometimes needing access to information that may be in somebody else's files.

That is one form of sharing. There is the act on computer matching. There are procedures that are involved, and there are very stiff restrictions. Section 6103 of the Tax Code, for example, precludes this kind of sharing without a very detailed process.

We have been working to see whether new technology will help us protect the privacy of the information, because one of our objectives in sharing data would be to ensure that, no matter in whose hands it was, it was being protected and it was being kept confidential.

Another area that we have been working on, which I think has something to do with what you have been doing in the time that you have not been here this morning, has to do with statistical information. Right now, we ask American businesses to supply all sorts of information over and over and over again. If we could have the statistical agencies share more of that information—BLS, BEA, Census—you would be able to reduce the burden on respondents and therefore increase the likelihood of complete and honest and accurate responses. That is an issue which doesn't have personal information usually. It doesn't have even identifiable information. But it has sufficient protection and confidentiality that we need to work out the process whereby sharing can happen.

Those are just two instances where, if we can establish that we do protect the information, we could save the American citizens and the American government a lot of time and effort.

Mr. SAWYER. Mr. Baker, from the point of view of the committee that you have been working with, could you comment on that?

Mr. BAKER. It is interesting that the drive toward electronic government, there are a lot of great ideas coming up with Federal employees and their contractors for how to utilize information. And on the other side, you have the Privacy Act, Title 13 and other things that do I think to this point an appropriate job of governing that enthusiasm and keeping us from putting data bases together in ways that we know how to do but, frankly, the laws I think appropriately keep us from doing.

One of the things that I can't help but emphasize, and I am sure you are well aware of this given the other thing that you are working on, is the attention that Federal employees pay to the privacy issue. When you go out to census and you are sworn in as a Title 13 swearing-in person, they take that very seriously. They are the defenders of the public's privacy as Federal employees, and I don't think that we recognize that or emphasize that enough in the government is that those people view that as their life job, A, to do a good statistical job but, B, to that protect that information.

So I think that the intersection of those two forces, electronic government and what we can do, the Privacy Act, Title 13 and others, on what they keep us from doing so far has kept a balance in there. We have been able to move ahead but not too quickly and not without doing a tremendous amount of violating the people's privacy. I don't know how we change that, to be frank. It is interesting to work in it right now, and again it is a balancing act there.

Mr. SAWYER. Ms. Koontz, in preparing your analysis of all of this, it is fair to say that you looked at it largely from the perspective of protecting privacy rather than the concomitant need to share information where appropriate.

Ms. KOONTZ. I don't think we took actually either perspective. Our charge was, very simply, to use the same criteria that FTC uses, use their identical methodology and to evaluate Federal sites using that criteria and methodology. I don't think there was a particular view associated with that except to the extent that FTC may have a view on how they look at sites.

Mr. SAWYER. In that sense, without having the two different angles from which to view a complex problem, would it be fair to say that—without using words like—I don't want to use—I won't even use the word, but that it yields a less than fully developed portrayal of the complexity of the problem that we are trying to deal with here?

Ms. KOONTZ. I guess I look at this issue a little bit differently. It is true that you can't hold Federal sites accountable for not following the FTC methodology and the FTC fair information principles. They are subject to other rules, other laws, other regulations. But then, on the other hand, I think it is useful to look at what Federal agencies are doing in light of various standards as a way of, I think, continuing a debate on whether we are happy with the status quo. Are we happy with requirements that we have or do we need to take a re-look at them?

Mr. TAUZIN. Gentleman yield a second?

Mr. SAWYER. Please do.

Mr. TAUZIN. Just to point out, I don't think private sites are required to follow the FTC. There is no law following that.

Ms. KOONTZ. That is correct.

Mr. SAWYER. Thank you, Mr. Chairman.

Mr. TAUZIN. Chair recognizes the Mr. Wynn from Maryland.

Mr. WYNN. Thank you, Mr. Chairman.

I guess I take a somewhat conservative view starting with domain cookies, and I really would like to get a clear understanding of the rationale for domain cookies with respect to getting personal information and how that enables you to manage—how the identification of the user enables you to, quote, manage the site better.

Ms. KATZEN. Let me start, and then Mr. Baker might be able to add—will definitely be able to add something.

When we launched firstgov on September 22, everybody wanted to know how many hits did we get? And the question is, is that the same person coming back 12 times or is it 12 different people? If you have a cookie, you can tell whether it is the same person or not. Now that is how you use it for site management.

Mr. WYNN. If I could jump in, is that the best rationale?

Mr. BAKER. Sir, if I could, I think the best rationale is the one the private sector utilizes, which is personalization of a web experience is a real benefit to the consumer, if that is all the information is used for is that personalization. So, for example——

Mr. WYNN. But there is an assumption there that I am not ready to accept and that is that personalization is in the interest of the consumer. Says who?

Ms. KATZEN. Some consumers choose it. Mr. Goodlatte sat here and said he has no objection and indeed he sort of likes the idea that when he goes to Amazon.com they say, you like biographies. That is how they use it in the private sector.

Mr. WYNN. I want to go back to this. There is no opt-out so your assumption that it is good for the consumer to be personalized doesn't give the consumer the ability to say, no, I don't want to be personalized.

Mr. BAKER. I would agree with you. There needs to be opt-out.

Mr. WYNN. That is one item that I think is important for discussion. You agree there needs to be opt-out on domain cookie, is that your position?

Mr. BAKER. My personal position, it would be yes, recognizing that that will have an impact on, if you will, the value of the companies in the Internet who base a lot of what they do on being able to personalize, that personalized experience.

Mr. WYNN. That is fine. I am satisfied. I think we have got at least one policy option on the table, and that is let consumers out of this, and that is fine.

Now is there any other rationale for domain cookies that we need to be aware of? Okay, with respect to third-party cookies, shouldn't there be some probable cause standard or some restriction conditioning, however you would phrase it, to justify any imposition of third-party cookies. I think members of the panel seem to be saying the same thing in a lot of ways. I will be candid and say I have a very hard time of accepting the notion of third-party cookies unless someone presents a probable cause case for national security.

Ms. KATZEN. Federal web sites are not to have third party cookies.

Mr. WYNN. What is the penalty?

Ms. KATZEN. The penalty would be to immediately take the site down and hold the agency head responsible, as you would with any other kinds of violations of Federal policy. The assumption is that Federal employees will obey the policy as Mr. Baker indicated.

Mr. WYNN. There are no statutory penalties against a Federal employee that imposes a third-party cookie.

Ms. KATZEN. Not that I am aware of. But I am also not aware of any instances where they are, in fact, imposing them, as Ms. Koontz was indicating they——

Mr. WYNN. I thought you said there were about eight out of 65, is that correct?

Ms. KATZEN. That is where, as people are leaving the site——

Mr. WYNN. Please clarify that.

Ms. KOONTZ. We identified these using the methodology that FTC used. We picked up eight instances that we called third-party cookies.

Mr. WYNN. We can stop there. So there are instances—any requirement in law that those eight instances be justified or can we conclude that they are, per se, in violation of existing law?

Ms. KOONTZ. I don't know the answer to that question. I think that is——

Ms. KATZEN. It is not law, but policy. If they were placed by the agency, as opposed to the exiting link, which is what you had said earlier—many of these were placed as people click to go to some-

place else. It is the someplace else that puts the cookie on the person's machine. It is not the agency. But if the agency is doing it, they shouldn't be doing it unless they have gone through the materials that we have provided to them in terms of the finding that they need to make, privacy protections that need to be in place, and the other processes in reporting to OMB on this kind of situation.

Mr. WYNN. So they can make a showing to OMB, and it is okay to impose a third-party cookie?

Ms. KATZEN. It may or may not be okay, depends on what they show.

Mr. WYNN. What do they have to show to justify a third-party cookie?

Ms. KATZEN. That having the cookie is critical to obtaining their mission, and I think that is a pretty high showing.

Mr. WYNN. Well, it depends on whether it is national security or whether it is Department of Interior.

Mr. TAUZIN. Would the gentleman yield? If the gentleman will yield, I will quote from the memorandum for the gentleman.

It says that under this new Federal policy dated June 22nd cookies should not be used in Federal web sites or by contractors when opening web sites on behalf of agencies unless, in addition to clear and conspicuous notice—first of all, you have to at least give people the notice you are doing it—the following conditions are met: the compelling need to gather the data on the site—whatever that means—and appropriately and publicly disclosed privacy safeguards for the handling of the data on the site, appropriately and publicly disclosed privacy safeguards for handling information derived from the cookies, and personal approval by the head of the agency.

Mr. WYNN. I thank the chairman. If I could have 30 seconds——

Mr. TAUZIN. Gentleman is recognized for an additional 30 seconds.

Mr. WYNN. My concern is where is the oversight of the agency decision that they have a need to collect this information? I am perfectly willing to accept a national security, a law enforcement rationale, maybe the Interior does have a rationale, but where is the oversight that would enable those of us in Congress to know that these agencies are acting in fact within the scope of their authority?

Ms. KATZEN. Well, this information would ultimately be gathered together by OMB and OMB has very aggressive oversight committees that are constantly asking for, legitimately, this kind of information. I would also note this is a subject that has gotten a lot of play in the press because this is not something you can do in secret. The reason we are here is because there is a whole cadre of people there who are constantly testing us, the private sector, NGO's, they are constantly trying to discover these activities.

Mr. WYNN. In other words, agencies that report to you, it has a rationale—is there mandated reporting of that information to Congress?

Ms. KATZEN. No, sir.

Mr. WYNN. Thank you, Mr. Chairman.

Mr. TAUZIN. I thank the gentleman.

For the record—you can submit this for the record. It was raised by a number of members. When was the last criminal prosecution of a Privacy Act violation? If you can submit that for the record. We can't recall one. We can recall a lot of stories about personal data being released to the press—Kathleen Willey, Linda Tripp, all kinds of stories. Was there any prosecutions of violations of their rights?

Ms. KATZEN. We will be happy to do that.

[The following was received for the record:]

According to the Department of Justice, the last criminal prosecution under the Privacy Act was *U.S. v. Trabert* (D. Colo. 1997)

Mr. TAUZIN. Gentleman from California, Mr. Cox.

Mr. COX. Thank you, Mr. Chairman.

I just want to underscore my complete agreement with the concerns expressed by Representative Wynn; and I hope that also for the record, Mr. Chairman, if you would permit, perhaps we could see a list of those circumstances in which the collection of cookies, not temporary cookies, not session cookies, would be compelling for any agency under this memorandum.

Mr. TAUZIN. If the gentleman would yield a second, I want to make sure the request is specific.

GAO identified eight sites of the surveyed sites, and GAO only surveyed at random a certain number of sites and the top 30-some high-volume sites. What the gentleman is asking for the record is submission of all of the existing authorized cookies on all Federal sites, if you can identify those along with the compelling reasons for those cookies to be on those sites.

And I yield back to the gentleman.

Mr. COX. I think in Representative Wynn's question he had embedded the sense we all share that if a person is legitimately under investigation that obviously tracking them through their web usage is as legitimate as tapping their phone or anything else. But, you know, if the national security concern is that somebody might be hacking into our computers or what have you, then we are all for doing whatever we can to try to track that down. But putting that in a clear category of its own, literally intentionally investigating people, what are the reasons that OMB thinks the government ought to be placing cookies on people's computers for that are not just session cookies? And if you could answer that for the record, because I know that——

Ms. KATZEN. I would be happy to, although I should state that we don't have a preexisting list of conditions. We don't think persistent cookies should be on Federal websites, but since we do not know everything and we don't know all the different circumstances that could be presented, we established this process. But I will supply the information that you requested for record.

[The following was received for the record:]

Please refer to the response to Representative Tauzin's earlier question.

Mr. COX. All right, and I would just then conclude by saying I hope to get rid of the cookies. I think a policy——

Ms. KATZEN. So do I.

Mr. COX. If the concern is, gee, the government is so big, we can't get an answer to this question fast enough or we can't get it done

quickly enough, which is what the administration expressed to wired news when they put the question, the best way to get it done quickly is to have a clear policy.

Also, as you mentioned in your opening comments, if the objective is to instill confidence in the public that they are not in any way to be worried when they are going on to a government site, the easiest way to do that is to have a rule that the public can understand, which is no permanent cookies. And you know the notion that we have got cookies on computers. Some of the people on this committee, some of the staff have tracked this where the expiration days are 2034 where our government has been putting these cookies on lately. That is a very bad thing.

I just logged on the White House web site and checked out the privacy disclosure there with respect to the kid's site and the regular site, and it states that the White House is collecting IP addresses. Now, on IP addresses unique to a specific computer, I need to know why that is important, but that I would think you could answer now.

Ms. KATZEN. If you would—I would rather provide it for the record rather than now—and I will provide that for the record, sir.

Mr. COX. I thank the chairman.

[The following was received for the record:]

Unlike an e-mail address, which can serve as a personal identifier, IP addresses are not personally identifiable tags. They are assigned to each computer using the Internet or other similar networks an are an integral component of network communications. IP address are session based—every time a user uses the Internet, he or she receives a different IP address.

The White House web site is not unique in "collecting" IP address. Collecting IP addresses is an industry standard and all commercial software automatically collects IP addresses and compiles them into network activity logs. System administrators use these activity logs primarily for two purposes: first, to asses network and system performance and, second, as a standard security procedure to detect unauthorized intruders (i.e. hacking).

Mr. TAUZIN. Let me make an announcement.

We have a vote on the floor, Mr. Markey has arrived and wants to do a round of questions, and we want to recognize—before I do that, let me announce that both Mr. Shaw and Mr. Pitofsky have arrived, and we want to accommodate them as quickly as we can when we get back. So we will not have time I think, Mr. Shaw. So if you don't mind we will make this vote and come right back. We will take you up immediately, Clay, if that is all right with you. If you can just tell us briefly what your scheduling problem is.

STATEMENT OF HON. E. CLAY SHAW, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. SHAW. Well, the problem—I can dispose of this right new and leave this statement. This is a question of privacy issue having to do with Social Security. We are not—I know Mr. Markey is interested in that as well as the chairman, and this is something we should put high on our agenda next year when we return.

Mr. TAUZIN. I thank the gentleman. The statement will be part of the record. Thank you, Mr. Shaw.

[The prepared statement of Hon. E. Clay Shaw, Jr. follows:]

PREPARED STATEMENT OF HON. E. CLAY SHAW, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. Chairman and members of the Subcommittee, I commend you for holding this very important hearing, and I appreciate the opportunity to testify before you today.

As Chairman of the Ways and Means Subcommittee on Social Security, my particular interest lies in the area of protecting the privacy of Social Security numbers (SSNs). This summer, my Subcommittee held three hearings on SSN use and misuse. We learned about the tragedy of identity theft from retired Colonel and Mrs. Stevens of Maryland who have seen their SSNs used to open 33 fraudulent accounts and to rack up $113,000 of bad debt. We also heard from Mr. Bob Horowitz, a single father and small business owner from my district, who saw his number used to open five fraudulent credit accounts. Months and years later, they are still spending time, money, and energy to clear their names and in the Steven's case, bring their perpetrators to justice.

SSN misuse is a growing problem that needs to be addressed. In fiscal year 1999 alone, Social Security's Office of Inspector General received 62,000 allegations of SSN fraud, and the average number of monthly allegations has been increasing. This growth in SSN crimes has raised serious concerns over privacy and has emphasized the need to better protect SSNs in the law.

When SSNs were created 65 years ago, their only purpose was to track a worker's earnings so that Social Security benefits could be calculated. But today, use of the SSN is rampant.

We have literally developed a *culture* of dependence on the SSN. Businesses and governments use the SSN as the primary way of identifying individuals. It is integral to their business operations, program administration, record-keeping systems, and data-sharing systems. All of us know how difficult it is to conduct even the most frivolous transaction without having to cough up our Social Security numbers first. And once we provide this information for one purpose, it is often sold without our knowledge or used for other purposes without our consent.

Although SSNs are used for many legitimate purposes, their prevalent use has made them very valuable. For example, counterfeiting Social Security cards for illegal aliens and using false SSN information to obtain federal benefits illegally have become quite profitable.

Moreover, as we learned from Colonel Stevens and Mr. Horowitz, SSNs are so valuable, that someone who steals your SSN can literally steal your identity. Identity theft is now considered the fastest growing financial crime in the country, affecting more than 750,000 people every year and creating more than $745 million of monetary losses annually.

Despite the pervasive use of SSNs and the potential for fraud, SSNs receive very little protection under the law. Clearly, there is a need for a comprehensive law that will better protect this very personal information and protect the American public from being victimized.

Earlier this year, I introduced H.R. 4857, the Social Security Number Privacy and Identity Theft Prevention Act of 2000 along with several members of the Ways and Means Committee. This bill was drafted on a bipartisan basis, and it passed unanimously out of the Subcommittee and the Full Ways and Means Committee.

H.R. 4857 takes a comprehensive approach to SSN privacy by targeting the treatment of Social Security numbers in both the public and private sectors. A summary of the bill is provided below.

Restrictions on the Sale and Public Display of SSNs by Government Agencies

- Prohibits Federal, State and local governments from:
  - selling SSNs (limited exceptions are made to facilitate law enforcement and national security, to ensure the accuracy of credit and insurance underwriting information, and to allow for the effective administration of programs authorized under the Social Security Act),
  - displaying SSNs on Internet sites and public documents (limited exceptions are made to facilitate law enforcement and national security and to ensure the accuracy of credit information),
  - displaying SSNs on checks, employee identification cards, military tags, and identification documents issued by State Departments of Motor Vehicles, such as drivers' licenses and motor vehicle registrations, and
  - employing prisoners in jobs that provide them with access to SSNs.
- Strengthens verification requirements for birth records when someone applies for a SSN card.

- Requires the U.S. General Accounting Office to conduct a comprehensive study regarding how use of the SSN can be minimized at all levels and branches of government.

Restrictions on Sale, Purchase, and Use of SSNs in the Private Sector

- Authorizes the Federal Trade Commission to issue regulations restricting the sale and purchase of SSNs in the private sector.
- Discourages businesses from denying services to individuals who refuse to provide their SSNs by subjecting them to penalties under Federal law.
- Includes the SSN in the definition of "credit report" under the Fair Credit Reporting Act so that the SSN receives the same privacy protections as other consumer credit information.

The first two provisions are within the jurisdiction of the Commerce Committee, and the third provision is within the jurisdiction of the Banking Committee.

Enforcement, Fines, and Penalties

- Creates new criminal and civil penalties for violations of the law relating to sale, purchase, or misuse of the SSN.
- Allows Federal courts to order defendants to make restitution to the Social Security Trust Funds or the General Fund of the Treasury for violations of the law.
- Enhances law enforcement authority for the Social Security Administration Office of Inspector General.

In addition to these provisions, H.R. 4857 strengthens protections for Social Security and Supplemental Security Income beneficiaries whose monthly benefits are managed by representative payees. The bill also includes several technical amendments that were submitted by the Social Security Administration.

The Ways and Means Committee did not consider any of the private-sector provisions because they are not within the Committee's jurisdiction. However, we have received many comments about these provisions, which were forwarded to the appropriate Committee. In general, the comments we received emphasized the role of the SSN as a unique identifier which enhances the efficiency of commercial transactions, ensures the accuracy of consumer records, facilitates fraud prevention efforts, and helps enforce the law. I urge the Commerce and Banking Committees to consider the provisions that have been referred to them as soon as possible.

H.R. 4857 is a responsible and sensible bill. It balances concerns over privacy with concerns over efficiency. At the same time, it will effectively protect Social Security numbers and protect citizens from identity theft and other SSN crimes. Businesses and governments will need to re-think the way they do businesses so that customers are put first. Only through this type of re-tooling can we change the culture of dependence on Social Security numbers. Americans' right to privacy must be protected. I urge your Subcommittee to work with us so that together we can put the security back into Social Security numbers.

Mr. TAUZIN. The Chair now recognizes the gentleman from Massachusetts.

Mr. MARKEY. Thank you, Mr. Chairman.

Congressman Shaw and I have been working on this issue of privacy inside this Social Security context, and it just shows this is not a liberal or conservative or Democrat or Republican issue at all. It is an issue where the liberal left meets the libertarian right, isolates the pragmatic middle, okay, who just don't like to tell industry or their government employees that they can't do this. So there is kind of a pragmatist middle here that we just have to isolate and ultimately eliminate. That is the bottom line on this. That is the pragmatists, they are the problem here, because everybody else agrees on the issue.

The issue isn't really Big Brother. The issue is Big Browser. They give it to anybody, public sector or private sector. They can't control themselves. They just have to get this information. It is almost like a compulsion. It is an obsession. Because it is there, the technology controls the ethos. Because you can do it, you do it. Technology makes it possible. So it is the browser itself, it is this capacity to data mine, you know, to know all this information.

So, yeah, in a private sector, government context, you all call it security. You know, we need better security. From an individual's perspective, they say we need better privacy. It is all the same issue, though. Security, privacy, it all just means is the information secret or not.

Well, the industry says, we want stronger encryption technology so we can move this information from the consumer to us, but after we get it, we don't have any rules, we can do whatever we want with it. The government says, we want security, but that is just so we can keep our information private. But if we can gather information about private citizens that help us do our business, it is good. But from a consumer's perspective, it is all their privacies, their individual family's identity. So that is why self-regulation doesn't work. You can't allow the government to self-regulate; you can't allow the private sector to self-regulate.

You have got to have a certain minimal set of protections that every individual is entitled to, whether it be a big government agency or a big corporation or a small government player in your hometown or a small company in your hometown. Regardless of who it is, you have got to have this minimal set of rights that every American is entitled to, and so——

We have a roll call on the floor.

I thank all of our witnesses for helping us. I apologize for arriving late, but I thank you, Mr. Chairman.

Mr. TAUZIN. I thank the gentleman, and the Chair thanks the witnesses for their attendance and their participation. What we will do is declare a 15-minute recess, give everybody a break.

Chairman Pitofsky, we will be back. As soon as we come back, we will take you up first, as soon as we get back.

The committee stands in recess.

[Brief recess.]

Mr. TAUZIN. The subcommittee will please come back to order.

We are pleased to welcome the Honorable Robert Pitofsky, the Chairman of the Federal Trade Commission, who is elated today because the Senate just passed his reauthorization bill. He would love to see the House take it up before we leave.

Mr. Pitofsky, we have often had this conversation in private and public. We are at it again. Today we welcome you. Your statement, of course, is part of the record; and we welcome you to summarize your report to us today on privacy, both in the private and public sector.

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

Mr. PITOFSKY. Thank you very much, Mr. Chairman, members of the committee. As always, I appreciate this opportunity to discuss with you and the members these important issues relating to privacy.

As this committee knows very well, the Commission has acquired considerable expertise and experience in addressing privacy issues on-line and off-line in recent years. Our activities in this area are based on our statutory authority to challenge marketing practices that are deceptive or unfair. Let me start with some basics.

Protection of privacy is important to consumers. All surveys demonstrate consumer concern, and on-line commerce will not reach its full potential until and unless these privacy issues are adequately addressed.

Incidentally, I saw just yesterday a Harris survey that reported that among Internet users, they were more concerned with their privacy on the Internet than they were with health care, crime and taxes. A really remarkable set of findings.

Second, basic protections include notice of what information is collected and how it will be used, consent to use by consumers of their personal information, reasonable access to a data base to correct errors, and reasonable security arrangements as to how information is used.

Even if all these fair information practices are adopted, that is not enough. There must be effective monitoring and enforcement to ensure that privacy guarantees are really respected, and it is interesting that many in the business community have pretty much adopted the four fair information practices that I described.

The policy dispute in this area has turned on whether fair information practices can be best achieved through self-regulation or legislation. My own view is that neither approach should be exclusive. Self-regulation is essential, but it will be most effective if it is backed by a rule of law.

Also, Mr. Chairman, addressing an issue that I know you have raised with me, any policy choice must be flexible in the sense that it takes into account the possibilities that new technology may ease or modify the need for legislation.

The FTC has conducted or reported on three surveys. Our first, in 1998, found of all sites surveyed only 14 percent published a privacy notice. The second, in 1999, showed 64 percent. According to our 2000 survey, the figure had reached 88 percent. That is the good news.

But these numbers must be placed in context. Only 20 percent of the sites reviewed in the 2000 survey satisfied all four fair information practices. Of the 88 percent that did include a privacy disclosure, many offered a kind of notice that was inadequate, misleading or obscure. Most important to me, only 41 percent provided notice and consent, in my view the two essential fair information practices.

I should add that if you didn't look at these numbers from the point of view of all sites but only the hundred most visited, the numbers would be much better. For example, notice and consent are provided on 60 percent of the most-visited sites.

Beyond statistics, there is a policy question of what to do about firms that provide inadequate notice or no notice at all. Those advocating an exclusively self-regulatory approach argue that firms should be denied a seal of approval and consumers observing the absence of the seal will choose to do business with other on-line sites. There are quite a few flaws with that approach.

First, even in our 2000 survey, our most recent survey, only 8 percent of web sites posted a seal of approval; 92 percent did not. More important, I do not see that denial of a seal of approval will really influence the outliers, the relatively few unprincipled firms,

that are collecting and selling private data and will ignore industry standards designed to change their ways.

The fact of the matter is that the best self-regulatory programs among advertisers, funeral directors and others are effective because they are backed by a rule of law.

Beyond this fundamental question of legislation versus self-regulation, the Commission has been active in other areas.

We commended the self-regulatory practices by the Network Advertising Initiative, an organization comprised of leading Internet advertisers, to develop a framework for self-regulation in the profiling area, although we said there, too, that legislation to back them up would be appropriate.

We issued rules interpreting Congress' statute entitled the Children's On-line Privacy Protection Act designed to protect young people from exploitation.

We issued rules under Gramm-Leach-Bliley designed to protect consumers' privacy when dealing with financial institutions.

Finally, the Commission has brought three cases in the past year challenging deceptive or unfair conduct in connection with web sites, and with additional support from Congress on our budget we will be more active in the future.

To conclude, my hope is that in the next Congress, government, consumer advocates and the business community can join forces in finding their way to a moderate, balanced, forward-looking and sensible form of privacy protection.

I would be glad to answer your questions; and, if I may, I would like to invite our Bureau Director, Jodie Bernstein, to join me for some of detailed questions that we may run into. Director Bernstein.

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

PREPARED STATEMENT OF 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 an overview of the Commission's work over the past year in protecting consumers' privacy.[1]

I. INTRODUCTION AND BACKGROUND

As you know, the Federal Trade Commission is the federal government's primary consumer protection agency and our responsibilities are far-reaching. The Commission's 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] Pursuant to these responsibilities, the Commission has acquired considerable experience in addressing privacy issues

[1] 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 other 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).

in both the online and offline worlds,[4] and has long had particular interest in, and gained extensive experience dealing with, privacy and consumer protection issues.[5]

The Commission's interest and involvement in online privacy dates back to 1995. From that time forward, the Commission has held a series of public workshops on online privacy and related matters designed to educate itself and the public on the many issues involved. In addition, the Commission has been active on a number of privacy fronts. We have examined web site practices in the collection, use, and transfer of consumers' personal information; encouraged and evaluated self-regulatory efforts and technological developments to enhance consumer privacy; developed consumer and business education materials; and have studied the role of government in protecting online information privacy, including in particular, the online collection and use of information from and about children.[6] The Commission also has issued a series of reports to Congress regarding privacy online, including the topics of online profiling and the global aspects of Internet privacy.

II. COMMISSION INITIATIVES IN THE LAST YEAR

The past year has been a very busy one for the FTC in the area of consumer privacy.

Our efforts have included the following:

- surveying Web sites to examine their information practices and privacy statements;
- convening the Advisory Committee on Online Access and Security to study and provide recommendations pertaining to (a) consumers' access to their personal information; and (b) appropriate measures to protect the security of that information;
- issuing a report to Congress on online privacy;
- issuing a series of reports to Congress on third-party online profiling;
- issuing Rules implementing the Children's Online Privacy Protection Act (COPPA) and the Gramm-Leach-Bliley Act (GLBA);
- providing comments to other government agencies examining privacy issues; and
- bringing law enforcement actions against Web sites that violate the FTC Act.

What follows is a brief summary of our work in each of these areas.

2000 Online Privacy Survey and Report to Congress

In its most recent report to Congress on online privacy, a majority of the Commission recommended legislation requiring consumer-oriented commercial Web sites that collect personal identifying information from or about consumers online to comply with the four fair information practices: Notice, Choice, Access, and Security.[7] The Report analyzed the results of the Commission's survey of commercial Web sites' information practices, conducted in February and March 2000, and discussed the work of the Advisory Committee on Online Access and Security, which the Commission convened in December 1999.

The Advisory Committee on Online Access and Security, a group comprised of 40 e-commerce experts, industry representatives, security specialists, and consumer and privacy advocates, provided advice and recommendations to the Commission regarding the implementation of the fair information practice principles of Access and Security online. In a series of public meetings, the Advisory Committee discussed options, and the costs and benefits of each option, for implementation of these principles. The Advisory Committee submitted a final report to the Commission in May

---

[4] The FTC Act and most other statutes enforced by the Commission apply equally in the offline and online worlds. *See, e.g., FTC v. ReverseAuction.com, Inc.,* No. 00-0032 (D.D.C. Jan. 6, 2000) (discussed *infra*); *In re Trans Union,* Docket No. 9255 (Feb. 10, 2000), *appeal docketed,* No. 00-1141 (D.C. Cir. Apr. 4, 2000) (holding that defendants' sale of individual credit information to target marketers violated the Fair Credit Reporting Act).

[5] In particular, the Commission has law enforcement responsibilities under the Fair Credit Reporting Act, which, among other things, limits disclosure of "consumer reports" by consumer reporting agencies, 15 U.S.C. §§ 1681 *et seq*., and under the Gramm-Leach-Bliley Act, which restricts the disclosure of consumers' personal financial information by certain financial institutions, 15 U.S.C. §§ 6801-6809 (Subtitle A).

[6] *See, e.g., Online Profiling: A Report to Congress, Part 2 Recommendations* (July 2000); *Online Profiling: A Report to Congress* (June 2000); *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000) ("2000 Report"); *Self-Regulation and Privacy Online: A Report to Congress* (July 1999); *Privacy Online: A Report to Congress* (June 1998); *Individual Reference Services: A Federal Trade Commission Report to Congress* (Dec. 1997); *FTC Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure* (Dec. 1996); *FTC Staff Report: Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (May 1996).

[7] The Commission vote to issue the Report was 3-2, with Commissioner Swindle dissenting and Commissioner Leary concurring in part and dissenting in part.

2000 which highlighted the complexities of implementing Access and Security and, in light of the differing views of Committee members, developed several different options for providing Access and Security.[8]

The Commission's survey included two groups of sites drawn from a list of the busiest U.S. commercial sites on the World Wide Web: a census of 91 of the 100 busiest sites (the "Most Popular Group"), and a random sample of 335 sites that had at least 39,000 unique visitors per month (the "Random Sample").[9] The survey results showed that 88% of sites in the Random Sample and 100% of the sites in the Most Popular Group posted at least one privacy disclosure, and that 20% of Web sites in the Random Sample that collected personal identifying information, and 42% in the Most Popular Group, implemented, at least in part, all four fair information practice principles. The Commission also examined the data to determine whether Web sites were implementing Notice and Choice only. The data showed that 41% of sites in the Random Sample and 60% of sites in the Most Popular Group met the basic Notice and Choice standards.

Based on these results, as well as on the lack of a widely-adopted self-regulatory enforcement mechanism, a majority of the Commission recommended that Congress enact legislation to protect consumer privacy online. The proposed legislation would require Web sites to implement: (1) notice (providing clear and conspicuous notice of their information practices); (2) choice (offering consumers choices as to how their personal identifying information is used beyond the use for which the information was provided, including choice for both internal and external secondary uses of the information); (3) access (offering consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information); and (4) security (taking reasonable steps to protect the security of the information collected from consumers).[10]

Online Profiling Workshop and Reports to Congress

In November 1999, the Commission, together with the Department of Commerce, held a public workshop on "online profiling"[11] by third-party network advertisers, firms that place advertisements on Web sites. The workshop was designed to educate the public about this practice, as well as its privacy implications, and to examine current efforts by network advertisers to implement fair information practices. At the workshop, industry leaders announced the formation of the Network Advertising Initiative (NAI), an organization comprised of the leading Internet network advertisers, to develop a framework for self-regulation of the online profiling industry. Following the workshop, the NAI companies submitted drafts of self-regulatory principles for consideration by FTC and Department of Commerce staff. After lengthy discussions, a set of principles emerged that a majority of the Commission found to be a reasonable implementation of the fair information practice principles. The Commission discussed the NAI Principles in Part 2 of its Report to Congress in July, 2000.[12]

---

[8] Available at http://www.ftc.gov/acoas/papers/finalreport.htm.

[9] 2000 Report at Appendix A.

[10] 2000 Report at 36-38. The proposed legislation would govern U.S. commercial Web sites to the extent not already covered by the Children's Online Privacy Protection Act, 15 U.S.C.§ 6501 et seq.

[11] Online profiling is the practice of aggregating information about consumers' interests, gathered primarily by tracking their movements online, and using the resulting consumer profiles to deliver targeted advertisements on Web sites. The transcript of the workshop, as well as public comments filed in connection with the workshop, are available at <http://www.ftc.gov/bcp/profiling/index.htm>.

[12] *See Online Profiling: A Report to Congress, Part 2* (July 2000). The Commission vote to issue Part 2 of the Report was 4-1, with Commissioner Swindle dissenting and Commissioner Leary concurring in part and dissenting in part. Both Commissioner Swindle and Commissioner Leary commended NAI's self-regulatory program. A copy of the NAI principles is attached as an appendix to that report. The report is available at <http://www.ftc.gov/os/2000/07/onlineprofiling.htm> and the NAI principles are available at <http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf>. Among other things, the NAI Principles provide that consumers will receive notice of network advertisers' profiling activities on the Web site they are visiting (the so-called "host" or "publisher" Web site) as well as notice of their ability to choose not to participate in profiling. Where personally identifiable information is collected for profiling, a heightened level of notice, "robust" notice, will be required at the time and place such information is collected and before the personal data is entered. In addition, material changes in the information practices of a network advertising company cannot be applied to information collected prior to the changes, and previously collected non-personally identifiable data ("clickstream") cannot be linked to personally identifiable information without the affirmative (opt-in) consent of the consumer.

Despite the NAI companies' commendable self-regulatory initiative, however, a majority of the Commission found that backstop legislation was still required to fully ensure that consumers' privacy is protected online. The majority reasoned that while NAI's current membership constitutes over 90% of the network advertising industry in terms of revenue and ads served, only legislation can compel the remaining 10% of the industry to comply with fair information practice principles. The majority believed that self-regulation also cannot address recalcitrant and bad actors, new entrants to the market, and drop-outs from the self-regulatory program. In addition, the majority found that there are unavoidable gaps in the network advertising companies' ability to require host Web sites to post notices about profiling, including Web sites that do not directly contract with the network advertisers, and stated that only legislation can guarantee that notice and choice are always provided in the place and at the time consumers need them. Accordingly, a majority of the Commission recommended legislation that would set forth a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites with respect to online profiling.

The Children's Online Privacy Protection Act

In its 1998 Report to Congress on online privacy, the Commission documented the widespread collection on the Internet of personal information from young children, and recommended that Congress enact legislation to protect this vulnerable group. In October 1998, Congress passed the Children's Online Privacy Protection Act of 1998 ("COPPA"),[13] As required by the Act, on October 20, 1999, the Commission issued the *Children's Online Privacy Protection Rule*, which implements the Act's fair information practice standards for commercial Web sites directed to children under 13, or commercial sites that knowingly collect personal information from children under 13.[14] Violators of COPPA are subject to FTC law enforcement action, including civil penalties of $11,000 per violation.

There have been several press reports indicating that some Web sites directed to children have experienced difficulty in complying with COPPA, particularly in the context of children's chat rooms (online discussion groups). Staff believes that, to some extent, these concerns may have been caused by misunderstanding of the Rule's requirements or unfamiliarity with the exceptions built into the Rule. FTC staff is working hard to educate Web site operators on these issues; staff hosted a well-attended "compliance clinic" for operators in August, and has scheduled a second clinic on the West Coast in November.[15]

Some Web sites also have decided to discontinue children's chat rooms rather than to meet COPPA's requirements of either obtaining parental consent or monitoring chat rooms to prevent the disclosure of children's personal information. The operation of unmonitored children's chat rooms, which provide the opportunity for children to disclose personal information to third parties, has raised serious concerns about children's safety online. Those concerns contributed to the Commission's decision to recommend that Congress enact legislation to protect children's privacy online.

In addition to the compliance clinic, the FTC has undertaken a number of initiatives designed to enhance compliance with the Rule. First, we have been active in monitoring compliance. FTC staff recently "surfed" a number of children's sites, and sent an email to those sites that seemed to have substantial compliance problems, alerting them to COPPA's requirements. Second, the Commission has begun a pro-

---

[13] 15 U.S.C. §§ 6501 *et seq.* The Act 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.

[14] The rule became effective on April 21, 2000, 16 C.F.R. Part 312, and is available at <http://www.ftc.gov/opa/1999/9910/childfinal>.

[15] The FTC's August compliance clinic was held at FTC headquarters and included presentations on privacy policies and parental notices, how to obtain verifiable parental consent, and safe harbor programs under the Rule. FTC staff focused in particular on how Web sites can take advantage of the Rule's exceptions for collection of an e-mail address to provide interactive content to children. The program also demonstrated ways in which sites can identify their younger visitors by asking age in a manner that minimizes their incentive to provide false information to gain entry to the site.

gram of law enforcement against Rule violators. To date, we have filed suit against one Web site for COPPA violations, and we have a number of other investigations ongoing.[16]

Further, the FTC has undertaken a number of important and widespread educational initiatives to encourage compliance with COPPA's provisions. The Commission launched a special Web page at www.ftc.gov/kidzprivacy to help children, parents, and site operators understand COPPA and how it will affect them. Resources available on the Web site include guides for businesses and parents and "safe surfing" tips for kids. Staff has handled several hundred telephone and e-mail compliance inquiries since the Rule was issued in October of 1999, and has prepared a publication, entitled COPPA FAQs, to answer more than 50 of the most frequently asked questions about COPPA and the new Rule. FTC staff also is working with staff of the Department of Education to develop educational materials for schools about COPPA and online safety and has partnered with the private sector to help with outreach efforts.

The Gramm-Leach-Bliley Act

On November 12, 1999, President Clinton signed the Gramm-Leach-Bliley Act ("GLBA") into law.[17] Subtitle A of Title V of the GLBA ("Disclosure of Nonpublic Personal Information") requires a financial institution to disclose to all of its customers the institution's privacy policies and practices with respect to information it shares with both affiliates and nonaffiliated third parties and limits the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties. Specifically, it prohibits a financial institution from disclosing nonpublic personal information about consumers to nonaffiliated third parties unless the institution satisfies various disclosure and opt-out requirements and the consumer has not elected to opt out of the disclosure.

The GLBA's financial privacy provisions require the Commission, along with the federal banking agencies[18] and other federal regulatory authorities,[19] to prescribe such regulations as may be necessary to carry out the purposes of the financial privacy provisions of the GLBA. On May 24, 2000, the Commission published its GLBA Final Rule.[20] The Rule takes effect on November 13, 2000. In recognition of the range of financial institutions covered by the Rule and the extent of system-wide changes necessary for compliance, as well as concerns about consumer confusion, the Commission extended the deadline for full compliance by financial institutions and other persons under the Commission's jurisdiction from November 13, 2000, to July 1, 2001.[21]

The GLBA also obligates the Commission to promulgate a rule requiring financial institutions to safeguard their customer records and information. On September 7, 2000, the Commission issued a notice and request for comment pertaining to development of its Safeguards Rule in the Federal Register,[22] to garner public input concerning the safeguarding of consumer information by the wide range of financial institutions subject to the Commission's jurisdiction. After comments are received, the

---

[16] On July 21, 2000, the Commission filed an amended complaint with the U.S. District Court in Massachusetts alleging that Toysmart.com, an online toy retailer, collected personal information from children in violation of COPPA, and had offered to sell its customer list to the highest bidder notwithstanding statements made in its privacy policy that it would never share customer information with a third party. As evidence of the COPPA violation, the Commission alleged that the site collected names, e-mail addresses, and ages of children under 13 through its Dinosaur Trivia Contest without notifying parents or obtaining parental consent. *FTC v. Toysmart.com,* 00-CV-11341-RGS (D. Mass. filed July 21, 2000).

[17] Public Law 106-102, codified in part at 15 U.S.C. 6801 *et seq.*

[18] Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), and Secretary of the Treasury.

[19] National Credit Union Administration (NCUA) and Securities and Exchange Commission (SEC).

[20] 56 Fed. Reg. 33646. The Rule is codified at 16 CFR Part 313. The Federal banking agencies jointly published final regulations implementing the GLBA privacy provisions on June 1, 2000 (65 Fed. Reg. 35162). The NCUA and SEC published similar rules on May 18, 2000 (65 Fed. Reg. 31722) and June 29, 2000 (65 Fed. Reg. 40334), respectively.

[21] Section 505(a)(7) of the GLBA provides that the Commission has jurisdiction over financial institutions not subject to regulation by either other federal agencies listed in footnotes 17 and 18 above or state insurance authorities. It also assigns the Commission authority to enforce the GLBA against "other persons" who receive protected consumer financial information covered by the GLBA. The broad scope of the Commission's jurisdiction is discussed in detail at the outset of the Federal Register notice (65 Fed. Reg 33646, 33647), which analyzes 16 CFR 313.1, the "Purpose and Scope" section of the Commission's rule.

[22] 65 Fed. Reg. 54186. The comment period is now scheduled to close on October 24, 2000.

Commission will publish a Notice of Proposed Rulemaking, review comments received in response to that Notice, and issue a Final Rule.

Comments

The Commission has also shared its expertise in consumer privacy with other government agencies dealing with privacy issues through the submission of public comments. Recently, Commission staff submitted comments in response to the request for public comment by the Department of Justice, the Department of Treasury, and the Office of Management and Budget regarding their study of how a consumer's filing for bankruptcy relief affects the privacy of individual consumer information that becomes part of a bankruptcy case.[23] The staff comment focused on the privacy and identity theft[24] concerns raised by the collection and use of personal financial and other information in personal bankruptcy cases. The staff comment suggested that the agencies may wish to (a) consider the extent to which highly sensitive information must be included in public record data; (b) prohibit the commercial use by trustees of debtors' nonpublic data for purposes other than those for which the information was collected; and (c) evaluate the interplay between consumers' privacy interests and the Bankruptcy Code.[25]

Earlier this year, at the request of the Department of Health and Human Services ("HHS"), the Commission submitted comments on HHS' proposed Standards for Privacy of Individually Identifiable Health Information[26] (required by the Health Insurance Portability and Accountability Act of 1996).[27] The Commission strongly supported HHS' proposed "individual authorization" or "opt-in" approach to health providers' ancillary use of personally identifiable health information for purposes other than those for which the information was collected. The Commission also offered HHS suggestions it may wish to consider to improve disclosure requirements in two proposed forms that would be required by the regulations.[28]

Enforcement

The Commission has also brought three cases in the past year challenging deceptive or unfair conduct in connection with Web sites' posted privacy policies. In *FTC v. ReverseAuction.com, Inc.,* No. 00-0032 (D.D.C. Jan. 6, 2000), the Commission settled charges that an online auction site allegedly obtained consumers' personal identifying information from a competitor site and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business. In *FTC v. Sandra Rennert, et al.,* No. CV-S-00-0861-JBR (D. Nev. July 6, 2000), a group of individuals and Web sites involved in providing prescription drugs online collected consumers' personal medical information through an online consultation form in addition to billing and shipping information. The Commission's complaint alleged that defendants misrepresented the security and encryption used to protect consumers' information and claimed that the defendants used the information in a manner contrary to their stated purpose.

In another recent matter, as noted earlier in note 15 *supra*, the Commission challenged a Web site's attempts to sell personal customer information gathered pursuant to a privacy policy that promised that such information would never be disclosed to a third party. *FTC v. Toysmart.com,* 00-CV-11341-RGS (D. Mass. filed July 10, 2000).[29]

In addition to these public enforcement actions, the Commission is currently conducting numerous nonpublic investigations of Web sites to determine if their privacy policies are deceptive or unfair.

---

[23] *See* Federal Register Notice Requesting Public Comment on Financial Privacy and Bankruptcy, 65 Fed. Reg. 46735 (July 31, 2000).

[24] Identity theft is another privacy-related area in which the Commission has expertise. The Commission has implemented the Identity Theft and Assumption Deterrence Act of 1998, which directed the FTC to establish the federal government's centralized repository for identity theft complaints and victim assistance. For a description of the FTC's identity theft activities, *see* Statement of the Federal Trade Commission on Identity Theft, United States House of Representatives, Committee on Banking and Financial Services (Sept. 13, 2000) <http://www.ftc.gov/os/2000/09/idthefttest.htm>.

[25] The staff comment is available at <http://www.ftc.gov/be/v000013.htm>.

[26] 64 Fed. Reg. 59918 (November 3, 1999).

[27] Pub. L. No. 104-191, 110 Stat. 1936 (August 21, 1996).

[28] The Commission's comments are available at <http://www.ftc.gov/be/v000001.htm>.

[29] These cases follow in the footsteps of two the Commission brought in 1999. In *Liberty Financial Companies, Inc.,* FTC Dkt. No. C-3891 (Aug. 12, 1999) the Commission challenged the allegedly false representations by the operator of a "Young Investors" Web site that information collected from children in an online survey would remain anonymous. In *GeoCities,* FTC Dkt. No. C-3849 (Feb. 12, 1999), the FTC settled charges that the Web site misrepresented the purpose for which it was collecting personal identifying information from children and adults.

III. CONCLUSION

The Commission is committed to the goal of ensuring privacy for consumers and will continue working to address the variety of privacy issues raised by our increasingly information-driven society. I would be pleased to answer any questions you may have.

Mr. TAUZIN. Thank you, Mr. Chairman, and welcome.

Mr. TAUZIN. Obviously, the first question you know I am going to ask you is you gave the industry a grade in 1998 with only 14 percent posting privacy policy, and the grade you gave them was incomplete. In 1999, after 64 percent had complied with posting privacy policy, you gave the industry a B-plus for effort and a C overall. In 2000, 88 percent in your survey and now posting some privacy policy—good, bad or adequate but a privacy policy—what grade are you giving the industry today on effort and what do you give them overall?

Mr. PITOFSKY. I want to give the private sector some credit here because I truly believe that they recognize that invasion of privacy is a problem and they have worked hard to solve it. So on effort I would give them A-minus. I would say they are doing better.

Mr. TAUZIN. You are moving it up.

Mr. PITOFSKY. I am moving it up.

On overall performance, I would move that up from C to C-plus, but C-plus is not good enough to protect consumers or the Internet. But they have certainly committed financially and in terms of energy to try to improve the situation, and they deserve credit for that.

Mr. TAUZIN. When it comes to grading, let me first thank the FTC for training the GAO officials who conducted the Federal web site survey that Mr. Armey and I requested.

As you know we asked that it be done using your criteria because we felt that we wanted some sort of comparison whether it was a good one or not that it was on an equal basis between Federal sites and commercial sites do you know what grade the FTC got?

Mr. PITOFSKY. The FTC was found wanting in that report.

Mr. TAUZIN. So you were not part of the 3 percent that passed all of your own criteria?

Mr. PITOFSKY. We were not.

Mr. TAUZIN. Where were you found wanting?

Mr. PITOFSKY. Let me explain that because I think this is important.

Mr. TAUZIN. Yes, it is.

Mr. PITOFSKY. The FTC satisfies anybody's standards in terms of notice, access, and security. The problem was with choice. Let me explain why that happens.

Mr. TAUZIN. Why did the FTC not make the grade on choice? Your own standard?

Mr. PITOFSKY. Let me give you an illustration.

Mr. TAUZIN. Okay.

Mr. PITOFSKY. Congress has generously supported something we run called Consumer Sentinel, in which we gather complaints from consumers, we analyze them, we marshall them and then we share that information with other law enforcement agencies. That was the whole point of Congress giving us the money—that we would

share it with law enforcers, FBI, State AGs and so forth. I think it has been quite successful.

Now we tell people in our notice statement, if you give us the information we are going to share it with the FBI and the State AGs. We do not give them the option of saying we want to give you the information but do not share it.

Mr. TAUZIN. So you do not give them an opt out?

Mr. PITOFSKY. We do not give them an opt out. And of course we shouldn't. It would undermine the whole point of the program.

Mr. TAUZIN. You shouldn't give your web site users an opt out. Suppose I want to give the information about a complaint that I make but I do not want you sharing that. I do not want to have repercussions from someone else because I complained to you. Shouldn't I have the right to do that, Mr. Chairman, without your sharing it with people without my consent?

Mr. PITOFSKY. Remember, it is all in the notice.

Mr. TAUZIN. But you are telling me that I can't complain to you without you sharing that complaint with other people. Shouldn't constituents have a right? I give them that right in my office they can use my web site and complain to me about a Federal agency or they can complain to me about a third party business in my district, and I give them an assurance on my web site that I will not share that information with anyone else.

But shouldn't we at least give them the choice that you wouldn't share it with someone else if that is what they wanted?

Mr. PITOFSKY. I take your point, but I do think that since the whole point of gathering the information is to share it, that to allow them, to give them that choice, does not make any sense.

Mr. TAUZIN. But isn't part of your business as an FTC agency to in fact collect complaints from consumers and is that not also a good thing to do without necessarily sharing that worthy people pursuant to this act?

Mr. PITOFSKY. Let me make a more general point. Our fair information practices are designed to control the marketing sector of the economy. We are not selling anything to these folks. The FTC is not selling them books or records.

Mr. TAUZIN. I understand.

Mr. PITOFSKY. So it seems to me when you talk about choice in that context it is really a little different.

Mr. TAUZIN. I understand that Mr. Chairman, but I think you are making my point which is that in your own analysis, your own review of other commercial web sites, we hear the same complaint. That your own, if you will, methodology for examining and grading these web sites does not often make room for those kind of distinctions as to what it is being used for and whether the site for example may have a security but it does not say it has security. And therefore it gets graded down under your criteria. One of the problems that Mr. Armey and I wanted this GAO study done was exactly that. Was to I guess amplify the fact that the methodology itself is not necessarily perfect, that it has flaws and that therefore the reports that are issued by the agency are not necessarily as reliable as they perhaps should be.

I think you would say that the FTC, as an agency that is examining other sites, would want to be as good about privacy as any

agency of the Federal Government, and yet under your own methodology you fell short.

I think that makes our case about how this methodology perhaps needs to get further fine-tuned so that it does not reflect bad onsites that are really trying, that deserve the A minus for effort and perhaps even better than a C plus for performance.

Mr. PITOFSKY. Let me take your comments to heart and think about them. We did say in our response to GAO that to transpose our four fair information practices exactly intact away from the commercial area to the government area might lead to misleading conclusions. But I hear what you are saying and I would like to think about it.

Mr. TAUZIN. Yes, what we are also saying is to use that methodology on commercial sites without making room for those kind of distinctions that you make for your own site may be misleading and that is my point, but I thank you for at least considering it because obviously what you say publicly about the performance of the private sector has some real weight in the Congress and with the American public. And obviously it is important that whatever assessment you make be as clear and as precise as you can make it.

I want to first of all, finally, rather, thank you for continuing this effort. You and I have had this private discussion. I think that the FTC constantly monitoring and reporting on the progress of the industry and making cases where fraud and deceptive practices are appearing on the Internet is very good. How come only three cases if it is really that bad out there, why have you brought only three cases?

Mr. PITOFSKY. First of all, it is three cases in just this past year in which we continued this kind of program.

What we try to do is bring cases against the most egregious misconduct—we do not want to hit people for technical violations.

Mr. TAUZIN. You go after the really bad players. But again does that say something about the overall effort in the private sector that you found three egregious case not 10, 12, 20, 100 last year?

Mr. PITOFSKY. Well, I don't know, Jodie?

Ms. BERNSTEIN. If I could add something to that Mr. Chairman, among the techniques that we have tried to use, because this is a whole new area we conduct something we call "surf days" where we look at the sites all at one time, and in many of those instances instead of bringing cases against all of them we will send out a notice saying this is a new kind of inquiry on our part, do you know that you may be violating these——

Mr. TAUZIN. You are giving them fair warning sort of like a traffic policeman who gives me a warning and says you are going through a school zone, you better slow down.

Ms. BERNSTEIN. Exactly right. And then we go back maybe after 30 days and we have found a lot of them have dropped out or have corrected.

Mr. TAUZIN. So you do not have to take action.

Ms. BERNSTEIN. I think it is one way, it is a fair way and helps us get to the ones where we think we can make a difference.

Mr. TAUZIN. The gentleman from Ohio.

Mr. SAWYER. Thank you, Mr. Chairman. Let me thank our witnesses for being here. You heard my question earlier about the way in which we assure the ability of agencies to share information with one another while preserving their mutual guarantees of privacy in the information that they gather. Do you have any inside guidance that you could offer us this morning or would you prefer to answer that later?

Mr. PITOFSKY. Well, I think it is the right question. When you are talking about the government and not a commercial marketer, you want to ensure that the collection of information can serve government purposes, including the sharing of information where that is appropriate.

Mr. SAWYER. Where it is appropriate.

Mr. PITOFSKY. Yes, where it is appropriate.

Mr. SAWYER. While guaranteeing the confidentiality of information that is being shared.

Mr. PITOFSKY. Yes, and on the other hand you do not want to unnecessarily invade people's privacy. It has got to be designed to serve your mission purpose and that is what we have tried to do.

Mr. SAWYER. Do you have policies and principles which guide you in making that judgment in terms of where it is appropriate? Largely a subjective decision but one that you try to squeeze as much subjectivity out of.

Mr. PITOFSKY. Within my own agency we certainly do.

Mr. SAWYER. Can you describe those for us?

Mr. PITOFSKY. I will be glad to submit that to the committee. We probably have the most—one of the most clear and conspicuous non-obscure notice provisions that you are ever going to see.

Mr. SAWYER. It is not just notice. It is the protocols for sharing.

Mr. PITOFSKY. But nobody could misapprehend what we are going to do with this information. We also provide reasonable access and reasonable security. It is only on this question of choice which the chairman has raised with me. The tradeoff is whether we can share this information the whole program is designed to collect and share, or should we give people an opportunity to say, look, I want to complain to you, but I don't want this information going to the FBI and some States? We have cut in the direction of giving them notice as to what we are going to do with it but sharing the information for law enforcement purposes.

Mr. SAWYER. Thank you, Mr. Chairman.

Mr. TAUZIN. I thank the gentleman. Again, Mr. Chairman, let me thank you and let me for the record indicate again that you actually, your office actually trained the GAO in the survey that they collected; is that correct?

Mr. PITOFSKY. I believe that is right.

Mr. TAUZIN. And they did use your methodology in examining your agency and other agencies.

Mr. PITOFSKY. They did.

Mr. TAUZIN. And they did find that under your methodology, only 3 percent of the Federal sites surveyed met all of the criteria that your office uses to judge private sites; is that correct?

Mr. PITOFSKY. I understand that is correct.

Mr. TAUZIN. As compared to 20 percent of the private sector that met all five of those criteria; is that correct?

Mr. PITOFSKY. Yes.

Mr. TAUZIN. Is it fair to conclude that the private sector is doing better than the government sites?

Mr. PITOFSKY. No, I don't think that is fair.

Mr. TAUZIN. Tell me why.

Mr. PITOFSKY. I don't know why other government agencies have failed to satisfy fair information practices.

Mr. TAUZIN. We have got a list and it is pretty interesting.

Mr. PITOFSKY. I suspect it is often this issue of sharing the information with other agencies and not giving people the opportunity to say count me out. They say: I want to complain, I want to submit information but I don't want to share——

Mr. TAUZIN. But you know a lot of them failed because they just did not post a privacy policy. A lot of them failed because they did not give notice to consumers that they were gathering information. Some of them failed because they said they were not gathering person information and they were. Some of them failed because they had cookies. By the way what is a cookie? Not everybody knows what a cookie is. We are talking about a new cookie monster here in effect.

Mr. PITOFSKY. People have learned what it is about. It is a device that is placed on the hard drive of the computer of the person who is surfing which allows the collector of information to trace where you have been and what you are doing. I described it as like a technology that would allow your TV set to keep track of what programs you watch, what ads——

Mr. TAUZIN. Worse than that it is like having a camera follow you around for the rest of your travels all day long, all week long, perhaps for 35 years. Pretty bad stuff.

Mr. PITOFSKY. I think that is a fair analogy of what we are talking about here.

Mr. TAUZIN. And some of these—14 percent failed because they did have cookie on their site and in some cases without advising consumers.

Mr. PITOFSKY. I heard Sally Katzen say that she does not intend to defend cookies on government web sites and I am not going to step in to do it.

Mr. TAUZIN. The only point I want to make is that when you compare—we have a comparison sheet of the Federal sites, and the private sites, on every standard that you use to judge private sites, Federal sites fared worse on every standard. On the question of frequency of disclosure, 100 percent of commercial sites compared to 85 percent of the government sites. On all four principles, 42 percent of the Federal sites and only 6 percent of the high impact sites, 20 percent at random and only 3 percent of the at random Federal sites. In fact, there was only one category at all that was comparable between the Federal and the public sites—I mean the Federal and the private sites.

We have a copy of this I want to make sure that you get it. But it basically says that when your criteria was applied to the public sites where we have to share information in many cases, that privacy was less protected than in the commercial sites of America. That is not a good finding. Mr. Armey and I have asked a simple

thing of our government: Maybe we need to clean up our own house as we go by grading and commenting on someone else's house.

But again, I thank you for both cooperating with our effort to examine the Federal sites and second, for continuing your monitoring of the private sites and invite you and your staff to stay in close touch with us because I think we have all come to the conclusion that next year we are going to have to move legislatively in some of these areas.

Mr. PITOFSKY. I am glad to hear that and I do want to continue working with you and this committee.

Mr. TAUZIN. Thank you, Mr. Chairman, and we will stand in recess for another 10 or 15 minutes.

[Brief recess.]

Mr. TAUZIN. We are going to get started and anybody who misses this is just going to miss a lot of good time. The committee will please come back to order.

Let me welcome our final panel. Mr. Larry Chiang, Chief Executive Officer of MoneyForMail.com; Ms. Glee Harrah Cady, Vice President for Global Public Policy, Privada, in Sunnyvale, California; Ms. Parry Aftab, Special Counsel for Darby and Darby in New York; and Mr. Mike Griffiths, Chief Technology Officer of Match Logic Inc., and Mr. Andrew Shen, Policy Analyst for Electronic Privacy Information Center.

I apologize for the long day, but I suspect we are going to have a lot of long days thinking this business through. Part of what we are doing is building a record, so all of your written statements are part of that record. And trust me on this, members and staff actually read those statements and get into them because we are desperate for understanding here. And what you will provide for us on this panel is a little more depth of understanding about what is happening in the marketplace of privacy and the technology and the private sector.

So let me please welcome you, and we will begin with Larry Chiang, MoneyForMail.com. Welcome.

STATEMENTS OF LARRY CHIANG, CHIEF EXECUTIVE OFFICER, MONEYFORMAIL.COM; GLEE HARRAH CADY, VICE PRESIDENT FOR GLOBAL PUBLIC POLICY, PRIVADA; PARRY AFTAB, SPECIAL COUNSEL, DARBY AND DARBY, P.C.; MIKE GRIFFITHS, CHIEF TECHNOLOGY OFFICER, MATCH LOGIC INC.; AND ANDREW SHEN, POLICY ANALYST, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. CHIANG. Thank you, Mr. Chairman. Thank you, members of the subcommittee. I come to you as a person who is on his second business. I am an entrepreneur. My background is in engineering, so I am fortunate to head up a very popular company called MoneyForMail. This is my second company. My first company was one that sold credit cards to college students. And my efforts in starting new businesses is to empower consumers to control and empower them both on two fronts, both on credit understanding and an understanding on privacy.

And what MoneyForMail does basically in a little nutshell is it empowers consumers to opt in their information so that they control their own information so that the people that previously com-

piled and sold information to companies such as Trans Union, Equifax, Experian profited by selling this data.

Mr. TAUZIN. Give me an example of how that works.

Mr. CHIANG. For example, let's say you are a car leasing company and you want to sell cars to people in their middle 20's that have a good job with good credit. So you can send a prequalified lease to those people using credit data. Now, a consumer today and up until the past 20 or so years has not been able to control their own data. So if a car leasing company wants to buy that information and extract that information from the three credit bureaus, they are able to do so without knowledge and consent of a consumer.

Where you are now bringing forth a number of these privacy issues also then starts to question previous legislation on the Fair Credit Reporting Act with who exactly owns and controls pieces of credit data.

So what MoneyForMail tries to do and does successfully is it compiles credit data along with demographic data so the demographic data is information that gets collected on different surfers and their preferences, their gender, what State they live in, maybe even some detailed information as to what sports they like to watch or participate in.

What we do with that demographic data is we add in credit data so that advertisers now have more pieces of the information to then collect this information and then send out advertising messages that are geared toward it.

To backtrack a little bit, the reason all of this is such a large issue is simply because advertisers know that when they spend money, 50 percent of that money is simply wasted. Now the question is what 50 percent did I waste? With the Internet you are allowed to target specifically demographics of your advertising, let's say men's suits from a previous example, target men's suits, advertising solely to men that are prepared to buy a suit, whereas previously you are just shotgunning that advertising message to everyone. So the Internet as a medium allows that.

That is why this issue is going to balloon further because how many billions of dollars are spent on advertising and how many of those billions of dollars could potentially not be wasted should there be a better methodology in sending out these types of messages.

It not only permeates the Internet, where, yes, it is personalized content, but in the future you will talk about cable TV advertising. Right now everybody in certain markets gets the exact same advertisement. What if you opted in your demographic data and were able to control your own demographic data and then the cable TV companies can send you specific ads based on your needs, your usages, your preferences?

So the situation that I come to you today with is, No. 1, the parallel nature of how credit data previously was compiled without regulation, and how the Fair Credit Reporting Act obviously is legislating and regulating the three bureaus in compiling this data to also then translate that where the FTC regulates that data. I see a parallel where the FTC also similarly will further regulate privacy issues in a simple, easy to use, easy to understand principle.

Whereas right now if you visit a lot of these web sites you are faced with pages, literally pages where you have to scroll down, and how many users actually read and understand the privacy statement?

What I think in the future is you are going to be allowed to go to something similar to a Schumer box where some of these ideas that I bring forth are not really necessarily my own ideas but based on historical regulatory ideas. How the Schumer box then translates to privacy is maybe in five major points, similar, an annual fee, interest rates, terms, and junk fees, a privacy policy box or someone's name box then can therefore disclose the five major points or six major points for how it is that you as an Internet web surfer can then be assured of some type of standardized policy.

[The prepared statement of Larry Chiang follows:]

PREPARED STATEMENT OF LARRY CHIANG, CEO, MONEYFORMAIL.COM INC.

I. INTRODUCTION

Mr. Chairman and Members of the Subcommittee:

Good morning. I am Larry Chiang, CEO of MoneyForMail.com in Palo Alto California. I welcome this opportunity to comment on the current state of Internet privacy and the impact of compiling consumer data for consumers and businesses.

I am here to testify on what I believe are reasonable standards for promoting consumer safety for those who use the Internet, and to report to you the efforts my company has taken to help consumers "take back" their personal information.

The comments and views expressed in this Statement are offered in my capacity as CEO of MoneyForMail.com, and my experience in dealing with privacy and credit issues since 1989. I will discuss:

- Economic benefit of matching surfing data with "real world data"
- How these combined data files may be abused
- Potential discrimination using today's technology
- How privacy issues tie into Fair Credit Reporting Act
- Future trends of consumer demographic collection
- Pending privacy scandals

I believe strongly that you, the members of Congress, will play a critical role in shaping legislation that will enhance privacy by expanding and strengthening the consumer's right to control his or her own own personal information. I appreciate the opportunity to share my views on that topic.

II. ECONOMIC BENEFIT IN MATCHING SURF DATA WITH "REAL WORLD DATA"

Advertisers are willing to pay for advertising that better targets an audience. The medium of the Internet naturally lends itself to specifically targeted ad messages for users groups as small as one person.

Internet advertising agencies can earn a premium by matching online demographic data and "surf pattern" data with "real world" data. Surf data is the tracking of user movements from web site to web site. Real world data is purchasing history, club memberships, newspaper and magazine subscriptions and credit-related data.

By "spooling up" banner ads to a person visiting particular web sites, the real world data serves as a qualifier of purchasing power and offline interests.

III. HOW THESE COMBINED DATA FILES COULD BE ABUSED

Two particular industries have definite potentials for abuse: credit and insurance.

Say a web surfer visits a Las Vegas Hotel site and his combined profile dictates that he visits Vegas three times a year. An insurance company underwriter may find that behavior tends to increase the likelihood of filing a fire insurance claim. Therefore, the insurance applicant may be rejected for fire insurance because of the Las Vegas visits. Now take this example and apply it to breast cancer sites, Bible study sites, scuba diving sites—and the potential to abuse privacy is very likely.

While this may sound far-fetched, is it unreasonable to assume it could not happen? I don't believe so. After all, who would have guessed ten years ago that your credit record—a report of how you've managed your bills—would be a better predictor of how many insurance claims you would file than your driving record? Yet

today a number of insurance companies rely on credit records when evaluating insurance applications.

Combined data files put more information into everyone's hands. While it may seem innocuous for a web site that sells BBQ grills to sell surf information to Midwestern beef houses, the consumer needs to control and know what data files are being used and distributed.

IV. POTENTIAL DISCRIMINATION USING TODAY'S TECHNOLOGY

Since web sites can be made dynamic to each and every particular web user, certain collected data files could be used to discriminate against consumers.

For example: access to low-cost mortgage rates could be kept from those individuals that have an online surf pattern of perpetually visiting job listing boards. The mere act of visiting a job listing board could signify job instability. Or, an insurance company could determine that people that purchase adventure gear (ski equipment, sky diving supplies or mountain climbing ropes) are not a good risk. These are the types of discrimination that are made possible using technology available today.

V. HOW PRIVACY TIES INTO THE FAIR CREDIT REPORTING ACT

Nearly thirty years ago, Congress enacted the Fair Credit Reporting Act to protect consumers' credit reports. Your predecessors realized that this information played an important role in consumers' lives, and that people should have the right to review their reports and challenge their accuracy. In addition, Congress acknowledged that this sensitive information should be available for limited purposes.

Today we are beginning to see interesting overlaps between companies that collect credit data and companies that collect other data about consumers. Experian, one of the major credit reporting agencies, owns 19.9% of MyPoints.com and 6.4% of AdForce. Both are companies that derive the majority of their income from Internet advertising.

Is it such a stretch, then, to ask Congress to consider regulating Internet data collection just as it did credit data? Or is it unreasonable to ask the FTC to oversee these practices as it does the credit reporting agencies?

VI. FUTURE TRENDS OF CONSUMER DEMOGRAPHIC COLLECTION

The holy grail of advertising has always been getting the right message to the right person. The complaint of advertisers has been, "I know I am wasting 50% of my advertising dollars, I just don't know which 50%." Collecting Internet demographic data and marrying it with real world data will only increase as advertisers try to narrow their targets.

VII. PENDING PRIVACY SCANDAL

Right now the pieces are in place for a number of privacy scandals.

In Silicon Valley, you have (1) young CEOs—some in their 20's—(2) heading up cash-strapped companies, (3) oblivious to privacy concerns, and (4) controlling private information worth a great deal of money. These ingredients up the likelihood of a privacy scandal which will negatively impact e-commerce.

VIII. CONCLUSION

It is my opinion that Congress should act now to establish guidelines for the collection and use of personal data on the Internet. At a minimum, consumers should be told what information will be collected when they visit web sites, what it will be used for, and steps they can take to ensure their privacy. The Federal Trade Commission should be given regulatory authority to ensure privacy, and to protect consumers' rights.

Mr. Chairman and members of the Committee, I hope this overview has been helpful for you. If you have any questions, I will try to answer them.

Mr. TAUZIN. Thank you very much, Mr. Chiang. Now we welcome Mrs. Glee Harrah Cady, the Vice President for Global Public Policy of Privada.

STATEMENT OF GLEE HARRAH CADY

Ms. CADY. Thank you, Mr. Chairman. It is a pleasure for me to be here today to talk to you, not only about what my own company

does in privacy enhancing technologies but what our industry is doing as a whole.

Privada itself is based in Sunnyvale, California, and we build privacy infrastructure systems for financial service companies, for network service providers and for other people who, in turn, would like to offer privacy services to their customers. You may have seen a recent series of advertisements on the television by a large credit card company that is going to be partnering with us in future products, and we expect to have further announcements like that.

Generally, technology is quicker than legislation. I know this point has been made to you a number of times. And we can today provide help to your constituents and the people who are genuinely concerned about a genuine problem with technologies that will assist them to protect their privacy while the debate goes on here in the Congress.

Since early this year, I think there has been something like 700 different announcements made about privacy enhancing technologies, and of course we are all terrific. Mr. Boucher and Mr. Goodlatte mentioned today the Internet Caucus and earlier this year, in fact just 3 weeks ago, we were privileged to be part of a privacy technology fair. And I know that this little booklet has been added into the record so that people can see who demonstrated there at that time.

Finally, we have this lovely poster that we have also provided you that was developed by the privacy leadership initiative. There are more of these in the back of the room for those in the room who would like to have that. It is a description of some people and their technologies that are in the market today.

Today, not next Congress, not tomorrow, not next week. So these technologies range from companies who provide complete anonymity all the time to people who are occasionally called infomediaries who will broker information on your behalf. Choosing among them might be complex at this point, but they are all there. I have tried to provide links to lists of these technologies in my written testimony, and I would urge you to encourage your constituents to look at these pieces of information, and if anybody has any questions about specific technologies or what any of the companies can do to help them, I would be happy to answer them.

Thank you.

[The prepared statement of Glee Harrah Cady follows:]

PREPARED STATEMENT OF GLEE HARRAH CADY, PRIVADA

Mr. Chairman and members of the committee, thank you for the opportunity to discuss the progress that technology companies have been making in the development of privacy enhancing technologies to protect consumers.

My name is Glee Harrah Cady and I work for Privada, Inc,[1] a Sunnyvale, CA based company that builds comprehensive privacy solutions. We deliver those solutions through Network Service Providers, financial institutions and other digital enterprises. By building a virtual "curtain" between the user and the Internet, Privada gives users control over the dissemination of information about themselves. Our services make it possible for businesses to offer privacy-based services to their customers.

Our current partners (which include American Express, Cisco, and Portal) will integrate Privada's privacy protection into products that meet their customers' need for digital privacy. Our joint commitment to providing sound and robust digital pri-

[1] The Privada website may be found at http://www.privada.com

vacy will ensure that individuals maintain choice and control over their personal information.

Privada works with other technology and consumer product and service companies in trade associations and coalitions to inform and educate policy makers, press, and individuals about digital privacy. We are members of the Commercial Internet eXchange Association, the Internet Alliance, the Information Technology Association of America, the Online Privacy Alliance,[2] the Software and Information Industry Association, the United States Council for International Business, and TechNet. We support the efforts of the Privacy Leadership Initiative. And we were pleased to be selected to participate in the recent Privacy Technology Fair sponsored by the Internet Caucus.

Today's privacy debate has been fueled by two very opposing views—one side advocates exploitation of personal information for any and all purposes, and the other wishes to prohibit the use of personal information for any and all purposes. As the debate acknowledges, we fear intrusion into our private lives by both government and business. We all want the benefits of personal services but fear the possibly unpleasant surprise of someone we don't know knowing too much about us. This is why digital privacy is so important to us. With Internet access we have grand opportunities to gain knowledge, improve communication, and have products and services delivered to us wherever we are, whenever we want them. But we know we are being watched and we don't like it

Each day, too, individuals become more aware that they need to think about the business behind the website. Who are these people and what are they doing? We hope that the Platform for Privacy Preferences (P3P) will be a language used by all to make finding and understanding a privacy policy easier, so that the "who" and "what" questions are answered. Rick Jackson, Privada's CEO, frequently says that as consumers we also should look to see how a company is making its money. A company's revenue source most often tells us what is important to the company and its investors. With that information, we can determine how the company values us as consumers and customers—whether we are customers or information assets.

The polls illustrate that increased sales and larger numbers of repeat customers are a likely consequence of strong privacy policies and more individual control over personal information. A sponsored survey by research firm IDC (released on Monday of this week) found that consumers are concerned about the sharing or selling of personal information collected during online purchases. Almost 60% of the respondents were concerned that Web sites will share or sell information about them. The press release announcing the survey also reported that 91% of the respondents value privacy management tools and services that assure protection of personal information when making online purchases. This survey echoes the words of SIIA's 2000 Report on Trends Shaping the Digital Economy.[3] The chapter on "Customer Empowerment" shows that the customer, who has always "been right", now has new ways to interact with the vendor and those ways are increasingly automated and increasingly personalized. SIIA recommends that retailers planning to use technology to advance remember to combine airtight privacy policies with business models that defer to customer empowerment. Those businesses that do not place customer service above all else will fail. The report also notes that, on the Internet, it is very, very easy for an unhappy consumer to find another store selling the same or similar products almost instantaneously—and tell all their friends when they do.

Companies like Privada are happy to hear that individuals want to control the distribution of their personal information and that people want to receive the marketing advantages that accrue from smarter business marketing. American consumers want great deals without junk mail and personalized service without telemarketing calls. Privada provides a privacy infrastructure where building such services is possible: you can get what you need without unknowingly releasing personal information. Privada systems support reasonable uses of personal information by providing online identities that are separate from your real world identity. Your online identity, not your real one, will be the recipient of any personalized services you choose. And you don't need to give up any information that you don't wish to release. Privada-based services support the points of both sides of the privacy debate by allowing the enjoyment of the benefits of the information economy—keeping it moving and expanding to benefit even more people—with no compromise of personal data.

Privacy is an intensely individual matter. The choices I make about my personal information will not necessarily match yours. For example, I don't mind if you know

[2] The Online Privacy Alliance is on the web at http://www.privacyalliance.org

[3] The Software and Information Industry Association Report on Trends Shaping the Digital Economy is at http://www.trendsreport.net/customer/1.html

that I am a proud parent—if you give me a chance I will certainly boast about my wonderful children. But in fear of predators, some people don't want others to know they have children. I don't mind if you know what kind of car I drive—certain of my friends say that I sound like a car commercial. Others don't want you that information available unless you are the car manufacturer and there is a product recall. I don't want you to have access to my financial information unless I give you that permission so you can help me with a financial transaction. I don't want intimate details of my medical records in the public domain. Unless I know you well, I am unlikely to share a list of the email addresses of my fellow Privada employees. Email addresses of public employees, however, are frequently readily obtainable.

Because we don't yet have concensus about privacy among individuals, businesses, and government, and because the technology is changing almost daily, governmental solutions necessarily lag behind. Laws take an even longer time than computer programs to define, construct, test, and implement. Here is where technologies play a significant role. While committees like this one strive to determine the best way to provide legal protection, technology can provide tools for individuals to use to protect themselves. With each of us in control of our individual information, the rewards of the digital economy can reach more people. This is a win for individuals; for business, with more consumer confidence; and for government, with one less area to track. Privacy enhancing technologies can benefit everyone.

Today there are many and varied technologies designed to provide differing types of digital privacy protections to individuals. The available products and services range from complete digital anonymity services to products that broker your information on your behalf. The recent Internet Caucus Privacy Technology Fair[4] in the Capitol invited 19 different companies to show their technologies. The Privacy Leadership Initiative has listed 27 technological tools on a poster entitled "Privacy Technology in the Digital Age, Version 1.0". The Information Technology Industry Council's Digital Frontier[5] site mentions 29 different privacy enhancing technologies (not including ours, so I guess I am going to have to call them up and tell them about us). "Know the Rules, Use the Tools,"[6] is a 31-page handbook developed by Majority Staff of the Senate Judiciary Committee at the request of Senator Orrin Hatch and first released at the Internet Caucus event.

Some products help other businesses construct understandable, and machine-readable, privacy policies. Some services allow individuals to purchase items over the Internet as anonymously as if they were using cash. Some are tools to install on an individuals own computer (client-based tools); others are tools that individuals access through the Internet (server-based tools); and still others are combination tools that use a client program to initiate the protected transmissions. Some technologies provide for web-browsing without leaving tracks that are individually-identifiable. Some provide anonymous communication. Some manage your many account passwords and release only the information the individual has specified. Since the Internet Caucus Technology Fair just three weeks ago, several new privacy technology companies have launched and respected technology companies have released new privacy products. We at Privada can see that the privacy business is becoming more competitive each day.

On the Internet there are so many different ways to gain access, to present items for sale, and/or to search for information: supported by advertising, bid for in auctions, pay-per-use, subscriptions. Many companies are searching for the right business model to provide services just as individuals are searching for the right mixture of tools, effort, time, and money to use those services. Here in Washington, legislative and administrative policy makers are seeking the right mixture of consumer protection and business encouragement, one that doesn't encourage irresponsible businesses nor penalize those who are striving to find new ways to deliver their products. Sometimes the discussion has centered on legislating a particular method of consumer choice (opt-out versus opt-in). Sometimes the discussion has focused on a particular delivery vehicle (the World Wide Web). Someone usually points out that not all Internet sites are in the United States (nor do we want them to be) so that laws would not reach all potential sites. And clear and conspicuous notice isn't as easy as it sounds. Privacy enhancing technologies can be used for protection while the discussions continue. This means that protection need not wait until we all agree on what constitutes legal protection.

---

[4] The listing of companies demonstrating technologies at the Internet Caucus Privacy Technology Fair is at http://www.netcaucus.org/events/privacyfair.shtm

[5] The Information Technology Industry Council Digital Frontier paper on Personal Privacy Solutions may be found at http://www.itic.org/digital—frontier/consumer/intro.html

[6] The Senate Judiciary Committee booklet may be found at http://judiciary.senate.gov/privacy.htm

What you on the committee can do today is to help us spread the word. When your constituents voice their fears in your town hall discussions, tell them how to find help. If they are already on the net, you can point them to one of the links I've included here. If they are not on the net, I'd be happy to help them find a service that meets their needs. Have them call me. Let's not leave anyone out.

Thank you.

Mr. TAUZIN. Many of these are free; right?

Ms. CADY. Yes, sir, many of them are free.

Mr. TAUZIN. Now we will hear from Ms. Parry Aftab, Special Counsel for Darby and Darby, New York.

STATEMENT OF PARRY AFTAB

Ms. AFTAB. Thank you, Mr. Chairman, and thank you for inviting me to testify here today. I am a privacy lawyer. I specialize in the children's industry, and I am often called the kid's Internet lawyer. But about half of my time is also spent running nonprofits. I run Cyber Angels, the largest Internet safety and health group in the world, and Wired Kids. I am also the author of the parents' guide to protecting your children in cyberspace. And my testimony will be a blend of both my expertise as a privacy lawyer and my advocacy for children.

Mr. TAUZIN. This is the book that you are talking about?

Ms. AFTAB. It is, Mr. Chairman. Thank you very much.

There are roughly 25 million children online in the United States. These are children under the age of 18, and there are web sites that are very valuable to children that can help them with education, give them games. They can be very entertaining. Children can have web sites where terminally and seriously ill children can communicate with each other and talk to children around the world.

We are here to talk about problems, but I would like all of us to remember that the Internet is a wonderful place, especially for children, and the greatest risk our children face in connection with the Internet is being denied access.

And no one cares more about children than the children's Internet industry, except perhaps the FTC, who I would like to compliment during my testimony here today for being always available, always listening and always trying to help the Internet industry as a whole. They are willing to speak at all of the conferences. They are willing to do many things, and in fact today I bear an invitation from the government of Singapore for the FTC to come and teach them about regulating privacy in the area of children.

But there are serious problems that the children's Internet industry is facing. This morning on Good Morning, America they talked about "dot gone," and problems with the Internet industry generally. The children's Internet industry is facing even greater problems because they have no generally accepted viable business model. Advertising is not working because children are not directly engaging in e-commerce. There are lots of problems in this area and one of the things we need is more flexibility on the part of the FTC to have greater discretion and exception under COPPA.

Today there has been a lot of discussions about parental consent. One of the biggest problems that we face is that parents, although they want their children to do these things, are not taking the time to actually give the consent to the web sites. And the choice is then

locking children out of these interactive tools. It is not merely a matter of children sharing personally identifiable information; it is a matter of whether they can send e-postcards or whether or not they can get a picture from Elmo. And it is important that we get parents involved in finding compelling reasons for them to be using the Internet.

We need several things that Congress, especially this subcommittee and your expertise, can help us with. No. 1, we need research on how children are actually using the Internet. We need research on what parents really want and what it will take to get them to be active in the kid space. We also need educational programs teaching children how to surf the Internet safely, how to use the best filter that exists, which is the one between their ears, Mr. Chairman, and teaching them how to use critical judgment when they are communicating with strangers online.

We also need to give flexibility and discretion to the FTC in carving out exceptions or special rules under COPPA for companies that put children's safety and privacy first forward innovation rather than putting extra strain on the industry. What we need to do is work together to make sure that the expertise that each of us brings to the table is used to help children, to help the Internet industry and to help everyone preserve their privacy and keep children safe at the same time.

We are also creating the children's Internet industry trade association. It is called KITA, the Kids Internet Trade Association, to help members of the kids Internet industry to come up with solutions and work together and work together with regulators and legislators on coming up with solutions that work. The greatest problem we have in the area of privacy is unexpected consequences when legislation has not been as thoroughly thought out as the chairman has been looking at here.

So I welcome the ability to help in any way that I can at any time, and thank you very much.

[The prepared statement of Parry Aftab follows:]

PREPARED STATEMENT OF PARRY AFTAB, SPECIAL COUNSEL, DARBY & DARBY, P.C.

SNAPSHOT OF THE CHILDREN'S INTERNET INDUSTRY

There is no more exciting or rewarding industry than the children's Internet industry. Where else can you have fun, help children and change the world at the same time? When you deal with children, safety, quality content and privacy are good business. Parents are partners in this. But, as exciting and potentially rewarding as it is, the children's Internet industry is facing many challenges, these days, and they need help from both within the industry and from regulators, in order to face those challenges and make sure that what's best for children is always foremost.

Who are the players? The children's Internet industry is largely dominated by U.S. sites. They typically fall into three categories, (i) large, well-recognized leaders in children's entertainment and media, such as Disney (disney.com), Viacom (Nickelodeon, nick.com, and nickjr.com, and MTV, mtv.com), Fox, PBS (pbs.org/kids), Sesame Workshop (the new name for Children's Television Workshop—Sesame Street, sesamestreet.org), Sports Illustrated (sikids.com), Nintendo (nintendo.com), and Cartoon Network (cartoonnetwork.com), (ii) new players to children's media, which came from the Internet, as opposed to traditional entertainment media, such as Surfmonkey (surfmonkey.com), MaMaMedia (mamamedia.com), Freezone (freezone.com)), Bonus (bonus.com), Alfy (alfy.com and cleverisland.com), Zeeks (zeeks.com), Lycoszone (Lycos's kids site, lycoszone.com), Yahooligans (Yahoo's kids site, yahooligans.com) and, until recently, Headbone (headbone.com), and (iii) sites that are linked to educational services, media and products, such as Chancery Soft-

ware (k12planet.com), Discovery Channel (discoverykids.com), Scholastic (scholastic.com), Weekly Reader (weeklyreader.com), National Geographic (nationalgeographic.com/kids), Princeton Review (homeroom.com), Big Chalk (bigchalk.com and homeworkcentral.com) and ePALS (epals.com, a penpal service for schools using e-mail rather than traditional postal mail).

How do they operate? Generally the children's Internet industry operates on a B to C business model. That means they are businesses delivering services to consumers. Essentially they offer kids content, games and interactivity to children. Most sites are free. Some sites require that children register to be able to access certain content and services. That registration may require personally identifiable information and therefore parental consent under the new children's online privacy law, The Children's Online Privacy Protection Act ("COPPA," described later in this testimony and the appendix), but many only require that a child inputs a user name (using anything they want) and password. Some sites operate on a subscription model, charging parents, sponsors and in some cases even parents' employers (see Kids Online America, kola.net), for subscriptions to special services and content for children.

But B to C models have fallen into disfavor with the venture capitalists, recently. Therefore, some children's Internet industry members have recently changed their model (or gone back to their original models) to a B to B model, offering their services to other businesses, even within the children's Internet industry itself. Most notable among these is, perhaps, Surfmonkey (surfmonkey.com) which started out as a technology company, specializing in browser technology and content management. When the market (and venture capitalists) cried out for portals, it repositioned itself as a children's portal, providing content, branded media and interactive features to children. It's now designing a special browser that provides content management to preapproved content, allowing parents to select content filters, and manage their children's access to chatrooms, instant messaging, e-mail and other interactive tools and even their time online. This is being offered to other children's sites to allow them to have interactive communities, without having to jump through the regulatory hoops.

THE CHILDREN'S INTERNET INDUSTRY IS FACING DIFFICULT TIMES.

Last month, there was an industry-wide conference for members of the children's Internet industry. A representative of one well-known children's site commented to a panel (that included me) on COPPA compliance in the kids Internet industry. This woman stated that if you are involved in the kids space, your primary obligation is safety and privacy. She said that all children's sites need to be obsessed with safety and privacy of their site visitors. A representative of another well-known children's site stood up, and said although they cared deeply about online safety and privacy for children, they were "obsessed" with the bottom line.

I have never heard a comment repeated within the industry as often as this response. That's because it spoke to the hearts of all members of the children's Internet industry. While most of the industry is focused on online safety and privacy and doing what's right for children, many have forgotten to stay focused on staying in business. There are several solutions for this, and no one area to blame. One essential solution is to educate sites on business models and help them work with others to stay successful. In response to this, we are forming the first children's Internet industry trade association, to operate in alliance with an existing umbrella non-profit dedicated to children's equitable access, education online resources and safety and privacy issues, WiredKids.org. This organization is creating KITA, the Kids Internet Trade Association, to help sites address these issues, learn what they need to know to keep their businesses operating and help them network with others within the industry and government on these issues. It will include filtering companies, ISPs, technology companies, educational services, content providers, media providers and others involved either directly or indirectly with this industry. But although a help to the sites, this will not address all of the issues faced by the industry.

Problems faced by the Children's Internet Industry: While children are online more and more (roughly 25 million in the U.S. alone under the age of 18), few children's sites have been able to find a single business and revenue model that works in the kids space. (Children's sites for the purposes hereof are directed at children and preteens.) While children may be loyal site visitors, parents aren't supporting the industry in sufficient numbers. The key to success of the children's Internet industry is to get parents to understand the value of their children's online activities, and support them.

Most sites in the kids space are using a combination of several revenue models that are helping them stay afloat until parents find a compelling reason to support

the children's Internet industry. (This will come over the next few years with the delivery of educational services, games, videos, online music delivery and new media and programmable toys that can only be programmed online.) When we can find the model that parents find compelling, the kids space will be very successful. But during this interim period, between the earlier excitement over the children's Internet industry and finding the right revenue model and what parents find compelling, the industry is facing hard and lean times.

This makes the industry particularly vulnerable to other factors and outside influences. Prime among outside factors are: tech and Internet stocks are down, the IPO market for the Internet industry has slowed, and the venture capitalist money in the Internet space has been drying up or directed at currently profitable e-ventures, generally, Many sites that were planning on rounds of financing after February, 2000, found themselves without funding because of the market downturn last Spring. Several proposed mergers and combinations that involved some of the kids space leaders fell through, causing these sites to waste months and even years in discussions. Time that would have been better spent, in hindsight, developing revenue models and maintaining their dominance in the space.

In addition, being involved in kids content development and delivery is very costly and particularly time intensive for sites other than Disney, Fox, Nickelodeon and the like, whose business is the development of content online and offline for children. Couple this with the high cost of maintaining a safe site for children (with moderators in chatrooms and oversight of what the children are doing and posting at the site), confusion over the years as to what the market needed (largely driven by the venture capitalists) and the speedbumps caused by regulations make it very difficult and costly to operate a children's site and it's no wonder many are struggling to stay afloat. Some wonderful sites have already lost and are losing that battle.

While many are now blaming the FTC and COPPA, however, this isn't fair and isn't a true reflection of the situation. It is a complicated combination of factors that is making the life of a children's Internet site precarious. Since many of these factors came to bear after the March downturn in the market, and COPPA came into effect in April, COPPA is an easy target for blame. But there is no *one* culprit here. And if there is, it isn't COPPA. COPPA plays a role in the problem, but more as a result of parental lassitude and in the lack of flexibility and discretion given to the FTC to administer COPPA and provide carveouts for other safe models.

There are seven issues that are creating special challenges for the industry: (i) no clear revenue model has been generally identified as working for the kids Internet industry, (ii) parents say they care about children's online safety and privacy, but aren't taking the time and effort to do anything about it and are unwilling to pay for most online content, (iii) the venture capitalists, angel funding and public security markets have become more cautious since the Spring 2000 downturn of the Internet markets, (iv) content development is very costly and time-consuming, (v) children are not candidates at this time for viable e-commerce and direct purchasing online, (vi) parents are often unwilling to use credit cards and other adult verifiers online, without a compelling reason to do so, and (vii) regulations pose difficulties when preteen-interactivity is involved, which decreases traffic, which further decreases the likelihood of obtaining financing. Each of these points, either individually or in combination with one or more of the other points, is examined below.

No generally identified business and revenue model exists yet for the children's Internet industry: Currently the children's Internet industry is struggling to discover a viable generally-applicable business model for supporting children's content and features online. At this time, most are using a combination of revenue models to support the high cost of maintaining entertaining and fresh content for children and preteens. Some good sites, which children enjoyed and parents approved of, have been unable to survive during this difficult time for the children's Internet industry. Even the ones that have survived the downturn on e-commerce and Internet investments, the falloff of the IPO markets, the high costs of safety and privacy safeguards and legal compliance, and the lack of parental enthusiasm and support, are struggling to find a viable and consistent business and revenue model.

Advertising: Advertising, while a portion of most site's business models, isn't able to support the costs of maintaining children's online content. Advertisers are currently seeking a new interactive model for Internet-based advertising that may be more effective with children, but the advertising typically used (click-thru banners) isn't producing the results advertisers are seeking. This will, hopefully change. Children, while capable of influencing offline and online purchases, are not yet participating in e-commerce. This both affects the advertising rates and the ways in which advertisers are willing to work with children's sites.

E-Commerce: Children, for the most part, don't purchase products online. They research products and services, but are not purchasing them online. Teens are starting to become an e-commerce force online, but this has not extended to children and preteens. Children and preteens influence offline spending of their parents in large amounts, however. While a few kids e-commerce sites exist (relying largely on the gift registry and gift certificate concept, such as iCanBuy.com, RocketCash.com and doughNET.com), this isn't generally a standalone viable business model at this time for the children's Internet industry, either. E-commerce for children isn't compelling enough yet for parents to support in large enough numbers. This will change over the next few years when services and products that children want most are only available online (such as programmable toys, computer games and, to serve the desires of parents, educational services; for an example, see Homeroom.com, offered by Princeton Review).

Sponsorship: Sponsorship is a business model used by many children's websites during the last few years. Some use it to handle the costs of a particular feature or section of their own site. Others use it to design sites for other companies. Some large brick and mortar, offline corporations have paid for the development of special sites directed at children. Fleet Kids (designed by Headbone, one of the saddest casualties of the children's Internet industry) is a notable example of how the offline industry can join forces with the children's Internet industry to develop educational and entertaining resources for children. But, the revenues raised through sponsorships are generally insufficient to defray the costs of running an entire children's site. Some notable specialists in the area of kids website designs for other companies are Media Jelly, which designed the Magic School Bus site for Scholastic and Goosebumps, among other award winning sites (www.mediajelly.com), and Zeeks (formerly a popular child portal and now using their expertise to create sites for others).

Marketing and Collecting Data: One model many general audience sites use is collecting marketing and demographic information about site users. They may have site registrants provide personal information, such as income, occupation, educational levels, addresses, telephone numbers and e-mail addresses and pair this with their surfing practices, marketing preferences and buying practices. Many members of the children's Internet industry had been collecting personally identifiable information from children at their site. When parents learned about this, they reacted strongly. This is one of the abuses COPPA was designed to prevent.

But marketing and demographic aggregate information not tied to a specific child could be a partial business model for popular sites. While children's sites could easy collect and aggregate non-personally identifiable information and still be in compliance with the law, most either don't know how to do this, or haven't discovered the value of sharing their expertise about children's preferences with marketers, in aggregate demographic mode. For example, Nike wouldn't need to know that Billy Smith from 100 Main Street in Englewood, N.J. who attends fourth grade at the Englewood Grammar School likes blue sneakers more than black ones. They need to know that fourth grade boys in the NY metropolitan area prefer blue sneakers to black ones. This lets them market to all fourth grade boys, rather than directing ads to Billy via his e-mail or by directing special ads to him when he surfs online. This isn't as valuable to advertisers that may be seeking direct marketing opportunities, but it may help increase revenues. And here, COPPA levels the playing field between those sites willing to collect and mine personally identifiable data from children, and those that refuse to use their young site visitors in that way. With advertisers limited in what can be collected and shared without verifiable parental consent, the sites find it easier to direct them to aggregate demographic information options.

Subscription-Based Models: The subscription model hasn't been successful to date. Parents are unwilling, generally, to pay for children's online content. Some new sites will be offering special features and content, which may hopefully change this. Alfy, one of the leading kids content Internet sites is launching its new subscription-based model, cleverisland.com. Disney is focusing again on its Disney Club Blast! (disneyblast.com) subscription site (the site has been in existence for several years and is now entirely made-over). This has the additional parental attraction (and therefore, potential for success) of being Disney content. Juniornet (juniornet.com) has been a subscription-based service since its launch in 1997, and was the first of the new types of closed access services, which provide selected Internet content within a "walled garden" rather than from the Internet itself.

The experts see the subscription model as one of the most hopeful for the children's Internet industry, at least until software, games and educational services are regularly delivered online (about two to three years down the road) and parents are forced through market pressure to pay attention to their children's online activities.

Parental Involvement: Parents care about privacy and online safety, but they aren't interacting with the sites or supporting the sites that protect their children's safety and privacy. It may be that they are intimidated, or just plain too busy. But the children's online laws depend on obtaining parental consent, and if parents aren't bothering to provide consent, sites are running into problems.

Bonus's experience is a case in point. It found that out of the parents who were asked for their consent for Bonus to use children's information internally, 51% never replied, 31% provided consent and 5% said "no." (13% are still pending from this sample group.) This was a six to one ratio of parents allowing their children to use those services, over those who wouldn't allow them to share the information. But the 51% of parents not bothering to respond is frightening.

Bonus is losing more than half of the children who want to participate. And Bonus doesn't have chat, e-mail, e-commerce, on instant messaging. Bonus is a site that has games for children, and sends newsletters to their site visitors. This is a typical situation faced by many children's sites.

The solution is two-fold. One we need to teach parents how important they are to their children's safe and private online experience. They often feel that since their children understand the technology, they don't have to get involved. But they need to recognize that, although their children's technological skills may exceed their own, their children haven't yet developed the requisite judgment for handling communications with strangers online safely, at a younger age. Kids have better tech skills, but parents have better judgment.

We need them to understand the real risks children face online. Parents need to see the Internet as the telephone, rather than the television. While they may be concerned about too much sex and violence on television, parents are rarely compelled to take action in connection with what their children see on TV. Yet, all parents feel compelled to make sure our children do not talk to strangers. None of us would allow our child to talk on the phone with an adult stranger for two hours. Yet, their children often do just that, online in chatrooms and using instant messaging. Once we can get parents to see their children's safety and privacy in terms they understand, such as the telephone calls with stranger, they can use common sense to help their children learn how to surf safely. (Detailed information on all aspects of online safety for children can be found in my new book, The Parent's Guide to Protecting Your Children in Cyberspace, McGraw-Hill, 2000 (retail price $12.95), copies of which will be provided to the Subcommittee.)

Two, we need to make it easy for parents. If they need to provide consent to ten sites their children visit, separately, they just won't do it. We have worked on this issue as well, by developing a central site registry where parents can make a donation to Wired Kids via credit card, and register at one time for as many member sites as they want. A second service for parents is being developed with Wired Kids, where parents give noted online safety experts the right to approve sites for their children, based on certain criteria set by the parents, such as moderated chatrooms.

But these are a drop in the bucket, and more intensive parental consent mechanisms need to be developed. Offline consent, obtained at certain store locations from parents may be one possible solution. Parents who are shopping at a store may be able to use an offline consent gathered there to give the level of consent for their children's online interactivity. Schools are another place to collect consents.

Schools are being used by large sites for parental collection systems already. Big Chalk works with more than 26 million children in more than 42,000 schools. Chancery Software (k12planet.com) works with 20 million children in US schools. Under existing regulations and guidelines, sites are permitted to rely on the school's representation that the parents have consented to the student providing the personally identifiable information or using interactive features at the site. If schools make this representation, the site has millions of registered children and has complied with COPPA without having to deal directly with the parent. This is creating a risk management issue for schools, however, which may or may not have actually obtained the parents' verifiable consent.

Sources of Funding and Financing: Venture capitalists have pulled back from the children's Internet industry. A couple years ago, venture capitalists first became interested in the children's Internet industry. Until then, their main focus had been in e-commerce, but as more and more children got online (with a growth from 6 million in 1996 to more than 25 million today in the United States alone), the children's portion of the industry became more attractive. But the venture capitalists were looking for potential IPOs, and the IPO market has been dry for most of the Internet industry. Without IPO potential, and with no presently viable generally-recognized business model, venture capital dried up, and the chance for many children's sites to survive largely dried up with it.

Many sites had periodic financing schedules. Those that managed to raise their financing prior to the market correction this past spring are sitting pretty in the kids space. Others have international investment and business and revenue models. This too gives them more flexibility. But many found their expectations of being able to raise the financing they needed, as they always had raised them, unrealistic. Depending on how long they had waited in the financing cycle, many found themselves unable to keep their doors open. Most cut staff, changed operations and looked to other avenues for revenue. Licensing content and strategic alliances were seen as potential new revenue models, and have helped several sites survive and have brought others a higher profile outside of the traditional kids space. Brick and mortar children's industry players became more important and educational resources, which had additional value to bring to the mix, became more prominent.

KIDS ONLINE PRIVACY, THE FTC AND COPPA:

While there is a substantial focus on COPPA today, and the costs of compliance and to the industry, it is also important that we remember why COPPA was passed in the first place, and the serious risks to children is was intended to address.

COPPA was intended to address two separate concerns, (i) over-marketing to children and collection of personally identifiable information from children that is shared with advertisers and marketers, and (ii) children sharing information with online predators who could use it to find them offline. Both are valid concerns and need to be addressed.

Children's Online Marketing Practices: The FTC has conducted several surveys of websites, both sites directed at children and general audience sites. In each survey they learned that sites were collecting personal information from children, not informing the site visitors about their information collection practices and what they did with the information collected, and in many cases sharing this information with marketers and advertisers. While the bulk of the credible online community took this issue very seriously and drafted clear privacy policies and instituted ethical collection practices when children were involved, far too many sites ignored the FTC's warnings and plea for self-regulation from the children's Internet industry itself.

Interestingly enough, the practice of collecting and sharing personally identifiable information about children has been almost entirely eradicated. No credible children's site is currently collecting personal information from children for outside marketing, and none are knowingly sharing information collected with third parties. So COPPA works in this respect. It has changed an industry practice—one that parents wanted changed.

A sunset provision has been adopted and is in effect until April, 2002, that allows sites to collect personally identifiable information from children (this includes e-mail addresses, as well as what we would normally consider personally identifiable information) for internal use only with less than full-fledged "verifiable parental consent" (which is currently, typically, via telephone, credit card or debit card verifiers, regular postal mail or fax). During the sunset period, parents can provide their consent via e-mail, provided that the e-mail requesting this consent is delivered in such a way as to make it more likely that the parent and not the child will receive the e-mail and provide consent, and providing that the email consent is confirmed in some way. This is an "opt in" model that only permits the child's information to remain on file and be used if the parents affirmatively consent to it, by replying to the notice. As discussed in more detail later, we describe the actual statistics obtained from a leading children's site, Bonus. Bonus reports that more than 51% of the parents don't bother to respond to this e-mail. Of those who do respond, there is a six to one ratio of those providing consent, as opposed to refusing it.

Protecting Children from Online Predators: The second concern intended to be addressed by COPPA was children being lured and stalked by online predators who gather information about them from chatrooms, instant messaging, e-mails, websites and the like.

This is a very real risk, and one that should be addressed. Last year the FBI's Innocent Images Unit (charged with investigating crimes against children online) opened 1500 new cases of suspects who were attempting to lure a child into an offline meeting for the purposes of sex. Based upon my experience, about the same number of cases were opened by state and local law enforcement agencies last year for the same crime. Out of 25 million underage Internet users from the U.S., 3,000 cases may not seem like very much (especially when often it is a law enforcement agent posing as a child who is being lured, not a real child victim), but one if too much and all of these cases are currently avoidable. Also, most child molesters have a history of abusing children, so each case represents harm done to more than one child. Our children go willingly to offline meetings with these people. They may

think they are meeting a cute fourteen year old boy, but find that they are meeting a 47-year old child molester instead. Teen People has an article I worked on with them, on this very issue, in its new November issue, now out on the stands.

Law enforcement is not aware of anyone who is using the information children provide online to seek them out offline, by hiding behind a bush or grabbing them on their way home from school. But it's only a matter of time before this happens, since universal access to the Internet means that even violent sexual offenders who are online can use it for their own horrible purposes.

COPPA in Practice

Parents have told me that having to provide verifiable consent is a burden, although they are grateful that someone is notifying them of their children's online activities. They are also complaining that their children cannot use the interactive tools immediately upon obtaining their consent, given the current process which is largely offline. They object to using their credit card information, and credit card companies are unhappy that their verification systems are being used for this purpose. The charge to a site for credit card verification, for these purposes, is $.10 to $.20 per verification (generally per child). Sites are also being pressured not to use the merchant account systems for this purpose.

Obviously, the issues that COPPA was designed to address are still of great importance. But many of the problems cited in connection with COPPA could be handled easily if the FTC had more discretion in approving exceptions to full verifiable parental consent for safe applications and site practices. The law, as finally adopted, gave the FTC little or no discretion in this regard. It is the lack of flexibility, rather than the law itself, which presents the greatest problem.

While COPPA has received much criticism from members of the children's Internet industry, whether or not it is warranted, the FTC deserves only praise. The FTC has been outstanding in trying to inform the industry of what COPPA provides and how to comply with COPPA. They have been available for private meetings with site operators, have held a clinic on COPPA and how to comply, and have been active speaking at industry conferences on the law and how it affects the children's industry and general audience sites.

Cost of COPPA-compliance: We have polled most of the mid-sized children's websites for the cost of COPPA-compliance, in hard dollars, not as to any lost revenue or loss in traffic. This can run from more than $115,000 per year to $290,000 per year, depending on whether the site is fully interactive, with chatrooms, etc. and what level of consent they collect. Here's what they told us:

- $10,000-15,000 for legal, including audits and construction of privacy practices and policy
- Cost of toll-free telephone and dedicated fax service
- $35,000 in engineering costs to make the site complaint
- $2,500-$10,000 monthly for professional chat moderators (price differs depending on training, hours of operation and organization)
- $35-60,000 per year for one person to oversee offline consent, respond to parents questions, review phone consents, and review permission forms.
- $35-60,000 per year for person to oversee compliance, database security, respond to verification and access requests.

One specific example of a site and how it is dealing with COPPA is ePALS.

ePALS Classroom Exchange' is the world's largest online classroom community and the leading provider of collaborative classroom technology. ePALS pioneered the collaborative classroom concept in 1996 and now connects more than 2.5 million students and teachers in 182 countries worldwide.

ePALS Community members use a set of free, collaborative tools to meet and correspond online, combine professional expertise, join interactive projects, and develop international friendships. This tool set includes extensive profile creation and search functions, monitored email with profanity filters, moderated discussion boards, private chat, and soon, photo sharing technology. ePALS works to balance participation in the global community and learning through collaboration against the safety concerns of our educational community.

Educators turn to ePALS for a safe, creative way to integrate technology into the curriculum and to introduce students to the skills they'll need to participate in the global community. The ePALS commitment to safety is an ongoing success story.

ePALS has developed a simple COPPA consent package for American teachers who are already registered with ePALS. Teachers download this package directly from www.epals.com, print it and distribute consent forms to their students to take home to their parents. Only when all the consent forms have been received is the teacher free to carry on with ePALS activities. For all new teacher registrations,

ePALS requires teachers to collect consent forms before they can set up monitored email accounts for their students.

All individuals registering with ePALS must now submit their birth date and citizenship. If the individual is under 13 and from the United States, the registration process requests the parent's email address to complete the sign-up. Without the email address, the registration cannot be completed. If the child does provide his/her parent's email address, ePALS sends the parent a copy of the ePALS privacy policy (http://www.epals.com/privacy/index—en.html) and a consent form, which must be signed and returned via fax or post. Parents may also use a special toll-free number to provide their consent. ePALS will not activate a child's account without verifiable parental consent.

Beyond securing parental consent, the ePALS site offers three additional layers of security:

1) All profiles submitted to ePALS must be read and approved by a trained Site Support Coordinator before they are added to the site. Suspicious profiles are refused immediately.
2) The profile creator, the teacher or parent, is the first point of contact for anyone interested in a class/group profile. The teacher or parent can decide to refuse any communication.

The teacher or parent has comprehensive access to ongoing communications for his/her group of children. He/She can read every incoming and outgoing piece of email before it is received or sent, or simply choose to read specified pieces—ones with attachments, profanity, etc. The choice is up to the teacher or parent.

An example of what had to be undertaken to make ePALS COPPA-compliant:

- Massive revision of registration system to capture age, nationality, and parent/guardian information, send data to parent/guardian, and restrict access to appropriate users
- Revisions of Privacy Policy
- Creation of COPPA consent forms
- Installation of dedicated phone and fax system
- Hiring and training of Site Support staff to administer COPPA consent process
- Ongoing legal counsel
- Teachers cannot use ePALS in their classrooms until parental consent is received

Potential Solutions in Connection with COPPA: As discussed in more detail at the end of this section, solutions will come from three areas.

First is from Congress itself:

- We need studies conducted about how children use the Internet, and what help parents want and need.
- We also need funding for Internet safety education in schools and community groups.
- We need governmental support of leading Internet safety advocates t help them do their job in educating parents and children, and providing helplines for those who run into trouble online.
- We need more funding for law enforcement, to fight crimes against children online.
- We need more training of state and local law enforcement agencies to help fight crimes against children online.
- We need more discretion given to the FTC, and practical and reasonable carevouts from COPPA, or reduced consent levels, for sites that can demonstrate that they care about children's privacy and online safety.
- The FTC needs more funding to hire and retain quality staff experienced in this field. (The FTC staff is stretched too thin, and its staff members are too often recruited and hired by Internet industry members who need experienced advisors.)

Second is from the FTC itself, many of which are already implemented:

- We need more education of the industry in how COPPA works, and how sites can comply. (The FTC held an unprecedented clinic on compliance in August, and has been outstandingly proactive in this area.)
- We need a close interaction between the industry and the FTC in the area of online safety and privacy, and new technologies. (Here, too, the FTC deserves praise for its accessibility to the industry and its willingness to keep open dialogue with members of the children's Internet industry, large and small.)
- We need more FTC staff in the area of privacy and Internet consumer protection issues.
- Once more discretion is given to the FTC, we need it to address other methods of protecting children's safety and privacy under COPPA, which may allow sites to avoid the offline consent mechanisms.

- We need help in educating parents and children about online safety and privacy. Third is from the industry:
- We need to work together to form solutions, such a central registries, and joint consent mechanisms, and consent mechanisms where parents set the standards and allow a trusted third party to select the sites which satisfy the guidelines approved by the parents.
- We need to educate the children's Internet industry on business and revenue models and provide them with skills they need to run their businesses profitably. (The new trade association will help address that.)
- We need to educate parents about online safety and privacy, and educate children on safe surfing practices and how to exercise critical thinking online.
- We need to develop new technologies that make Internet safety and privacy as seamless as offline safety and privacy.
- We need to share our concerns and recognize that, as an industry, we survive or fall together.
- We need to share our expertise with Congress and the FTC. No one knows kids better than members of the children's Internet industry. The more we share our knowledge and expertise, the better Congress can legislate in this area, and the better the FTC can administer those regulations and advise Congress.

An analysis of COPPA, how it works and why it was adopted is included in the appendix. I divide the issues addressed into two areas: data collection and interactivity.

Sites should have to jump through many hoops before they are permitted to collect and share personally identifiable information from children. They don't need to collect personally identifiable information, other than e-mail addresses. And sites should have a very good reason before being allowed to collect more. Parents agree wholeheartedly.

But it would be very helpful for Congress to enable a study on what information is being collected, how it is being used and what parents really want. Most of what exists is more anecdotal than scientific. Parents send me about 600 e-mails a day, in my role as author of the leading book for parents on children's Internet safety and privacy, The Parent's Guide to Protecting Your Children in Cyberspace (McGraw-Hill, 2000), and in my position as Executive Director of Cyberangels (the world's largest Internet safety, help and education group), and President of WiredKids.org (which includes UNESCO's online safety project for the U.S.). They care about finding reliable and safe sites for their children to enjoy online. They care about spam (unsolicited junk e-mail, often linking to adult content sites), more than any other single issue. They care very much about their own and their children's privacy. I am not sure that they care about providing offline consent, or online credit card or similar identifiers for their children to be able to chat or use interactive community tools at sites that have adopted safety guidelines and procedures.

With respect to interactivity, requiring the highest level of consent from parents before children can use chat, e-mail, instant messaging, and the like was designed to address the danger posed by pedophiles and other bad actors. But there are two things that can address it even more effectively.

One is educating our children on smart surfing practices. We, at WiredKids.org, working with Cyberangels, are designing a curriculum for teachers to use in the classroom to teach safe chatting and online communication skills. Congress can be very effective in helping promote online safety education, especially for children. Our Teenangels program educates teens to teach other teens and children about safe surfing. This can be expanded nationally, with support from schools and community groups. Our new online safety video for children and teens will teach practical safe surfing tips. But we need more programs like this and funding for these programs, in order to be effective.

Two is getting sites to use safe surfing practices, such as moderated chat, and parental approved e-mail and instant messaging correspondent lists. Closed list of permitted correspondents, like the Buddy list used by AOL and the Cyberfriends list used by Surfmonkey are good examples of how parents can pre-clear certain real life friends for communication, while locking out strangers. These kinds of interactivity, when designed with children's safety in mind, should be permitted without having to get parental consent. Not, in my opinion, that parent's won't give the consent if they took the time to focus and respond, but because parents aren't bothering to respond. This is an issue that providing the FTC with more discretion can resolve.

Perhaps, by providing the FTC with more discretion in this area, the sunset provision for "email plus" consent may be extended, and certain types of activities at safe sites can be permitted with a reduced level of consent or notification. Sites could submit their practices to either the FTC or a safe harbor entity for approval. This

would allow sites the flexibility they need and provide incentives for adopting safe surfing and ethical privacy practices.

For example, the FTC should have been permitted to allow sites which have designed a safe chatting setting, such as clear site rules, trained chatroom moderators and use of technology to filter out certain prohibited terms, to avoid the onerous task of getting prior parental consent. Sites should have been permitted the option of presenting a package safety and privacy solution and approach to the FTC for approval, and for exceptions to the prior verifiable parental consent rule.

The way it currently operates, a site can get parental consent to any interactivity, no matter whether it is designed with the child's safety in mind. This actually provides a disincentive for safety and privacy practices at the site. And given the cost of moderating children's chatrooms, it is a choice many sites are making.

If the FTC had more discretion, it could approve these systems and permit the sites that use them to avoid the full-fledged verifiable consent mechanisms. It would encourage more innovation in this area, and keep our children safer at the same time. Sites which were approved could boost traffic by providing chat and interactive features children enjoy, which would in turn improve their financial position. This would provide further incentive for developing safe programs for children.

Offline consent mechanisms, digital signature development, school-related programs, and central registries are essential to helping the children's Internet industry navigate the current challenges it faces. But giving the FTC more discretion to provide exceptions to the verifiable consent requirement is one of the most important changes that could occur, and one of the most important things that this Subcommittee can recommend.

Our children are worth it, and so is the Internet. Too often blamed for everything from the Black Plague to the sinking of the Titanic, the Internet is a wonderful tool for learning, communication and entertainment. It levels the playing field between the haves and the have-nots. All children look alike online. No one is classified by their race, ethnic origin, religion, accent or physical ability. Online they are all just children. And like it or not, the Internet is here to stay.

We're all in this together. Let's work together to make the Internet fun, safe, private and educational for children. And let's work together to make sure that the children's Internet industry, which has so much to offer our children, flourishes!

For the children.

I remain willing to help, and provide input and expertise in any way this Subcommittee can use my help and expertise.

I wish to thank the Subcommittee, its chairman and all its members for inviting me to present this testimony on such an important subject.

APPENDIX—COPPA DEVELOPMENT AND ANALYSIS

The Children's Online Privacy Protection Act ("COPPA"), and the regulations thereunder which took effect on April 21, 2000, require all commercial sites to take special measures when they collect personal information from children or allow children to use interactive features, such as e-mail, instant messaging and chat (if they could share personal information with others using those tools). Many sites are confused about what the law provides, since it uses the word "collection" and they see that as something affirmative they are doing. But "collection" includes letting children use e-mail accounts or post messages publicly through a chat room or discussion board, as well as fill out forms. And it has nothing to do with adult content children may see online.

While the regulations are aimed principally at the children's Internet industry, they are fully effective against general interest sites with actual knowledge that a child is using their services. Few lawyers, even among experienced cyberspace practitioners, understand the children's Internet industry and the regulations and safety concerns that apply to it. But failing to understand what information can be collected from children, how it can be used, and what must be accurately disclosed to parents has cost many companies dearly.

There are two issues dealt with by COPPA and the existing consumer protection authority of the FTC. One is privacy, the other is safety. Both are regulated by the FTC, although states are permitted to enforce consistent local laws. In brief, privacy relates to the collection, maintenance, or use of personally identifiable information from children 12 years old and under. Safety is impacted, legally, when a child under the age of 13 is able to share personally identifiable information with others online.

The safety concern is that someone such as a pedophile may be able to contact the child either online or offline because the child has shared such contact information, whether intentionally or not. Last October, the FTC promulgated its final regu-

lations implementing the Children's Online Privacy Protection Act of 1998 (COPPA). Yet few were aware that the FTC already had the ability to enforce the privacy and safety concerns noted above, and has expressly set forth the parameters of that authority since mid-1997.

The salient document is the "Kids-Com Letter." Online since February 1995, KidsCom was one of the first children-only sites on the Internet. It did not use "cookies"—which glean data about site visitors—to gather information, but collected data through registration forms, contests, and pen pal programs. It was directed at children from ages four to 15 and came under criticism for its collection practices. (As a result of the FTC investigation, KidsCom revamped its site and is very popular among parents and children.)

In May 1996, the Center for Media Education, a consumer watchdog group, filed a petition with the FTC requesting that the agency investigate KidsCom and bring an enforcement action against it. CME asserted that KidsCom's data collection practices violated Section5 of the FTC Act's "anti-deception" laws in two ways. First, KidsCom collected information from children without accurately disclosing the purpose, and second, KidsCom failed to disclose that it was paid to endorse certain products. In July 1997, the FTC issued its findings in a letter. The FTC determined that KidsCom's disclosure was "likely" inadequate and misleading, but declined to take any punitive action against KidsCom since the company had already changed its data collection practices and cooperated in the FTC investigation. The FTC discovered that KidsCom was sharing information collected from children with third parties, though this information was provided only in an aggregate form (e.g., 10-year-old boys from New York preferred baseball over football).

In issuing this ruling, the FTC for the first time publicly announced its guidelines for data collection from children on the Internet. Relying on '5 of the FTC Act, which prohibits unfair and deceptive practices in or affecting commerce, the FTC stated: "It is a deceptive practice to represent that a Web site is collecting personally identifiable information from a child for a particular purpose (e.g., to earn points to redeem a premium), when the information will also be used for another purpose which parents would find material, in the absence of a clear and prominent disclosure to that effect."

Second, the FTC stated, when collecting personally identifiable information, "adequate notice" of such practices must be given to a parent because of a child's limited ability to understand the disclosure. "Adequate notice" requires disclosure of: (1) who is collecting the personally identifiable information; (2) what information is being used and for what purpose it is being used; (3) whether it will be disclosed to third parties, and if so, to whom and in what form; and (4) how parents can prevent the "retention, use or disclosure" of that information.

Third, the FTC articulated its "unfairness" test for Internet child safety, noting that the disclosure of children's personal information to third parties is of particular concern, and that parents must be given adequate notice of such use and the opportunity to deny their consent to it. The FTC has had broad regulatory powers when dealing with safety issues, under its unfairness authority in section 5. Under that section, a practice is unfair if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable and not outweighed by countervailing benefits to consumers or competition.

In its fourth and final principle, the FTC criticized KidsCom's endorsement practices as misleading and deceptive. KidsCom had "New Product" areas, where products were reviewed and endorsed. What it had not disclosed was the fact that, in exchange for an endorsement, product manufacturers had to contribute at least $ 1,000 worth of product, which was used for premiums and prize redemptions. The passing off of an advertisement as an independent review or endorsement is a deceptive practice under '5 of the FTC Act. KidsCom failed to clearly and conspicuously disclose that the product information was solicited from manufacturers and printed in exchange for in-kind payment.

Following the issuance of the KidsCom Letter, the FTC broadened its principles to include offline consent for children 12 and younger anytime their personal information may be shared online in chat rooms or similar third-party communications, and before any site collects and stores their personal information, even an e-mail address.

The adoption of COPPA was in direct response to the lack of industry compliance with the law as articulated by the FTC in the KidsCom Letter.

In June 1998, the FTC presented its Privacy Online Report to Congress, documenting the online collection of personal information from children. The FTC rearticulated its prior concerns that collection of personal information from a child under the age of 13 without informed parental consent would be a deceptive trade practice. The FTC reported to Congress that even in chat rooms, children innocently

and without request may reveal where they live or go to school or their real e-mail addresses. The FTC informed Congress that parents need to understand the risks and consent to any such collection and disclosure of personal information. Congress apparently agreed, and wasted no time in acting on the FTC's report. Within months, COPPA was law.

COPPA requires that commercial Web sites obtain verifiable parental consent before collecting personal information from a child under the age of 13. Failure to obtain such consent is an unfair and deceptive trade practice and can result in fines of up to $11,000 per occurrence.

COPPA applies to commercial Web sites, online services "targeted at children," and any online service operators with actual knowledge that they collect personal information from a child. (Actual knowledge can be as simple as a child's sharing her grade or age in a monitored general audience chat room on a site, or can be supplied by an e-mail or phone call from concerned parents who object to the collection practices on behalf of their child.) Personal information includes such items as full name, home address, e-mail address, telephone number, Social Security number, or any other information that the FTC determines "permits the physical or online contacting of a specific individual."

The regulations require covered operators to:

1. Provide notice on the Web site of what information is collected from children, how information is used, and the Web site operator's disclosure practices for such information (notice this applies to all information, not just "personal information");
2. Obtain verifiable parental consent (which requires more than a mere e-mail consent from the parent) to collect, use, or disclose children's personal information before it is collected from the child, with certain exceptions and special rules for newsletters and internally used information;
3. Upon request, provide parents with a description of the types of information collected from their child, or the actual information obtained from their child, and the opportunity to refuse to permit the further use, maintenance, or future collection of the child's personal information. Thus, in addition to having to obtain initial consent from the parents, if a parent withdraws consent at any time, the operator must remove that child's personal information from the system;
4. Cease conditioning the child's participation in games, contests, or any other activity upon the disclosure of more information than is reasonably necessary to participate, including permitting parents to allow the site to collect personal information but refusing to let the site share the information with third parties;
5. Maintain reasonable procedures "to protect the confidentiality, security, and integrity of personal information collected from children."

The law also details three different levels of consent, as well as the various types of notices required under the statute, which cover everything from the content of those rules to the look and placement of the link to the privacy policy displayed at the site, as well as the technical requirements for obtaining "verifiable" parental consent.

All websites need to look hard and thoroughly at their collection practices. Even if COPPA doesn't apply to the site, they may still run afoul of the FTC Act if their privacy policy does not accurately and completely disclose what personal information they collect from their users and what they do with that information. If they collect personal information that includes a person's age or grade or similar information, they may then have actual knowledge that they are collecting personal information from a "child" and need to comply with the full panoply of COPPA regulations. Even if they don't overtly request that information, if they have monitored chat rooms or discussion boards at which a user may disclose information from which the site should know they are under 13, that may provide the requisite knowledge under COPPA.

If the site collects any personally identifiable information from its users or provides any means of public disclosure of such information (such as through an e-mail service, chat room, discussion boards or instant messenger service), and the site is alerted that a particular user is a statutory "child," then the site must also comply with COPPA.

Banner advertisers and network advertising companies are covered by COPPA and its regulation if they advertise at children's sites and collect personal information from children who click through from such sites. They are also covered if they have ownership or control over such information collected directly at the children's sites. Advertisers at general audience sites may also be covered by COPPA if they collect personal information from people who click through, and that information discloses that the visitor is a child.

We have learned that many companies are collecting data from their Web site visitors without knowing why they are collecting it or if they are using it properly. Unless companies are under investigation or have heard of another company under investigation, their legal departments rarely communicate with Webmasters. With this new law on the books, all commercial Web sites must be vigilant in ensuring that the rights of parents to notice and consent are honored. If such companies ignore parents' concerns regarding privacy and advertising, they will have to face more than the FTC they will be facing the even tougher scrutiny of a disgruntled parent.

Mr. TAUZIN. Thank you.

Mr. Mike Griffiths, the Chief Technology Officer of Match Logic Inc. Welcome.

STATEMENT OF MIKE GRIFFITHS

Mr. GRIFFITHS. Mr. Chairman and members of the committee, I want to thank you for inviting me to testify. My name is Mike Griffiths. I am the Chief Technology Officer and one of the founders of Match Logic, an Internet marketing and advertising services company that provides strategic marketing solutions to Fortune 500 companies. We were founded in 1996 and currently operate as a subsidiary of a leading broadband Internet service provider, Excite at Home.

I am here representing the Network Advertiser Initiative, an industry group comprised of the leading Internet advertising companies. The NAI was formed at the behest of the Federal Trade Commission and the Department of Commerce to address consumer privacy concerns by developing self-regulatory guidelines on the practice of online preference marketing or profiling. The NAI companies represent more than 90 percent of the Internet advertising industry in terms of revenue and numbers of ads served.

Mr. Chairman, as you know, the NAI announced its self-regulatory principles in July of this year after months of intensive consultations with the Federal Trade Commission and with the Clinton administration. The Internet advertising industry needed to adopt rules of the road for its information practices in order to satisfy legitimate user concerns about privacy.

For the industry to write these rules in a manner that would garner public confidence, the NAI needed the guiding hand of public officials. The talks between the NAI and the Federal Government were tough but fair in that the industry had to make a number of important concessions. Ultimately, we were pleased that the NAI could develop industry self-regulatory guidelines that are meaningful and real and which the FTC, Clinton administration and Members of Congress on both sides of the aisle unanimously applauded.

The NAI principles dealt with the practice of online preference marketing. We define this as data collected over time and across web sites which is used to determine or predict consumer characteristics or preferences for use in ads delivery on the web.

In other words, we try to figure out which is the best ad to play to the consumer at a given point in time. We believe that OPM, if done responsibly, benefits both consumers and businesses. Consumers benefit because they receive banner ads targeted to their interests. If you are interested in golf, for example, you will see more advertisements for the latest golf equipment. If you buy a lot

of women's clothing, you will see more women's clothing ads. Advertisers benefit because targeted advertising is more effective and they get a better return on their investments. Finally, web sites benefit because the more effective the advertising, the more they can charge.

This brings us back to the consumer. Without targeted advertising, advertisers will pay less, web sites will earn less and consumers will suffer. Currently a vast majority of web sites are free. If Internet advertising does not work, these web sites will not be able to survive or they will have to move to a subscription model that charges users for services.

Our companies allowed tens of thousands of small and medium sized web sites to compete with bigger players for advertising dollars. We give them the economy of scale that they would otherwise lack. So in summary, our job is to make the Internet a more efficient and competitive advertising medium that will further stimulate the growth and viability of the Internet as a source for free content.

We at Match Logic and at the NAI understand that consumers are very concerned about Internet privacy. We share these concerns. If consumers are not comfortable that their privacy is protected, then the Internet will suffer. That is why the NAI companies came together with the Federal Government to develop landmark principles on data collection and the level of notice and choice that we must give to consumers. These principles lay the ground rules and safeguards for the collection and use of nonpersonally identifiable or unanimous information, the collection and use of personally identifiable information, and the merger of PII with non-PII.

In summary, here are the guidelines: First of all, NAI companies have agreed that we will not use personally identifiable sensitive health information, sensitive financial information, or information of a sexual nature for the purposes of profiling. We do not believe that these categories of data should be used, and we will not use them. For non-PII, we require notice and choice. NAI members must disclose their OPM practices through their web sites and through the NAI gateway web site. In addition, where possible they must contractually require their web site partners to disclose the collection of non-PII for OPM. NAI members will provide mechanisms for consumers to opt out from the use of PII for OPM.

For personally identifiable information, or PII, we require that NAI members follow the online privacy alliance guidelines for online privacy policies. These policies require the adoption and implementation of a privacy policy and that notice and choice be afforded.

Importantly, for the merger of non-PII with PII, we have two scenarios. The first case is where PII is linked with previously collected non-PII. In this case, members will not without prior affirmative consent or opt in, merge PII with previously collected non-PII.

The second case is where PII will be merged with non-PII for OPM purposes on a going forward basis. In this case NAI members will provide consumers with robust notice and choice. The NAI principles include several examples of what would be considered robust notice for each of these scenarios.

The NAI members have also agreed to establish a third party enforcement program that will include random audits by the third party enforcer, the ability to file and handle consumer complaints and the ability to redress lack of compliance though sanctions such as revocation of the seal or through a designated public or government forum such as the Federal Trade Commission.

Finally, the NAI members strongly believe that industry, government, consumer, and advertiser pressures to set and maintain high standards for privacy will render participation in the NAI all but mandatory for network advertisers. Moreover, because of the contractual reach of these NAI companies across literally thousands of web sites, the NAI principles will have a tremendously broad impact on web privacy.

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

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

[The prepared statement of Mike Griffiths follows:]

PREPARED STATEMENT OF MIKE GRIFFITHS, CHIEF TECHNOLOGY OFFICER, MATCHLOGIC

Mr. Chairman and Members of the Committee, I want to thank you for inviting me to testify. My name is Mike Griffiths, and I am the Chief Technology Officer and one of the founders of MatchLogic. MatchLogic is an Internet marketing and advertising services company that provides strategic marketing solutions to Fortune 500 companies. We were founded in 1996 and currently operate as a subsidiary of the leading broadband Internet service provider Excite@Home.

Before I begin I would like to thank Chairman Tauzin for holding this hearing and taking an active role on the important issue of Internet privacy. We have consulted with Chairman Tauzin and his staff during the development of the self-regulatory principles that I am here to discuss and his leadership helped us put forward guidelines that both protect user privacy in an unprecedented manner while, at the same time, allowing internet advertising to thrive. So, again, thank you Mr. Chairman and Congressman Markey for your hard work and for holding this hearing.

I'm here today representing the Network Advertising Initiative, an industry group comprised of the leading Internet advertising companies. The NAI was formed at the behest of the Federal Trade Commission and the Department of Commerce to address consumer privacy concerns by developing self-regulatory guidelines on the practice of online preference marketing, or "profiling". The NAI companies represent more than 90 percent of the Internet advertising industry in terms of revenue and numbers of ads served

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

that are meaningful and real and which the FTC, Clinton Administration and members of Congress on both sides of the aisle unanimously applauded

The NAI principles deal with the practice of Online Preference Marketing. We define this as "data collected over time and across web-sites, which is used to determine or predict consumer characteristics or preferences for use in ad delivery on the Web." In other words, we try to figure out which is the best ad to play to a consumer at a given point in time.

We believe that OPM, if done responsibly, benefits both consumers and businesses. Consumers benefit, because they receive banner ads targeted to their interests. If you are interested in golf, for example, you will see more advertisements for the latest golf equipment; if you buy a lot of women's clothing, you will see more women's clothing ads. Advertisers benefit because targeted advertising is more effective and they get a better return on investment. Finally, web sites benefit because the more effective the advertising, the more they can charge.

This brings us back to the consumer. Without targeted advertising, advertisers will pay less, web sites will earn less and consumers will suffer. Currently, a vast majority of web sites are free. If Internet advertising does not work, these web sites will not be able to survive, or they will have to move to a subscription model that charges users for their services. Our companies allow tens-of-thousands of small and medium size web-sites to compete with the biggest players for advertising dollars. We give them the economy of scale that they otherwise would lack. So, in summary, our job is to make the Internet a more efficient and competitive advertising medium that will further stimulate the growth and viability of the Internet as a source for free content.

We at Matchlogic and at the NAI understand that consumers are very concerned about Internet privacy. We share these concerns. If consumers are not comfortable that their privacy is protected then the Internet will suffer. That is why the NAI companies came together with the Federal government to develop landmark principles on data collection and the level of notice and choice that must we must give to consumers.. These principles lay out the ground rules and safeguards for the collection and use of Non-Personally Identifiable (or anonymous) information, the collection and use of Personally identifiable information, and the merger of PII with Non-PII.

In summary, here are the guidelines:

First, all of the NAI companies have agreed that we will not use personally identifiable sensitive health information, sensitive financial information, or information of a sexual nature for the purpose of profiling. We do not believe that these categories of data should be used, and we will not use them.

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

For PII, we require that NAI members follow the Online Privacy Alliance (OPA) guidelines for Online Privacy Policies. These policies require the adoption and implementation of a privacy policy, and that notice and choice be afforded.

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

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

The NAI members have also agreed to establish a third-party enforcement program that will include: random audits by the third party enforcer, the ability to file and handle consumer complaints, and the ability to redress lack of compliance through sanctions such as revocation of the seal, or through a designated public or government forum such as the Federal Trade Commission.

Finally, the NAI members strongly believe that industry, government, consumer, and advertiser pressures to set and maintain high standards for privacy will render participation in the NAI all-but-mandatory for all network advertisers. Moreover, because of the contractual reach of these NAI companies across literally thousands of Web sites, the NAI Principles will have a tremendously broad impact on Web privacy.

In conclusion and to summarize, the NAI self-regulatory principles are designed primarily to accomplish two things: first, to make sure that advertisers and web-sites post notices that are strong and clear where OPM occurs, and second, to make

it easy for users to opt-out. Under these principles, NAI companies agree to afford consumers with important notice disclosures and appropriate methods of choice for participation, while at the same time one of the main engines behind this nation's booming new economy, the Internet, can continue its remarkable growth and improve as a provider of free and reduced-price content.

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

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

Mr. TAUZIN. Thank you.

Finally, Mr. Andrew Shen, Policy Analyst for the Electronic Privacy Information Center here in Washington.

STATEMENT OF ANDREW SHEN

Mr. SHEN. Thank you, Mr. Chairman. Thanks for inviting me to speak on a very important issue to the American public and, obviously, also to members of this committee.

I will try to keep my remarks very short since I am the very last speaker of what has been a very long morning. My name is Andrew Shen, and I am a Policy Analyst at the Electronic Privacy Information Center. EPIC is a public interest research center located here in Washington, DC. Today while I am here formally on behalf of EPIC, I am really speaking here to represent the views and interests of American consumers.

EPIC believes that privacy has and will be one of the defining consumer protection issues for Internet, and what we have seen in these early years of electronic commerce is that the Internet has resulted in a vast amount of information collection that I think is unprecedented, and that information collection has resulted in corresponding concerns about personal privacy.

Now, when I speak in public at events like these, I do my best to address the concerns of American consumers and those that really just want to ask a very simple question, and their question usually goes something like this: How do I protect my privacy? How do I keep my personal information within my control?

To some extent, fellow members of my panel have tried to address that problem. Some have proposed self-regulatory guidelines, some have proposed technologies. Some have proposed a mix of both. But I think it is important to sort of analyze what a typical consumer experience of these approaches are.

Some suggest to a lot of consumers that they should change the settings in their browsers or use privacy tools or subscribe to anonymizing services. But this will not be sufficient for the protection of most American consumers. Many information collection technologies use jargon and terms that a lot of people are not familiar with. Terms like cookies, online profiling, online preference markets, opt in, opt out. This tends to confuse a lot of people. And here as evidence I want to cite a recent study by Pew Internet American Life Project. They found that 43 percent of Internet users—only 43 percent, less than half—know what a cookie is.

Even more astonishing than that are the results that of Internet users that have 3 or more years of experience online, that number only rises to 60 percent. That is for people who have been online for a very long time still do not know what a cookie is, let alone

what a company like Match Logic can do when they combine cookie technology with banner ads and huge networks.

Others may suggest that people can just read privacy policies and try to parse out what tend to be long, complex, and vague statements about what companies will do with their personal information. These privacy policies, as I already said, tend to be confusing. Larry spoke to this a minute ago. But I think a more important, more recent phenomenon is that these privacy policies are constantly changing. Many privacy policies will explicitly say: Our terms may change at any time. Please check back later. And that is just not good enough for the American consumers.

More recently than that, many consumers are simply being told that if the company fails or goes bankrupt or mismanages the resources they have at their disposal, their customers' personal information can be sold just like the computer sitting on their desk in the office as if it was their information to sell.

Now, do I have an answer for these people. I do not want to tell them they can't do anything. What I usually tell them to do is talk to lawmakers and legislators like yourself, tell them to say to you that they want their privacy protected, and tell them to tell you that you do have it within your power to protect their personal information. And Congress has done this before.

You listed off many bills earlier this morning, listing all the various sectors that have information that protect the personal information of consumers. These include information contained in credit reports, student records, e-mail messages, telephone toll records, video rental records, cable subscriber records. And they have succeeded in protecting American consumer privacy. And you can do the same for the Internet. You can protect the personal information that is submitted online.

But beyond that, because I realize that several members of your committee have introduced legislation. Congressman Luther spoke about it briefly this morning and so did Congressman Boucher. Sort of what is the law that we want to see? What is the ideal approach to the situation? And I would like to make a couple of points.

Chairman Pitofsky said that he believes that notice and consent were the most important parts of fair information practices. But in addition we need to think about access, a principle that has not been discussed a lot today. It is an important one. Access ensures that consumers can see the information that has already been collected on them, make sure it is accurate and up-to-date. And moreover, which I think is a very important point, it builds an ongoing relationship. I am providing my information to you and when I want to see my information you show it back to me. That sort of trust and confidence is something that e-commerce will definitely need going forward in the future, and I hope that you will include that as the protections that you choose to provide to American consumers.

[The prepared statement of Andrew Shen follows:]

PREPARED STATEMENT OF ANDREW SHEN, POLICY ANALYST, ELECTRONIC PRIVACY INFORMATION CENTER

My name is Andrew Shen. I am a Policy Analyst at the Electronic Privacy Information Center (EPIC)[1]. At EPIC, I work largely on consumer privacy issues. Earlier this year, I served as a member of the Federal Trade Commission (FTC) Advisory Committee on Online Access and Security[2]. I have been a panelist at FTC and Department of Commerce workshops on online profiling and more recently, online privacy technologies.

EPIC works with consumer organizations on a wide range of privacy issues. We also work on the international level within coalitions such as the Trans Atlantic Consumer Dialogue (TACD) that brings together consumer advocates from the U.S. and Europe[3].

I want to thank the Committee for inviting me to testify today on an issue that is of growing importance to the American public.

SURFER BEWARE REPORTS

Since 1997, EPIC conducted annual "Surfer Beware" surveys on the state of Internet privacy. EPIC's survey of Internet privacy policies "Surfer Beware: Personal Privacy and the Internet"—the first survey of online privacy ever conducted—found that only 17 of the 100 most frequently visited websites posted privacy policies and that none met basic standards for privacy protection[4]. That report recommended that Internet websites make privacy policies easy to find, clearly state how and when information is collected, provide access to data already collected, make cookie transactions more transparent, and continue to support anonymity.

"Surfer Beware II: Notice Is Not Enough" assessed the online privacy practices of members of the Direct Marketing Association (DMA)[5]. The DMA was and is a leading proponent of industry self-regulation with regards to personal information. The report found that only 8 of the 40 new DMA members with websites had privacy policies and only 3 complied with the DMA's own guidelines published nine months earlier.

Our most recent report "Surfer Beware III: Privacy Policies without Privacy Protection" was conducted shortly before last year's holiday shopping season[6]. Looking at the top 100 e-commerce sites, we found that not a single one had a privacy policy that complied with the benchmark of Fair Information Practices. For example, many websites posted privacy policies but did not provide access to personal data already collected.

We also found that many of the privacy policies were confusing and inconsistent. While over 80% of the websites that we surveyed did post a privacy policy, our survey proved that posting a privacy policy has no significant correlation with a high level of protection.

In the years between our first and last reports, we have documented the lack of protections for consumer privacy in these crucial early years of e-commerce. It is no secret that consumer concerns about privacy on the Internet have not dissipated in this time. If anything, recent developments such as online profiling indicate that the current approach of self-regulation may be putting consumer privacy at increasing risk.

ONLINE PROFILING

Online profiling caught the attention of consumers earlier this year when online advertiser, DoubleClick, proposed to created detailed profiles on Internet users. The company came under fire for linking personal information such as a name and address to online profiles, records of what Internet consumers were doing online. In doing so, it reneged on earlier statements made in its privacy policy that all information it collected would remain anonymous[7]. In testimony before the Senate Com-

---

[1] EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. More information about EPIC is available at the EPIC website, http://www.epic.org

[2] http://www.ftc.gov/acoas/

[3] http://www.tacd.org

[4] http://www.epic.org/reports/surfer-beware.html

[5] http://www.epic.org/reports/surfer-beware2.html

[6] http://www.epic.org/reports/surfer-beware3.html

[7] For more information, see http://www.epic.org/doubletrouble/

merce Committee in July of 1999, EPIC was one of the first organizations to publicly discuss the change in DoubleClick's business model [8].

In early February, EPIC filed a complaint with the Federal Trade Commission (FTC) that DoubleClick had unfairly and deceptively misled consumers about its information collection practices. At the end of July, the FTC approved a set of self-regulatory guidelines that permits wholesale tracking of Internet consumers and linking of those profiles to personal information without the knowledge or permission of the consumer. The guidelines were negotiated with the Network Advertising Initiative (NAI), a group of online profiling companies.

In response, EPIC along with 13 other consumer privacy organizations signed a letter pointing out that "the NAI Principles recently endorsed by the Federal Trade Commission fail to provide an adequate level of privacy protection" [9]. The letter said that

The Principles will allow online profilers to combine previously declared anonymous data with personally identifiable data, like home addresses and telephone numbers. In the future, online profilers will be allowed to link information about online behavior with personally identifiable data on a burdensome opt-out basis. The persons profiled by these companies will have no guaranteed level of access to view what data has been collected on them. Personally identified profiles may also be distributed to any third party—for completely unrelated purposes—on an opt-out basis. All of these provisions, and others, will erode consumer control over the collection and use of highly detailed profiles [10].

Furthermore, the letter faults the FTC for failing to involve the consumer advocacy community in negotiations with the Network Advertising Initiative. The negotiations were done behind closed doors and EPIC had to file a Freedom of Information Act request just to see the record of those proceedings.

EPIC, along with Junkbusters, completed a full analysis of the Network Advertising Initiative guidelines entitled "Network Advertising Initiative: Principles not Privacy" detailing the vague and weak restrictions it offers [11]. That review concluded that

The Principles perpetuate the secretive tracking of Internet users and run counter to the standards that consumers want. The Principles place the burden of privacy protection squarely on the consumer by relying on opt-out for both tracking of Internet users and linking of profiles to personally identifying information [12].

Further, the report recommended that "strong laws and effective enforcement will spur Internet advertisers to adopt methods and technologies that promote consumer privacy" [13].

Online profiling remains a serious concern for Internet users. I urge the Committee to ask the FTC why, despite their own recommendations for Internet legislation, it chose to approve self-regulatory guidelines for online profiling companies—the most personal information intensive sector that has developed to date on the Internet.

BANKRUPTCY

Apart from the activities of online profiling companies, the most recent development facing online consumers is the growing number of Internet companies that are auctioning off personal information when they go bankrupt. In June, online retailer Toysmart.com went bankrupt and advertised the sale of its assets in the Wall Street Journal. What caught the attention of many is that the company also attempted to sell its customer lists and other personal information in violation of representations made when it collected that data. The ongoing dot-com shakeout will likely produce more companies trying to recoup capital for their investors, but how will the privacy of this personal information be protected?

The FTC was able to pursue Toysmart.com since the company said that the information collected was "never shared with a third party". The FTC's attempted settlement fell short of requiring the company not to sell the personal data of its customers. Since then, other companies have been failing, similarly putting the information of its customers at risk.

Over Labor Day weekend, Amazon.com told its millions of customers that in the event that it failed—it would also declare their personal information as a business asset. That statement and other changes to the company's privacy policy prompted

---

[8] http://www.epic.org/privacy/internet/EPIC—testimony—799.pdf
[9] http://www.epic.org/privacy/internet/NAI—group—letter.html
[10] ibid.
[11] http://www.epic.org/privacy/internet/NAI—analysis.html
[12] ibid.
[13] ibid.

EPIC's decision to cut ties with the online bookseller. In a letter to EPIC's newsletter subscribers, we said that "Because of this decision, and in the absence of legal or technical means to assure privacy for Amazon customers, we have decided that we can no longer continue our relationship with Amazon" [14].

Failing to guarantee that personal information will not be sold in the future is an obvious requirement of privacy protection but one that companies have avoided taking on. As bankruptcies become more common, the failure to provide privacy standards for online consumers allows companies to protect privacy only when it suits them. When bankrupt, the privacy of a company's customers is no longer important to the company and is no longer respected. Furthermore, the growing number of bankruptcies points to an underlying problem with the current reliance on privacy policies. By making privacy policies the only standard to which Internet websites are held, it allows companies to change the terms on consumers—most recently allowing companies to unilaterally declare personal information theirs to sell.

GOVERNMENT PRIVACY POLICIES

Another issue before the Committee today is the issue of government website privacy policies. While this will not be the focus of my own testimony, I do wish to make a few comments on this issue.

The General Accounting Office survey commissioned by Rep. Armey and others found that 97 percent of government websites did not comply with the FTC Fair Information Practice principles of Notice, Consent, Access, and Security.

We support efforts to strengthen the privacy safeguards for federal websites. History has proven that such restrictions are necessary to curtail possible governmental abuses of power. Events like Watergate spurred laws such as the Privacy Act of 1974 that provides citizens with an array of rights to protect their privacy.

I should also point out that government agencies—unlike commercial entities—are not free to use personal information however they wish. Government agencies have to comply with guidelines set out in law while commercial websites have to comply with privacy policies that they themselves write.

PRIVACY ENHANCING TECHNOLOGIES

Since the beginning of the online privacy debate, EPIC has urged the wide adoption of privacy-enhancing technologies to protect consumers. However, I would like to point out what makes a technology one that enhances rather than invades privacy. Privacy enhancing technologies make it easier to take advantage of rights as provided through Fair Information Practices and minimize or eliminate the collection of personal data.

Without legal guarantees that data is collected for limited specific purposes, is collected only with consent, is accessible to the consumer, is securely stored and transmitted, privacy technologies can currently do little to help consumers utilize their rights. Only when existing law provides those rights will technologies develop to help consumers take advantage of them. The Platform for Privacy Preferences (P3P) demonstrates that failings of online privacy technologies in an environment without privacy law. A report released earlier this June, entitled "Pretty Poor Privacy: An Assessment of P3P and Internet Privacy", details some of the protocol's failings [15].

There is however, one area in which technology can address privacy in the absence of laws. That is in the promotion of anonymity and elimination of the need to collect personal data. Most of the activities conducted online such as reading news, shopping for products, searching for information, can be done without the collection of information from consumers. However, the current trend towards "personalization" results in the increased storage and analysis of these basic online activities. Infomediaries that seek to provide information according to user preferences do not provide this anonymity. Rather than reinforcing that the dispersal of customer information should not be the norm, they seek to encourage more information collection by making it easier than ever for personal data to be disclosed.

CONCLUDING REMARKS

Internet consumers are facing an increasingly hostile environment. Faced by online profiling companies that seek to know about their online surfing habits and websites that change their privacy policies at will, consumers are increasingly left to their own devices in protecting their privacy. Technologies available to con-

[14] http://www.epic.org/privacy/internet/amazon/letter.html
[15] http://www.epic.org/reports/prettypoorprivacy.html

sumers, for reasons I mention above, have a role to play but will only have significant impact once legal standards become effective.

Congress has a critical role to play in safeguarding online privacy. It should build on the legal framework for privacy protection, consistent through many federal laws protecting personal information [16].

There is significant public support for Internet privacy legislation [17]. Consumers should not be left without legal rights in the online world.

Mr. TAUZIN. Thank you. I think it is important to point out that why we are finding it hard to put our arms around all of the many aspects of the privacy issue is that there is a lot of tension here. Consumers have different expectations about privacy. On the one hand they want their privacy protected. They also would like the advantage of people advertising to them very specifically and very effectively, as was pointed out; the notion that I do not necessarily want to see a lot of ads that are about things that I am not interested in, but I very much would like to get books and pamphlets and ads and e-mail and maybe Internet advertising on things that I am interested in.

At our conference, for example, we heard from a banker who installed all sorts of privacy protections, separations between each division in his bank about the information that was stored there, the mortgage side from the savings and deposit side. And the first thing they experienced was that their customers started leaving them because they did not like the service anymore. They did not like the people telling them we can't help you because we do not have that information about you.

Ms. Aftab has pointed out that the parental consent of COPPA is not necessarily functioning as well as people thought because parents do not take the trouble to go ahead and okay their kids onsites that kids probably should be visiting. It would be good for them to visit and have interaction with.

In addition, we have got some experience with that. We had incredible debates, my friend Mr. Markey and I, over a thing called the V-chip, and the percentage of parents who are using it now are still pretty small, and I don't think it is expected to grow because it is just something parents, as I predicted by the way, would not have time to go around programming the television for the week.

So we come to this issue understanding all of this tension, and the problems we also experience are how much should we legislate and how much should we count on consumers eventually controlling much of their own private data through technology and through information.

But there are several things we have learned today that I think are important. One, we can have all the privacy notices required in the world and the bottom line is people are not necessarily going to read them, and they do get changed and they are confusing and more consumers will not be adequately served if that is the way we solve this problem.

---

[16] Fair Credit Reporting Act (1970) 15 U.S.C. § 1681; Family Educational Rights and Privacy Act (1974) 20 U.S.C. § 1232g; Cable Communications Policy Act (1984) 47 U.S.C. § 551; Electronic Communications Privacy Act (1986) 18 U.S.C. § 2510; Video Privacy Protection Act (1988) 18 U.S.C. § 2710; See Telecommunications Act (1996) 47 U.S.C. § 222; Children's Online Privacy Protection Act (1999) 15 U.S.C. § 6501.

[17] Business Week/Harris Poll: A Growing Threat, March 20, 2000, http://www.businessweek.com/2000/00—12/b3673010.htm

Two is that there are some things that do help a lot. You brought some to our attention, some software, some hardware technology and seals. We know seals works pretty good. We heard from Chairman Pitofsky today that only 8 percent of the companies' surveyed web sites are using seals. Why is that so low? That would seem to be a real easy thing for consumers to build confidence in web sites and in advertisers and in commercial enterprises if they saw and recognized a seal on a site without having to go read all of this policy and understand it and opt in or opt out or what have you. If what we are looking for is a user friendly world on the Internet in the area of privacy, would not seals, some simple way of understanding what I am visiting and what my rights are here without having to read all and understand all of those terms, wouldn't that seem to be a very positive and sort of appreciated thing on the web? And why is so small a percentage of web sites choosing to get an approved seal on their site? Anyone?

Ms. AFTAB. Mr. Chairman, if I may, Parry Aftab, what we are finding is that consumers do not recognize the viability of certain seals. There is no one Good Housekeeping Seal of Approval that is recognized generally by consumers. Once consumers can find various seals that mean something to them, then the seals will become a market issue.

Mr. TAUZIN. Let me give you an example. If instead of having the problem you cited where parents have to always consent to let their kids visit a site and share information, if there was a kiddie seal that parents knew and recognized to be representative of a site where, in fact, their kids are not going to be abused and information is not going to be mishandled, if they knew that, wouldn't parents appreciate that instead of having to constantly okay a child's visit to a site?

Ms. AFTAB. Absolutely, Mr. Chairman.

Mr. TAUZIN. Are we ever going to get there?

Ms. AFTAB. We have a seal that is going to be coming out under Wired Kids, which is safety and privacy, a quality site, which is a subjective test, but put together by librarians and teachers and child advocates, saying trust us, we can brand it for you. That will be coming out of the Wired Kids——

Mr. TAUZIN. And I suppose the same thing happened with software and hardware, that if at some point the private sector were to build consumer awareness of software and hardware technologies that are available, that parents and consumers generally would prefer that than reading extensive notices and constantly checking to see if the terminology has changed or the notice has changed, is that right? Any one of you?

Mr. GRIFFITHS. Being a technologist, I have some faith that technology will provide part of the answer. I think there is a reason why people do not read a lot of privacy policies either. Even if we encourage every web site on the planet to have privacy policies, the nature of the web is very fluid and dynamic. If you are searching, you do not stop and read the privacy policy.

Mr. TAUZIN. You can't. You do not have time. You may not know all the terms.

Mr. GRIFFITHS. Exactly. So I believe that technology such as P3P that allows for automated negotiation of preferences with respect to a site policy are part of the answer.

Mr. TAUZIN. But they are all part of the answer, but the concern I have is when do consumers really understand which of these solutions works for them and have the confidence in them? I do not see that happening yet. I do not see people generally saying, you know, there is a good seal out there. There is a good software, there is a good program that I can attach to and feel comfortable with without having to study and read and constantly update my permission, if you will, on a site.

Mr. GRIFFITHS. I think the answer today is that the Internet is still changing. It is ever changing and expanding and growing.

Mr. TAUZIN. Is it too little too late?

Mr. GRIFFITHS. Well, I think we see approaches from a regulatory perspective, from a self-regulatory perspective, from a technology and an awareness perspective, and I think it will take some time to work through. I really do.

Mr. TAUZIN. Ms. Cady?

Ms. CADY. I wanted to first of all give a personal response rather than a corporate response to why I think there is a lack of understanding of seal programs on the part of people who are in business, not on the consumer end. On the consumer end, we have the branding problem, and we all know that consumer branding of anything takes time and money and effort and certainly the seal programs are working toward that.

From the other perspective of businesses, it is hard to know which seal might be relevant. And then it is: Can I actually participate? Because there is a cost involved to the web site owner and if they are a very small organization they may deem that joining a seal program is not something they could do at some point—at this point.

Mr. TAUZIN. But if legislation provided safe harbor from government regulation if you were sealed properly, that would help, wouldn't it?

Ms. CADY. That would solve the branding problems.

Mr. TAUZIN. That is one of the things we are looking at that might help a great deal.

Ms. CADY. On the issue of expanding protections, what Privada is working toward, quite frankly, is to not have to have you worry about a seal if you are a consumer, or not having to worry about knowing where the technology is. But what we are trying to do is build in down another layer so that it will be with you all the time. And so our vision is that privacy is provided for you by your financial service provider and/or your Internet service provider, and/or other service providers that are available to you and which you use and you use it in conjunction with the tools that you are already using, your current browser, your current e-mail clients so that you have that protection if you want, and it is available to you easily.

Now, we again have a sales and branding and growth problem. So that we can't say to you that today, Mr. Chairman, we can do this for everyone in this room and everyone listening to this hearing, but that is certainly where we are going. Thank you.

Mr. TAUZIN. Mr. Shen, you wanted to add something.

Mr. SHEN. Yeah. I just want to add on to your earlier comments, Mr. Chairman. I think obviously what we are trying to address here are really the needs of the consumers; and I think consumers, while they have an appreciation for the fluidity, the dynamic nature of the Internet, really don't want that fluidity and dynamic nature to touch their personal information. They want guarantees.

Mr. TAUZIN. Let me tell you something about that. We have a hard time gauging what consumers really want in this area, and I will tell you why. We find this out in a lot of our political surveys. When you ask consumers questions about this, they often tell you what they think they should want rather than what they really want. They often answer these questions with "I am supposed to want to protect my privacy," as opposed to "Yeah, I will take all these efforts to go operate all these consents and these opt-in and opt-outs."

What they really want is comfort, ease. They want to be able to use these systems with some credit confidence but also with ease, and user friendliness is a huge consumer desire we are finding in our meetings and town hall meetings and discussions and everything else about this.

When you really pin people down they say, yes, I want my privacy protected and protected at all costs. But they also tell you, when you really get away from any kind of public surveys where they are answering what they think you want them to say, what they say is they really want this to be easy. I don't want all this trouble. I don't want to have to work too hard to use these systems. I don't want to have work too hard to access, for example, credit or to access the store that sells me what I want on the web and to get the information I want; and I am willing to take some risk to do that.

But if you can make it, you know, reasonably secure for me, reasonably, you know, comfortable that I am not going to get burned on this, if you make it easy, I am pretty happy. That is what we are hearing. It is a real tension.

So it is hard to understand what consumers really want in the way of legislation and/or, you know, even regulation in this area. I hear you, and I know what you are saying. Because whenever we do surveys, privacy, No. 1, everybody wants it protected at all costs.

But then when you really get down to it they say, "Yeah, I really want my kids to go and visit those good web sites" and "Yeah, I really want the advertisers to know enough about me to target ads for my taste and my wants and my desires" and "Yeah, I don't want to have to read big notices and I don't really want to have decide which seal is a good seal and which program is a good program." I mean, we get real conflicting signals about this stuff. As much as we think we understand it, we constantly realize we don't.

The other thing I want to get into with you is the question of bankruptcies, mergers, acquisitions, change of leadership. Here we are collecting data. I may indeed agree that your company, your web site, can collect all my data because I trust you with it. I trust you are going to manage it well. But next week you die. Somebody else takes over the company. Next week the company merges with another company.

You mentioned merging personally identifiable data with non-personally identifiable data problems, but you have got a range of issues here, not just bankruptcy but issues where we change the management of the company, the stockholders may change, I may merge, I may sell the company, all sorts of different ways in which different people come in to control how the information I trusted with a certain group of people or a company that I trusted only to find out that company is a new company tomorrow because it merged or it was acquired or because it went bankrupt and was selling all its assets, including my information.

There are all sorts of different scenarios you can paint where information I thought was secure with this group of people in this company brand name that I trusted is all of a sudden now potentially under somebody else's control. How do we deal with that? Anybody.

Ms. AFTAB. Mr. Chairman, I will put my bankruptcy practitioner hat on because, before I started doing Internet law, I used to do Chapter 11 bankruptcies. There is a problem here in that there is a tension between the bankruptcy laws, which try to maximize the value of any asset of a company and the ability of a trustee or the debtor in possession, and the bankruptcy court to permit any contract to be modified. So that you can say it will never happen, but under the bankruptcy law and under policy you can move all those things around.

Mr. TAUZIN. But I mean we are talking about dot com companies now. Dot com companies, the physical assets very often are much less valuable than the information assets, the intangible assets. In fact, there is a huge debate over how to properly assess the value of a company and how do you measure intangible assets. As you know, FASB has got a big debate on its hands. We have engaged them on that very question.

But the point is that in dot com companies the information base is the asset, and if we say as a matter of law that because you collected that on a confidential basis with your consumer base that you can't ever transfer your company with that asset, you are basically devaluing that company significantly in commerce, are you not?

Ms. AFTAB. You absolutely are, Mr. Chairman. I think that is part of the tension, and part of what can be done is people can actually reach out to members of that list through e-mail and say we are moving this or this list is up, not an answer, certainly not an answer, but something that at least will raise additional questions.

Mr. TAUZIN. It is something we may have to address, right? Because it gets down to whether or not—in this case, the rights of the consumer is a matter of contract or we make it a matter of law, and if we take it from whatever the contract provided, whatever agreement I had with the company, we start making law on it, it could dramatically affect the value of dot com companies, the way in which dot companies are financed and the way the stock performs and everything about them. It could dramatically affect the whole dot com economy.

Mr. CHIANG. Well, Mr. Chairman, with regulating this facet of, let us say, the sale of information of the company, can't we look toward where—previous legislation where when two banks merged

and one person's ATM fee is $1.20, another person's ATM fee is $1.25, where you have maybe not just one e-mail notification but maybe a statement update or a card member services agreement update where you maybe don't just send one e-mail, maybe a series of three e-mails.

Mr. TAUZIN. But let us say I have a privacy policy at my bank that I will not sell or transfer your private financial information to anyone else, but now I go bankrupt and my bank is being sold and somebody else acquires it. Is the asset—my financial information—an asset of that company that can be transferred even though I have a contractual relationship with a bank that it not be shared with anyone else? Get my drift? These are weird questions.

Mr. CHIANG. Right. Previously, I think that is why if the FTC were given the regulatory authority—and I am not, you know, financially supported from them in that MoneyForMail is its own for-profit corporation. But in that instance where then the FTC can say in the specific example, the case study where I think a company called Toysmart went out of business——

Mr. TAUZIN. That is the one we are talking about. That case was built because, obviously, it went out of business. But the point I make is I can envision 12 different scenarios where the ownership, control of that information changes hands, not just through bankruptcy. We could have a major shake-up at the corporation, all the board of directors get fired and a new management team is brought in. Effectively, that is a new company now in control of my information.

Did I want that team to have my private information? Maybe people I don't trust. Maybe, you know, if a foreign entity moves in and I may have some problem with that. I might have—you know, we have got an entity seeking to buy a company in America that is government-owned right now. We are having a big discussion about that. Suppose that entity has private information? Now a foreign government is going to have information about me that maybe I didn't want a foreign government to know.

You get my drift. There are many scenarios affecting the collection and the use of private information by companies in this changing marketplace that we need to think about, and we are going to need some help in figuring all that out.

Mr. CHIANG. I think previously with the property question issue that was I think two panels ago, where who owns the data, it is shared data between the corporation and also the personal——

Mr. TAUZIN. Let us get away from the Internet. How do they work in the brick and mortar?

Mr. CHIANG. I think what is going to happen is that the Internet is causing a catalyst where in America it is very inexpensive to send out a piece of direct mail. I mean, if anybody goes home today and looks at how many credit card inserts that you are going to have, it is probably between 10 to 15. It is not price constrained. It is just logistics constrained—not even logistics constrained, but just——

Well, getting back to the point where I think what is going to happen with the Internet, it is going to cause people to say, hey, well, don't I also then control other pieces of data that is compiled and collected on me, not just Internet data where I like to purchase

these specific toys that are racing-oriented toys? Then what about credit data pieces? Don't I also control my own credit data? I mean, where everyone's talking about notice and choice and access—I mean, today I don't have access to my own credit report, and I work in the credit industry, and I do not have access unless I pay $8. That is going to catalyze some of the questions that I think are going to happen in the industry which is, who does control it? Is it shared control of the information?

Mr. TAUZIN. We have never settled all that, have we, about who owns the information about me and doesn't it have a lot to do with how you obtained it? I mean, you can observe me in this room and gather a lot of information about me, and so you are obtaining it in a public sense. How it is obtained may have something to do with whether or not we protect it in the person, we allow it to be in the public domain or publicly used or publicly traded. I don't know. But some interesting thoughts that we are going to have to have and some interesting discussions.

Mr. Shen, you look very thoughtful.

Mr. SHEN. You obviously bring up a lot of very interesting issues, basically why I like working on this issue as well. We are confronting new sort of conflicts, things that we have—tensions between bankruptcy, the need to try to satisfy creditors and also the need to protect consumer privacy.

I think, sort of adding on to what people have already said, there is no reason I think why most American companies cannot contact their customers if they are going to be bought or merged or acquired in some fashion. The Internet is interactive. It supposed to facilitate that sort of contact and communication.

I think, with all due respect to your earlier point, what happens in the off-line world is something we do have to go back and address. I think in the off-line world there is obviously not a great deal of protection for personal information in a bankruptcy proceeding. Is there a reason to go back and see if we want to reopen that issue? I definitely think so.

Mr. TAUZIN. The reason I raised the issue—if we get away from the Internet, take ourselves back in time a bit. If I have a little country store in Thibodaux, Louisiana, where I was born and raised, and I have a customer base that I have been selling to and I decide to sell out, I sell that information—we sold that information to the next guy that bought the store, and nobody complained. What is different about the Internet that makes us want to complain? What was it—Toys.Com, why was that such—whatever it was—why was that such a scary thing when that happened in the brick and mortar world with such frequency?

Mr. SHEN. Well, I think one possible answer—and that is not a complete answer—is that the information collection on the Internet is much deeper than it has ever been before. Perhaps if you had owned a small business in Louisiana with information about a person's name, maybe their mailing address in case you wanted to send a receipt to them. On the Internet you create profiles like this gentleman does right next to me. You create information, records about what they have been doing on-line across thousands and hundreds of web sites. I think that is at least one reason——

Mr. TAUZIN. Is part of it the fact that we all know that little store owner in town and we probably know the person who is buying the store but we don't know all these people on the web?

Mr. GRIFFITHS. Right. And it is important what the original premise was of the collection and that original relationship. I think if the party down the line meets and supports the original premises of collection, it will be used for this purpose and contact in this way, then it is seamless. If they dramatically change the premise under which they are contacting, then it is scary.

Ms. AFTAB. I think also in the Toysmart case there were children involved and I think there is this fear that parents have and knowledge that they have that their 8-year-olds know more than they do about what is going on with the computer and the Internet.

Mr. TAUZIN. And they do.

Ms. AFTAB. They absolutely do. If you have to have something fixed, you call the 8-year-old. But in this case, children were sharing information at the site, and the concern about the parents not even knowing what the kids may have shared and that now being sold to third parties is what had frightened people.

Mr. TAUZIN. When we were growing up, my parents used to be afraid of what we would tell our teachers about our parents.

Ms. AFTAB. That is it. And the most we had was the Birthday Club at Howard Johnsons.

Mr. TAUZIN. Now, we can tell people we totally don't know about anything. It is a totally different world.

We could keep this going a long time, and we probably will before we come to some conclusions, but I will invite you to do several things.

No. 1, the record stays open for 30 days. If something we have said here or something you have heard here has provoked some good thought and some good comment from you, please submit some more information to us.

As I said, this is an extraordinary learning process. Mr. Shen, you are right. It is one reason I love this work, too, because it is extraordinarily fascinating; and I don't know where it all comes out yet. I do know that we have got enormous tensions here, and you have heard from a lot of members how we need to proceed very judiciously here and carefully here because, obviously, we can make some rules that don't work. We can do like that bank. We can impose some conditions on people that we think people want only to find out not only they don't want it but it didn't work very well for them.

Finally, we obviously need some real-world thought and experience from those of you working with consumers to try and find solutions that work for them.

The record will stay open. We may have some questions we may want to submit to one or two of you.

I apologize for the lack of members here. That is the reason why I have always hated second and third panels because the members all leave and I am the only one left with you, but it has been a good experience for me. I have learned a lot, and we will try to make sure other members pick up your material and read it and learn from it as well. Thank you very much.

If you have got something final you want to tell me, this is a good chance.

Ms. AFTAB. I would like on behalf of the entire panel to offer all of our continuing expertise to anyone who is willing to listen.

Mr. TAUZIN. Thanks so much.

The hearing stands adjourned.

[Whereupon, at 2:50 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

PREPARED STATEMENT OF HON. DICK ARMEY, HOUSE MAJORITY LEADER

I would like to thank the Chairman, Ranking Member and the Committee for inviting me to testify today. Internet privacy is an important subject, and one that deserves our full attention.

And since we're talking today about the *government's* online privacy standards, we need to be doubly vigilant.

The government collects and stores vast amounts of personal information on you and me. The IRS knows how much you make, who you work for, and where you live. And the Department of Health and Human Services has access to many of your personal medical records.

You are required to give this information to the government. You have no choice. But you don't have to use a commercial website if you feel it has a bad privacy policy. And which worries you more? The IRS accidentally disclosing your personal financial information, or a website knowing how many books you purchase each year?

That's why the government must be held to absolutely the highest privacy standard. There is no excuse for anything less.

And that's why I was quite surprised when the GAO discovered that the government failed to meet the Federal Trade Commission's own criteria for online privacy. They didn't just fail, they failed big time. A mere 3 percent of the agencies surveyed lived up to the proposed standards. And the FTC wasn't even on the list of agencies that passed. They failed to meet their own criteria.

So when I hear administration or FTC officials talking about privacy, I can't help but think: *Doctor, heal thyself.*

There is more evidence of a certain cavalier attitude toward personal privacy on the part of the administration. A privacy watchdog group known as Privacilla recently issued a report last week that shows the White House and other administration websites violate the Child Online Privacy Protection Act.

Rep. Terry Everett and his subcommittee found that the Veterans' Administration computer system was so insecure that any 12-year-old hacker with limited skills could "own" the system and call up confidential medical records at will. And that's after the VA has spent over 5 billion dollars upgrading their computer systems.

Without proper security, there can be no privacy. Recently, Rep. Steve Horn gave the government as a whole a "D-" for its computer security efforts. But, even worse, several agencies such as the Departments of Health and Human Services, Justice and Labor that collect a lot of personal information failed completely.

Further, just three weeks ago the Department of Justice posted on its website a report about the review of its controversial "Carnivore" Internet cybersnooping system. But there was a problem—the agency didn't bother to adequately protect the personal information about the researchers involved in the study.

The clear message from all this seems to be: we need to get our own house in order.

Now, I have read many administration officials complain to the media that applying FTC rules to the government is unfair. They say it's like comparing apples and oranges. I don't think so. I say that we need results, not excuses.

When the FTC first began measuring private sector websites with its "Fair Information Practice Principles," it was a "pop quiz." It never gave advance notice to the companies that were checked. And I seriously doubt that the FTC would have let a commercial website get away with the excuse they were just "complying with the spirit of the FTC rules." Our GAO study was not a pop quiz. The government knew in advance the criteria by which they would be graded. And, in fact, the FTC was unable to meet its own criteria. There's no excuse for that.

Others in the administration have pointed to the Privacy Act as the reason why they failed to provide "notice" to website visitors. But the whole point of a privacy policy is to disclose to visitors what your policies are. How many people actually understand the laws and guidelines governing government websites? Just because you

can find guidelines in the Code of Federal Regulations doesn't mean you shouldn't post this information for website visitors in plain English.

It's entirely fair to see whether the administration can live up to the standards that they are trying to impose on everyone else. Government should live by the same rules it imposes on everyone else.

I was pleased to read Commerce Secretary Norman Mineta quoted as saying that he intends to make his agency's website adhere to the proposed FTC standard. So the claims that the government just can't meet these standards rings hollow.

The GAO report certainly has raised questions about the standards. And it certainly is interesting that several Administration officials have begun to point out deficiencies in the FTC criteria in light of the GAO report. None of these individuals spoke up when the FTC was using the same criteria to beat up on the private sector.

With this in mind, I think the FTC guidelines on privacy bear re-examination. Because I wonder how well a government that has this kind of a performance can presume to police the private sector on privacy.

Either the FTC standards are the correct measure of online privacy—in which case the federal government is an absolute privacy disaster; or, they are not the correct criteria, and the FTC should not be asking Congress to impose them on the private sector. It's one or the other.

That is, in fact, the main reason we asked GAO to perform this study. We are learning more about what it means to have principles governing website privacy. And we need to keep asking these sorts of questions before we assume we have all the right answers.

Make no mistake—the government's privacy failures should not be construed as an excuse for the private sector. Obviously private websites should observe good privacy habits. A few bad apples shouldn't be used as an excuse for the government to jump in and regulate the Internet. So long as the private sector continues to do a much better job than the government, and continues to improve its own practices, we should restrain the instinct to interfere with the Internet.