S. HRG. 106–1116

TO REVIEW THE FEDERAL TRADE COMMISSION'S SURVEY OF PRIVACY POLICIES POSTED BY COMMERCIAL WEB SITES

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

MAY 25, 2000

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

81–862 PDF WASHINGTON : 2003

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

JOHN MCCAIN, Arizona, *Chairman*

TED STEVENS, Alaska
CONRAD BURNS, Montana
SLADE GORTON, Washington
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
JOHN ASHCROFT, Missouri
BILL FRIST, Tennessee
SPENCER ABRAHAM, Michigan
SAM BROWNBACK, Kansas

ERNEST F. HOLLINGS, South Carolina
DANIEL K. INOUYE, Hawaii
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
JOHN B. BREAUX, Louisiana
RICHARD H. BRYAN, Nevada
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon
MAX CLELAND, Georgia

MARK BUSE, *Republican Staff Director*
MARTHA P. ALLBRIGHT, *Republican General Counsel*
KEVIN D. KAYES, *Democratic Staff Director*
MOSES BOYD, *Democratic Chief Counsel*

CONTENTS

WITNESSES

APPENDIX

TO REVIEW THE FEDERAL TRADE COMMISSION'S SURVEY OF PRIVACY POLICIES POSTED BY COMMERCIAL WEB SITES

THURSDAY, MAY 25, 2000

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 9:30 a.m. in room SR–253, Russell Senate Office Building, Hon. John McCain, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOHN MCCAIN, U.S. SENATOR FROM ARIZONA

The CHAIRMAN. Good morning. This morning the Committee will examine the recently released FTC report on online privacy. I welcome the members of the Commission and all the witnesses we will hear from today to the Committee. I also want to thank all of you for the hard work and dedication you have brought to this difficult issue.

Every accolade that can be ascribed to the Internet has been stated many times over. Needless to say, it continues to transform our lives and our economy. While the Internet promises great opportunities, it also presents new concerns and fears. Chief among those concerns is the ability of the Internet to further erode individual privacy.

Since the beginning of commerce, business has sought to learn more about consumers. The ability of the Internet to aid business in the collection, storage, and transfer of information about consumers, however, is unprecedented.

While this technology can allow business to better target goods and services, it has also increased consumers' fears about the collection and use of personally identifiable information. The Commission documented many of these concerns in its report.

Last year when the Committee reviewed the FTC's 1999 report on privacy, I made clear that my primary concern was to ensure that privacy policies were clear and understandable, that consumers could use them to guide their decisions, and that companies actually followed the policies they posted. Improving the depth of privacy policies is the primary factor motivating this Committee's interest in this matter.

This year's report demonstrates that the business community has had great success in providing consumers with some form of notice

of their information practices. However, the report makes it equally clear there is much work to be done to improve the depth of information practices on the Internet.

Consumers should not be forced to forego what has been described by Justices Brandeis and Warren as the "sacred precincts of private and domestic life" to enjoy the benefits of this new medium. It is clear that businesses should inform consumers in a clear and conspicuous manner how they treat personal information and give consumers meaningful choices as to how that information is used. While we may disagree on the manner in which we meet this goal, we all agree that it must be done.

I am hopeful that today's hearing will begin the process of developing consensus about the best way to accomplish this goal and enable consumers to protect their privacy online. I look forward to working with all of you to address this vital issue.

Welcome, Senator Hollings.

STATEMENT OF HON. ERNEST F. HOLLINGS,
U.S. SENATOR FROM SOUTH CAROLINA

Senator HOLLINGS. Well, Mr. Chairman, let me thank you for this hearing. We have toyed with the problem long enough. It worsens every day. Industry agrees that there should be privacy protection. They have all enunciated privacy policies, but that has added more to the confusion rather than assisted the problem because it is written either in legalese or it cannot be found or understood.

We have had the Federal Trade Commission, this distinguished group, work on it for at least 5 years. As a result of their fine work, incidentally, we passed a bill on children's privacy, and that is working. The intellectual community is saying that this technology is advancing so quickly that you cannot keep up with it; it is silly to try to even draw up a statute about it because it will be obsolete by the time it is passed.

That is not what they said when they came to us for protection of intellectual property, regarding movies, books, and everything else. We passed these other protections, and now we have got to do it for the individual. Mind you me, this is not a technology or advancement that was invented either by the Vice President or by the advertisers. It was started by Senator Stevens in the Defense Subcommittee back in the late sixties.

It has been free. It will stay free. And unless you are commercializing privacy, you do not have any worry about any statute on privacy. This is for those who are taking individual private information and commercializing it. Internet companies have agreed that there should be some protection for privacy. The question is how to give notice and consent with respect to access to what information the companies do have as well as the enforcement of the security.

So what we need to do is look at this issue. Several Senators have. I commend my colleagues Senator Wyden and Senator Burns. They have sort of led the way. I have consulted over the last 3 months now with various Senators and the FTC and other entities interested in it, with industry, and with the consumer groups. We have a bill on course now with ten co-sponsors, and I think we

have got a pretty good target for a good approach, which is very necessary at this particular time.

Do not let us come here and say that it is going to ruin the Internet and no longer is it going to be free. I have heard statements recently to that effect. That is outrageous nonsense. There is nothing wrong with the Internet. You and I cannot stop it. In fact, the President only yesterday said it is going to bring democracy to China. So it is a wonderful thing.

I will include my full statement in the record.

[The prepared statement of Senator Hollings follows:]

PREPARED STATEMENT OF HON. ERNEST F. HOLLINGS,
U.S. SENATOR FROM SOUTH CAROLINA

Today the Committee will hear from the Federal Trade Commission, the agency with unique expertise on the issue of Internet privacy. Having studied privacy online for five years, and having issued three consecutive annual reports on privacy policies online, beginning in 1998, the FTC concluded this week that it is time for legislation to protect consumer privacy on the Internet. This recommendation carries with it particular credibility in light of the FTC's record of extensive analysis on this issue and its two prior recommendations to allow self-regulation a chance to work.

In light of this recommendation, how should we respond? To answer that question, I first want to recognize the constructive efforts of two of my colleagues on this Committee, Senators Burns and Wyden, who attempted the first foray into the complicated issue of Internet privacy when they introduced their legislation last year. I look forward to working with them as we grapple with this significant consumer issue.

The bill that we introduced Tuesday with ten cosponsors, the Consumer Privacy Protection Act, grants consumers, not companies, control over their personal information on the Internet. We do that by coupling a strong federal standard to protect consumers online with preemption of state Internet privacy laws to ensure business certainty. Our strong federal standard tracks the time-honored "fair information practices" of notice, consent, access, security, and enforcement, that the FTC recommends we codify, and that we did codify with respect to childrens' privacy.

Specifically, we require companies to do what some like Alta Vista are already doing—namely obtain prior consent from consumers before collecting and using or disclosing consumers' personal information. At the same time, we need federal preemption to give industry the business certainty it cannot obtain from a mishmash of inconsistent state Internet privacy laws.

Notwithstanding this sensible approach, industry will claim that we should ignore the FTC's findings and give self-regulation more time. I say that is like letting the fox guard the henhouse. How can we trust companies whose every economic incentive is to collect, compile, enhance, target, and disseminate personal information for profit. Given these undeniable incentives, it is not surprising that industry argues so strenuously against regulating the protection of consumer privacy on the Internet.

What industry forgets is the Internet is not theirs. The truth is, Internet owes its existence to federally funded research by the Defense Department in the late 1960s. The DOD Advanced Research Project Agency (ARPA) developed a radical new type of computer based communications system. This system was enhanced and expanded to more users through funding via the national science foundation. To put it simply—the Internet was created for the public good—to facilitate scientific and academic research, to promote our national security, and to aid the exchange of ideas and information. The development of the Internet represents the single greatest modern example of government support for a revolutionary new technology. After its creation in 1969, the government sustained it for over two decades and now is subsidizing the commercial explosion on the Internet by refraining from imposing tax collection duties, and by exempting the Internet from regulations and fees that currently are imposed on other telecommunications companies. Protecting privacy online will enhance confidence in the medium and continue government's important and ongoing role as a promoter of the Internet's now exponential development.

Industry also argues our approach will undermine some business models on the Internet that are based on customized advertising targeted to individuals whose personal information has been collected. But *The New York Times* reports on May 7,

2000, that targeted advertising on the Internet may not be a sustainable business model. Most advertisers "say the response to their ads does not go up enough to be worth the extra cost and bother" of targeting. America Online's Robert Pittman appears to agree that targeted advertising is not necessary. "We don't need to track people. If you want to sell cars, you talk to people when they are in the car area." More to the point—we do not attempt to prohibit this advertising model on the Internet. We simply create a framework that requires that consumers be notified and consent to these practices, if businesses choose to collect information online.

One last point. Many of the same companies that oppose privacy regulation on the Internet were up here seeking protection for their intellectual property on the Internet just three years ago. They demanded legislation to protect their books, records, music, and software from copyright infringement on the Internet. They insisted that such protection could be accomplished notwithstanding the rapidly changing technology of the online medium. Now, these same companies argue that any government attempt to protect privacy online can't possibly comport with the rapidly changing technology in the industry. It's funny how, on the one hand, they demand Congress protect their intellectual property online and, on the other hand, flatly oppose congressional efforts to protect consumers' personal information on the Internet.

The CHAIRMAN. Thank you very much, Senator Hollings.

Senator Stevens.

STATEMENT OF HON. TED STEVENS,
U.S. SENATOR FROM ALASKA

Senator STEVENS. That one was long enough, Senator. You have got me becoming the grandfather. I do not want to get in a fight with Al Gore.

Senator HOLLINGS. Well, we started it in defense.

Senator STEVENS. You are right about that.

Mr. Chairman, I thank you for holding this hearing. I hope we have a series of hearings. I think this is one of the most complex issues we will face in regard to the Internet. I was privileged to have a discussion with the chairman here this past week. I look forward to working on it with all of you.

But I do have a firm feeling that this is not an issue to be hasty about. So I am glad you are holding the hearing and I hope we can pursue and understand what we are doing before we bring out a bill from this Committee.

Thank you. By the way, I am pleased to see all the members of the Commission here and to see that it was a unanimous position taken by the Commission.

The CHAIRMAN. Thank you, sir. I think we may require more hearings on this issue. As you say, it is very complex and it is changing rather dramatically as we find out with the reports that we receive every year from the FTC.

Senator Wyden.

STATEMENT OF HON. RON WYDEN,
U.S. SENATOR FROM OREGON

Senator WYDEN. Thank you, Mr. Chairman. I, too, appreciate your scheduling the hearing. At the outset, I want to thank Senator Hollings for his kind comments. I think Senator Hollings' bill is a very credible and very significant product. I want to assure the Senator I am looking forward to working closely with him.

Mr. Chairman and colleagues, Senator Burns and I introduced more than a year ago an online privacy bill. At this point, when you have been following the issue it probably is a little hard to fig-

ure out how it can be that the last time the Federal Trade Commission surveyed prospects for self-regulation things seemed very rosy, and now it appears that prospects are pretty dire.

My sense is that we are going to find that reality is probably somewhere in between. The fact is that until this week's survey, the Commission has shown extraordinary patience and support for industry self-policing. My read of the Federal Trade Commission's report is that they are still showing support for self-regulation, but I think it is appropriate that they are showing a little less patience.

In my opinion, the privacy situation was never as rosy as the headlines that last year's survey had you believe. The reality then was that some of the surveyed privacy policies were just as flimsy as they are today. Further, there was virtually no enforcement, little accountability, and many less-visited Web sites were ignoring privacy altogether.

The truth today, I suspect, is that things are not nearly as dire as some would have us believe. While the same problems exist today that were in place at the time of the previous survey, there are important steps indicating progress. The seal programs, I think, are getting better at what they do, and it does seem that more Web sites are taking privacy more seriously.

But, for more than a year, Senator Burns and I, as I stated earlier, have worked on this on a bipartisan basis and have said that the costs are just too high to wait and see if self-regulation alone can tackle the bulk of the online privacy problem. None of us, none of us, want to see an Exxon Valdez of privacy that undermines the extraordinary growth of e-commerce.

So the worst thing that we could do now is set back the progress of self-regulatory efforts. But what I think makes the best sense is to build on those kinds of approaches. That is what Senator Burns and Senator Kohl and I have sought to do, to reward and build on the self-regulatory efforts while creating a baseline set of requirements to ensure that there are important consumer protection standards that would apply to those who are unwilling to take consumer privacy seriously.

Mr. Chairman, I would ask that the rest of my statement be part of the record. I look forward to hearing from Chairman Pitofsky and, again, commend Senator Hollings and Senator Rockefeller for what I think is a very important bill that they have introduced as well, and I yield back.

[The prepared statement of Senator Wyden follows:]

PREPARED STATEMENT OF HON. RON WYDEN, U.S. SENATOR FROM OREGON

I'm sure many who have been following the online privacy issue in the newspapers are asking themselves how the situation at the time of the last FTC survey could be so rosy, and could now be so dire. I would counsel them that the truth, as usual, probably lies somewhere in-between.

The fact is that until this week's survey, the Commission showed extraordinary patience and support for industry's effort at self-policing. And by my reading of the report, they are still showing support for self-regulation: just a little less patience.

Frankly, the privacy situation was never as rosy as the headlines from last year's survey would have had you believe. The reality was that some of the surveyed privacy policies were just as flimsy then as they are today. Further, there was virtually no enforcement, little accountability, and many less-visited Web sites were ignoring privacy altogether.

And the reality now, I suspect, is that things aren't nearly as dire as some would have us believe. While the same problems exist today as were in existence at the time of the previous survey, the seal programs are clearly maturing and getting better at what they do, and more Web sites are taking privacy seriously than ever before.

For over a year, however, I have been saying that the costs are simply too high to wait and see if self-regulation, alone, tackles the bulk of the online privacy problem. I am pleased that the Commission now agrees with Chairman Burns and myself on this point. We also agree—and look forward to their amplification of this point—that the worst thing we could do now is set back the progress of the self-regulatory efforts.

Chairman Burns, Senator Kohl, and I have legislation that is founded on the idea of rewarding and building on the industry's self-regulatory efforts, while creating a baseline of behavior for those who are unwilling to take consumer privacy seriously. We believe that if some regulation is necessary, the lightest practicable regulatory touch should be used to protect consumers. Sensible regulation need not, and should not, stifle private sector innovation.

Several other members now have introduced online privacy bills, or have bills in the works. Senator Hollings has a new privacy bill with Senator Rockefeller and others, and it strikes me as a very credible and significant effort. Their bill raises a number of important issues, such as consumer choice with regard to personally-identifiable information, and I look forward to the Committee reviewing both bills, and others, as the debate moves forward.

I'll let the Commission speak for itself, but I think it's clear from the report that the Commission isn't here today to bury self-regulation, but to praise it. I sure hope that's the case. I look forward to hearing from Chairmen Pitofsky and the rest of the Commission, and thank the Chairman for holding this timely and important hearing.

The CHAIRMAN. Senator Burns.

STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

Senator BURNS. Thank you, Mr. Chairman, and thank you for holding this hearing today, as this continues to be a great center of interest when we start talking about the Internet and related items around it.

I think we are charged with issues like this today. If the Internet and electronic commerce continue to grow, we have to do something about safety and security and privacy and these types of things for it to reach its real potential. We have been amazed at the continuing spectacular growth of the Internet, which has become a staple in modern life, it seems. The tremendous reach of the Internet does pose challenges as well as opportunities.

Unfortunately, digital technology can be used by bad actors to collect nearly limitless information on individuals without their knowledge. I am convinced that legislation is necessary to provide consumers with a safety net of privacy in the online world. As I stated in the hearing on privacy held in the Communications Subcommittee last summer, I am very disappointed—I was very disappointed—in the Federal Trade Commission's report on online privacy last year. The July 1999 report acknowledged that fewer than 10 percent of the Web sites met the basic privacy protections, yet called for no Federal legislation to address this critical situation.

However, at that time I was encouraged by the chairman's pledge that if the industry failed to produce strong progress the Commission would call for action in this area. The chairman and the Commission have been true to their word in the report issued to Congress just this last Monday, which called for legislation.

I want to take a moment to specifically commend the work and the insight of Commissioner Anthony on these privacy matters. In retrospect, her dissenting opinion in last year's report has proved to be absolutely correct. Last year she stated that the legislation was necessary to ensure a minimum consumer privacy protection in the digital area. In her statement she expressed concern that the absence of effective privacy protection would undermine consumer confidence and hinder the advancement of electronic commerce.

That is exactly what has happened in this past year. While e-commerce has continued to grow, several studies point out that the primary reason that is preventing more people from making purchases online and doing more business online is the lack of privacy. While the Internet has continued to exhibit massive growth, less than 1 percent of all consumer retail spending is done online. In short, e-commerce still has a huge up side potential, but the potential will never be fulfilled without basic assurance of consumer privacy.

I am going to submit the rest of my statement, but I want to thank Senator Wyden and his hard work on our legislation. It continues to be massaged and to be made better.

I also welcome the introduction of Senator Hollings' piece of legislation and look forward in working with Senator Hollings, because we can find and take care of this problem, because it has to be done in a bipartisan way and it is not a partisan situation where we start talking about these building blocks of the future e-commerce of this country. So we welcome all of these ideas, and I am sure that we will come up with a bill that we can all support. So I appreciate that very much.

I would ask unanimous consent that the rest of my statement be put in the record.*

The CHAIRMAN. Without objection.

Senator HOLLINGS. Who is next? Senator Bryan.

STATEMENT OF HON. RICHARD H. BRYAN, U.S. SENATOR FROM NEVADA

Senator BRYAN. Thank you very much.

First, I would like to preface my comments by thanking Chairman McCain for calling today's hearing on this important issue of Internet privacy. Second, I would like to commend the FTC for all the work that it has done over the past 5 years in the area of online privacy. Each of the FTC's three reports to Congress detailing online privacy practices and the numerous workshops and hearings they have held on this issue have contributed greatly to the ongoing dialog about the best way to protect the privacy of consumers on the Internet.

The protection of privacy is a core value of our democratic society. Although not mentioned explicitly in the Constitution, the Supreme Court has recognized that a fundamental right to privacy is embodied in both the Fourth and the Fourteenth Amendments to the Constitution. The right to privacy recognized by the court is a reflection of our citizenry's long-held expectation that they should

*The information referred to was not available at the time this hearing went to press.

be able to engage in a range of day to day activities with a significant degree of autonomy and confidentiality.

The Internet presents new challenges as well as new opportunities for the protection of privacy. The sheer volume of personal information that is exchanged on a daily basis between individuals and businesses on the Internet, coupled with the ability of other entities to track the flow of this information with relative ease, poses serious privacy concerns for many customers.

A recent survey showed that 92 percent of consumers are concerned about the misuse of their personal information online. Conversely, the architecture of the Internet provides an opportunity for technology to enhance online privacy. Many innovative companies are focusing more and more resources on the development of privacy-enhancing tools that will enable consumers to have more control over the use of their personal information.

I agree with the recommendation of the majority of the Commission that the time has come for the Congress to establish a baseline standard for the protection of consumer privacy on the Internet. Earlier this week, I was pleased to join the distinguished Ranking Member of this Committee, Senator Hollings, in introducing consumer privacy legislation that largely tracks the recommendations of the majority FTC report. This legislation builds upon the framework of legislation that was established in legislation that I offered in the children's online privacy protection, which just took effect last month. It embodies the four widely accepted fair information practices: notice, choice, access, and security for the collection of personally identifiable information about consumers online.

The Commission's report does indicate that the industry has made progress with self-regulatory initiatives. But in spite of this progress, however, I remain concerned about the effectiveness of online privacy seal programs, especially in the area of enforcement. I agree with the Commission that legislation is necessary to complement the industry's self-regulatory efforts in order to enhance adequate protection of consumer privacy.

I fully understand the industry's concerns with the regulatory approach to protecting privacy on the Internet. But I am hopeful, however, that they will come to view this effort as an opportunity to enhance consumer confidence in e-commerce, much like what occurred in the offline world with the credit card industry in the 1970's. I look forward to working with the industry, much as I did during the Committee's consideration of the Children's Online Privacy Protection Act, to enact a responsible piece of legislation that adequately protects consumer privacy online in a manner that does not unduly burden the growing importance of e-commerce in the marketplace.

Senator STEVENS [presiding]. Senator Ashcroft.

STATEMENT OF HON. JOHN ASHCROFT,
U.S. SENATOR FROM MISSOURI

Senator ASHCROFT. Thank you very much. Thank you very much, Mr. Chairman. Thank you for holding today's hearing.

I do not see this hearing as merely discussing a report from a Federal agency to Congress. I think this hearing will help us determine whether the Federal Government should develop a significant

and sweeping regulatory scheme. We are here to understand whether the growth of a flourishing high-tech industry would be hindered by such an involvement. We must discuss this issue in terms of whether or not the American people will be well served by significant government involvement in this dynamic industry.

We should ask ourselves whether it will continue to grow or will it continue to provide jobs, new opportunity, and education and research. We should ask whether the involvement of government bureaucrats will dramatically diminish the new efficiencies gained by conducting business on the Internet.

All of us are concerned about consumer privacy. I am concerned that consumers who want privacy should have privacy. In fact, Congress recently has recognized through statutes which apply to every segment of the economy that sensitive consumer information, such as financial and medical records, should be treated with extra care. I would point out that those regulations apply to everyone, not just companies who conduct business in the traditional brick and mortar sense. But the privacy laws which we now have in place already apply to companies doing business on the Internet.

However, through the fear-mongering from Washington, in some situations consumers have been led to believe that there are no protections in place on the Internet, and that is simply not true. Not only do our new privacy laws apply to Internet transactions, so do our consumer protection laws. In fact, we have heard glowing testimony before this Committee about the work of the FTC, about the work that the FTC has done to fight consumer fraud on the Internet. The Internet has even been credited with giving the FTC new and powerful tools to fight such fraud.

A few months ago the FTC Commissioners sat before this Committee to discuss this very issue, and at that time I was concerned that the latest Internet sweep was predestined to reach the conclusion contained in the Commission's report, that is that there need to be special regulations that apply to the Internet that do not apply to other collections of data, do not apply to other businesses, and do not apply to the other utilizations of data in our culture.

For example, when people promote through the distribution of coupons refund opportunities for individuals who buy products, people mail in those refund opportunities. There are not special laws that relate to what they can do with that information or how it can be used. It is not on the Internet, but it is the collection of consumer data and it is distributed widely.

Many people like the opportunity to participate in refund schemes and are willing to trade the value of the refund for the utilization of that information, which is consumer data, by businesses. It is a big part of the way we do business in this country. In our household, my wife scarcely lets a refund offer go by without collecting the labels necessary to cash in. As a matter of fact, she keeps a file of labels so that when the offer comes out she does not have to go buy additional products; she already has the labels ready to mail them in.

Now, I would just point out that I think we have got to be careful that we do not impose on the Internet unnecessary regulation that is differential, specially designed, and would curtail and confine the

Internet from operating in ways that we do not ask for responsibility or we do not ask for regulation on the rest of commerce.

Further, I think we ought to make sure that when we are talking about choice we allow people the choice of saying that they want to receive data based on the kinds of practices they have and they are interested, for instance, in getting offers from companies and the like based on the kinds of interest they have expressed in purchasing patterns, whether it be through refund coupons or other devices.

Although regulating the Internet was the recommendation following the sweep by the Commission, I am a little confused about how the numbers really move us toward that result. Two years ago a sweep showed that 14 percent of Web sites had privacy policies. Today 90 percent posted policies. That really says that, in an industry that showed a 543 percent improvement in 2 years, that it was deemed to be failing in self-regulation.

So in the interest of time and because the witnesses will address this issue, I will not mention all of the significant work done by industry to improve privacy and security on the net. I just want to say that I hope that we do not single out the Internet for a kind of regulation which would stifle it, which would limit the kinds of choices consumers have, and make the Internet a place where it would be difficult to grow business in the same way that it might be available for growth in other settings.

With that note, I want to indicate again how I respect privacy and want to be able to protect privacy, but I do not have a clear picture of how I want to inhibit information on the Internet that is not inhibited in other sectors of our economy.

Thank you.

Senator STEVENS. Senator Kerry.

STATEMENT OF HON. JOHN F. KERRY,
U.S. SENATOR FROM MASSACHUSETTS

Senator KERRY. Mr. Chairman, thank you very much.

I am delighted that Senator McCain has called this hearing. I think there is going to be a unanimity among most of us on the Committee, as there is probably among most Americans, that they want their privacy protected. I applaud the FTC and the analysis that they have put into this, and I particularly respect the effort of Senator Hollings and colleagues on the Committee who drafted some legislation and who have moved in that direction.

But I differ a little bit with some of them with respect to the degree to which at this stage, at a 5- or 6-year point in terms of the development of the net, that Congress has the ability to move adroitly enough, fast enough, with sufficient analysis and information, to be able to properly regulate something that is developing even as we sit here so rapidly, with so many technological advances that have the ability to answer some of our questions without our constricting the creativity and the efforts that are going into this.

It seems to me that there are certain principles we could adopt, for instance anonymity. What I hear from people in the industry is that the technology is moving fast enough that there are ways that the offerings of the marketplace are going to make it very clear to people that they can use one service or another that pro-

tects their privacy and protects their options, without our setting up a rigid, strict structure, at least at this point.

I think the FTC sort of adopted this up until this sudden point, and one of the questions today obviously is why there is the moment of departure. Maybe they do not think things have moved fast enough, obviously. But initially self-regulation was certainly their guiding theory, and this is the first moment of departure from that.

The opt-in requirement on the whole, while obviously I favor opt-in as a principle and I think most Americans are going to want that kind of choice and demand it in the marketplace, but in point of fact to mandate that actually sets a standard that in some cases in terms of marketplace behavior is neither necessary nor technologically sound. There are certain instances where certain kinds of marketing can take place that do no harm to people, they may choose to participate in it; you do not require that kind of burden.

I think the Committee is very much behind the curve, the country is behind the curve, in analyzing the degree to which we are drawing distinctions for the online world that we do not draw in the offline world. When you go to a local store here, let us say you go in Georgetown, you visit some store and buy a bunch of goods and you swish your card through the thing when you leave, that entity could determine everything you bought. They can market accordingly.

I mean, I must get 40 or 50 magazines every 3 weeks that are targeted based on my offline behavior. Yet we are about to require language restrictions that have no relationship to what is happening in the offline world, and I do not think we have thought that through adequately.

So I think there is a lot more analysis that needs to be done, and I am going to introduce legislation that I think will kind of balance these interests, where we can establish what we think are the goals and principles by which this ought to be in its earliest stages developed. There ought to be maximum amount of opt-in, there ought to be anonymity. Clearly, in the marketing you do not have to know that it is John Smith at Myrtle Street. You have to know that X number of goods are being bought in a certain area by certain demographics. But there are ways to protect the privacy without our becoming, I think, extraordinarily mandating at the federal level.

I might add to that that it seems to me there are very significant realities of the marketplace, that Americans are going to opt for those entities that most protect them if that is what indeed they want. And if they do not want it, they can also have the opportunity to make that kind of conscious choice.

There is clearly a difference between what happens in opt-in and opt-out. We all know it. I will wrap it up very quickly. We fought that out on the Banking Committee last year and in the Financial Modernization Act. It seems to me that also we have not really balanced some of those kinds of equities in how the market works.

In my judgment, Mr. Chairman, I think we have to be very, very careful on this Committee and in the Congress not to move fast. I think there are ways to protect Americans, to protect our interests, protect our prerogatives to come back, protect the capacity of

the FTC to, in fact, regulate and enforce and, if we were to set adequate standards and goals, the FTC would, in fact, be leveraged in its capacity to enforce, particularly if each company adopts its own privacy regime.

So I hope we are going to measure this carefully and not move overly rapidly, and I hope the Committee can find a consensus on this with some careful deliberation. Thank you, Mr. Chairman.

Senator STEVENS. Senator Gorton.

STATEMENT OF HON. SLADE GORTON,
U.S. SENATOR FROM WASHINGTON

Senator GORTON. I will pass.

Senator STEVENS. Thank you.

Senator Rockefeller.

STATEMENT OF HON. JOHN D. ROCKEFELLER IV,
U.S. SENATOR FROM WEST VIRGINIA

Senator ROCKEFELLER. Thank you, Mr. Chairman.

I do not think the problem is whether we move slowly or quickly. This Committee has a history of not reacting at all on issues that we do not understand and, therefore, we have got to give ourselves ample time.

Well, there is no such thing as ample time in the world of the net. There is no such thing as ample time if I have diabetes, for example, and that is my own private information and that gets out and it is sold to a third party, and there are not controls, and I cannot get a job. That example is used often.

This is a different world. To compare, as the Senator from Missouri did, this—"Missoura"—this medium that we are talking about to sort of other things and what transactions he and his wife might make at home, is behind the curve. This is a new world.

There has been a 548 percent increase in online disclosure and privacy policies. Of course that is exactly what the FTC looked at, and it is the quality of what the privacy policies say. Can you find them? Can you read them? Is the print big enough, and is it written in words that only those who are lawyers can understand? The American consumer is not always the most sophisticated, and the American consumer when on the net or on a Web site is almost always in a hurry and does not take the time. It is simply understanding human nature in a medium which is changing and then rechanging every 6 to 8 months.

So this is not a question of should we wait and make sure that we do absolutely the most perfect thing. There are hundreds of thousands or millions of people whose lives are going to be intervened with in ways that are dramatic and dangerous if this Committee does not pass a bill which supports what the FTC basically says. That is, that the work is not being done sufficiently.

I would remind the Senators from Massachusetts and Missouri that we heard all these same arguments back in the 1970's when the credit cards started up. The credit card industry was all over everybody saying that you cannot regulate us. And it was only, in fact, when we did put regulations on the credit card industry that the 90 percent of American consumers who at that time perhaps were not using credit cards or who are not at this point on Web

sites or using the Internet the way they might gained confidence in precisely the industry that had just gone through some form of regulation.

It was the regulation and thus the privacy and the access and the security that in fact helped the industry to attract users. So it is a cliche to say, but it is through judicious and cautious regulation not irrational exuberance that will help protect Americans and which will also help the industry grow.

We will make a mistake here if we apply traditional values to our legislative course.

Senator STEVENS. Thank you.

Senator Cleland, do you have an opening statement?

STATEMENT OF HON. MAX CLELAND,
U.S. SENATOR FROM GEORGIA

Senator CLELAND. Yes, sir, I do. Thank you very much, Mr. Chairman.

More and more as a Member of this Committee, I feel like I am in a cul de sac on the information highway. I am still struggling, trying to find out what it is all about. I was thinking this morning of how to equate what we are facing now with what I understood. I am from a small town, and it was not that many years ago in my little town that there were only four numbers involved with a telephone. And it was a totally public line. It was a party line, it used to be called, and basically everybody else knew each other's business. My State director, who is only 5 years older than I am, remembers when he would go home from school in the afternoon, pick up the phone, call the switchboard operator and say: Where is my mother? And she would say: Over at Gracie's.

I wonder if here in the early days of the Internet that everybody that is online is actually on a party line and does not know it.

The information superhighway began just a few short years ago as a footpath and now it is an unlimited expressway. People can now use the Internet to shop at virtual stores located thousands of miles away, find turn-by-turn directions to far away destinations, and journey to hamlets, cities, and states across the country.

While the virtual world is available to us with just a few keystrokes and mouse clicks, there is one area of the Internet that many are finding troublesome. It is the collection and use of personal data. All too often, web surfers are providing personal information about themselves without their knowledge and consent. It is a party line, except people do not know they are on a party line.

There is so much information being collected on people visiting Web sites today that it would take several buildings the size of the Library of Congress to store it all. That is a lot of information, much of which is very personal, and I believe it must be kept that way.

My concern about privacy on the Internet is that this issue is keeping people from fully enjoying the marvelous technology available to them. According to a recent survey by the Center for Democracy and Technology, consumers are fearful of the sale of their personal information to others and Web sites tracking people's use of the web. I think the term "cookies" is a fascinating term. I love cookies, but not this way.

This survey seems to be pointing to the same argument that was made when credit cards were first introduced to the American public. At that time credit cards did not initially enjoy widespread usage because of the potential misuse by others, but it was only after regulatory intervention to protect consumers that this fear was somewhat dispelled. We should learn this lesson from the Internet and the challenges that it is experiencing over privacy concerns.

These concerns are translating into lost opportunities for consumers and businesses. Now, most of the dot-com companies doing business over the Internet today are very cognizant of the fact that privacy is a major concern. However, in a report you just released, you found that 92 percent of the Web sites that you surveyed were collecting great amounts of personal information from consumers and only 14 percent disclosed anything about how the information would be used.

Interestingly enough, the report, your report, found that a mere 41 percent, less than half, of the randomly selected Web sites notified the visitor of their information practices and offered the visitor choices on how their personal information would be used. Now, this report seems to suggest to me that industry efforts by themselves are, indeed, not sufficient to control the gathering and dissemination of personal data.

At one Web site visit, a company can collect some very interesting facts about the person who is on the other end without them knowing it. While surfing the web the other day, I hit on a Web site that provided me with the insight into just how much information can be collected. In less than a minute, the site reported what other sites I had visited, what sites I would likely visit in the future, what plug-ins are installed on my PC, how my domain is configured, and a lot more information that I did not really understand.

Many consider this type of tracking akin to stalking. I believe that the information that can be collected by Web site administrators can create problems for people through a violation of trust and invasion of privacy. I would say, as an old Army signal officer, I know that you cannot communicate important data unless you have a feeling that it is secure. Novice Internet users generally are unaware, as I was until visiting this site, of the extent of information being collected on them. Even those who are aware of the capabilities of firms to collect private data are frightened by what can happen.

I believe in increasing the level of protection for private information to a level that the people of our nation and the dot-coms can live with, and I believe in providing assurances to those who are providing information that their privacy rights will be protected. It seems reasonable to me that firms that are collecting private data should notify consumers of the firm's information practices, offer the consumer choices on how the personal information will be used, allow consumers to access the information that is collected on them, and require those firms to take reasonable steps to protect the security of that information.

However, I am looking forward to learning more about the Internet privacy issue this morning and hearing from experts like these

wonderful people at the table, Mr. Chairman, and the rest of our distinguished testifiers.

Thank you very much.

The CHAIRMAN [presiding]. Chairman Pitofsky, welcome. I am sorry for the delay. I apologize to all the Commissioners. Chairman Pitofsky.

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

Mr. PITOFSKY. Thank you, Mr. Chairman, Senator Hollings, members of the Committee. I welcome this opportunity to once again appear before this Committee to discuss this important subject, especially because this Committee has supported so consistently and so well our efforts to deal with the kinds of problems we will discuss today.

As you know, the Commission has been active in the area of protecting consumers on the Internet since 1995. To a large extent we have dealt with fraud on the Internet, but we have also addressed questions of privacy.

We all know that the Internet commerce sector of the economy is growing at an amazing pace. But we also know that many people, some surveys say over 90 percent, are apprehensive about the way their private information is being used, including people who go ahead and buy things on the Internet.

Most observers believe that consumer protection would require four fair information practices. Incidentally, the business community in their seal programs and elsewhere have also indicated that these are the four bases that need to be touched.

First, notice: What information is being collected and what are the collectors doing with it? Consumers ought to know that.

Choice, the opportunity of consumers to say that we do not want this information used for any purpose other than completion of the transaction.

Most people also think that there ought to be some access, so if sensitive information is involved in the data base and it is wrong, there is an opportunity to correct it, so that consumers are not injured by errors.

The fourth practice involves an obligation to keep the information firms collect secure.

The debate really concerns whether these rights can be achieved through legislation or through growing efforts of responsible companies in the field to engage in self-regulation. My own view is that neither legislation alone nor self-regulation alone is the right answer, but it ought to be some combination of the two.

I applaud the progress that has been made in self-regulation in recent years. On the matter of notice, we have gone from 14 percent notice on all Web sites to 88 percent notice on all Web sites in a little over two years. The question has been raised: If that is the case, why has a majority of the Commission changed its view about the adequacy of self-regulation? I would make a number of points.

First of all, the 88 percent figure is a little misleading. It includes "notice" that says in effect, "we protect your privacy," or it could include notice that says, "we do not protect your privacy."

The fact of the matter is if you ask the questions, "how many of these notices actually tell consumers what information is collected and how it is used?" then the figure falls down to about 55 percent for all sites, 89 percent for the most visited sites.

If you ask the questions, "what about all four information practices? Are they being adequately addressed through self-regulation?," it turns out only 20 percent of firms on the Internet, one in five, have adopted all four fair information practices.

Some have said, "Well, but access and security are difficult to understand, the industry is slow to move in those two areas." All right, let us leave out access and security and ask only about notice and consent. There, on all Web sites, we find only 41 percent have notice and consent, 60 percent of the most traveled sites.

Finally, the whole notion of self-regulation requires that companies be part of seal programs and if they do not abide by self-regulatory standards, the seal will be taken away. Well, we find in that area, even though these seal programs have been working for over a year and a half, almost 2 years, 8 percent of Web sites are members of seal programs. That does not seem adequate.

What is to be done? First let me say again that self-regulation has achieved a good deal and has an important role to play in the future. I have always been a strong advocate of self-regulation. It works in many sectors of the economy. But I tell you on the basis of my experience that the most effective self-regulatory programs are those that have a rule of law to back them up, so that the self-regulators can then say to the irresponsible few who do not go along with the standards that their behavior will be referred to a law enforcement agency.

The idea that the self-regulators can go to the less responsible few and say, if you continue to collect and sell this information without permission at a profit to third parties we are going to take your seal of approval away from you, just does not get the job done. It helps, but it is not in my opinion adequate.

Second, I do believe that Congress must be cautious in this area and not impose on this growing and wonderful pro-consumer marketplace burdens that will hamper the development of the marketplace.

Third, as our report tries to emphasize, there are many complicated questions that arise here: What is adequate notice? How much access is required? What do we mean by "security"? Therefore, I applaud those who say that we should be careful; we should get it right rather than rush to any judgment in this area.

Any legislation should be sufficiently flexible so that if there are technological solutions—and we hear about them all the time—if they really develop then they should be incorporated and they should be allowed to protect consumers rather than direct government regulation.

Finally, an issue that has been raised by several: Why are we emphasizing consumer protection online and not offline? First of all, it is possible to manipulate data online in a very special way. But more important than that, in our report we address the question of online privacy. We have not examined the question of offline privacy. Slowly, I have come around to the view, as we have moved through this area, that the argument that offline and online should

be treated in a radically different way just does not hold up and we should be addressing whether or not consumers offline, deserve protection as well.

Let me conclude my remarks with a reference to some basic principles. Millions of people now enthusiastically shop online and they have no problem at all supplying personally identifiable information—names, addresses, credit card numbers if necessary, even social security numbers—if necessary to complete the transaction. But many sellers on the Internet are not just in the business of selling a product or selling a service, but rather they are in the business of accumulating data—the books we read, the music we hear, the pharmaceuticals and cosmetics we buy, our travel and vacation plans, the information we research, on and on and on. And that is often sold at a profit to third parties with whom we have no direct connection whatsoever. We do not even know who they are or what they are doing with that information.

Many people do not object to that either, as long as they have an opportunity to say to the online seller: "If that is what you are going to do with the data, just leave me out; I visited your Web site to buy a product, not to provide information about my life, my family, my habits, or my economic class."

I think that is the goal that virtually all of us share. We must make sure that that option is available to consumers on the Internet. They should not be required to forfeit their privacy online in exchange for the rich benefits of electronic commerce. Careful, nonburdensome legislation, backed up by effective self-regulation, and the legislation would set minimum standards, seems to me at this point the right way to go.

Thank you very much.

[The prepared statement of Chairman Pitofsky follows:]

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

Mr. Chairman, I am Robert Pitofsky, Chairman of the Federal Trade Commission. I appreciate this opportunity to present the Commission's views on the privacy issues raised by the collection and use of consumers' personal information by commercial sites on the World Wide Web.[1]

I. Introduction and Background

A. FTC Law Enforcement Authority

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

---

[1] The Commission vote to issue this testimony was 5–0. Commissioners Anthony, Thompson, Swindle, and Leary have issued separate statements, which are attached.

My oral testimony and any 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 also has responsibility under 45 additional statutes governing specific industries and practices. These include, for example, the Truth in Lending Act, 15 U.S.C. §§ 1601

Continued

B. Privacy Concerns in the Online Marketplace

Since its inception in the mid-1990's, the online consumer marketplace has grown at an exponential rate. Recent figures suggest that as many as 90 million Americans now use the Internet on a regular basis.[4] Of these, 69%, or over 60 million people, shopped online in the third quarter of 1999.[5] In addition, the Census Bureau estimates that retail e-commerce reached $5.3 billion for the fourth quarter of 1999.[6]

At the same time, technology has enhanced the capacity of online companies to collect, store, transfer, and analyze vast amounts of data from and about the consumers who visit their Web sites. This increase in the collection and use of data, along with the myriad subsequent uses of this information that interactive technology makes possible, has raised public awareness and consumer concerns about online privacy. Recent survey data demonstrate that 92% of consumers are concerned (67% are "very concerned") about the misuse of their personal information online.[7] The level of consumer unease is also indicated by a recent study in which 92% of respondents from online households stated that they do not trust online companies to keep their personal information confidential.[8] To ensure consumer confidence in this new marketplace and its continued growth, consumer concerns about privacy must be addressed.[9]

---

et seq., which mandates disclosures of credit terms, and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 *et seq.,* which provides for the correction of billing errors on credit accounts. The Commission also enforces over 30 rules governing specific industries and practices, *e.g.,* the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices; and the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312.

In addition, on May 12, 2000, the Commission issued a final rule implementing the privacy provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 *et seq.* The rule requires a wide range of financial institutions to provide notice to their customers about their privacy policies and practices. The rule also describes the conditions under which those financial institutions may disclose personal financial information about consumers to nonaffiliated third parties, and provides a method by which consumers can prevent financial institutions from sharing their personal financial information with nonaffiliated third parties by opting out of that disclosure, subject to certain exceptions. The rule is available on the Commission's Web site at <http://www.ftc.gov/os/2000/05/index.htm#12>. *See Privacy of Consumer Financial Information,* to be codified at 16 C.F.R. pt. 313.

The Commission does not, however, have criminal law enforcement authority. Further, under the FTCA, 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) and (6)a of the FTC Act, 15 U.S.C. § 45(a)(2) and 46(a). *See also* The McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

[4] The Intelliquest Technology Panel, *Panel News,* available at <http://www.techpanel.com/news/index.asp> [hereinafter "Technology Panel"] (90 million adult online users as of third-quarter 1999). Other sources place the number in the 70–75 million user range. *See* Cyber Dialogue, *Internet Users,* available at <http://www.cyberdialogue.com/resource/data/ic/index.html> (69 million users); Cyberstats, *Internet Access and Usage, Percent of Adults 18+,* available at <http://www.mediamark.com/cfdocs/MRI/cs_f99a.cfm> (75 million users).

[5] Technology Panel. This represents an increase of over 15 million online shoppers in one year. *See id.*

[6] United States Department of Commerce News, *Retail E-commerce Sales for the Fourth Quarter 1999 Reach $5.3 Billion, Census Bureau Reports* (Mar. 2, 2000), available at <http://www.census.gov/mrts/www/current.html>.

[7] Alan F. Westin, *Personalized Marketing and Privacy on the Net: What Consumers Want,* Privacy and American Business at 11 (Nov. 1999) [hereinafter "Westin/PAB 1999"]. *See also IBM Multi-National Consumer Privacy Survey* at 72 (Oct. 1999), prepared by Louis Harris & Associates Inc. [hereinafter "IBM Privacy Survey"] (72% of Internet users very concerned and 20% somewhat concerned about threats to personal privacy when using the Internet); Forrester Research, Inc., *Online Consumers Fearful of Privacy Violations* (Oct. 1999), available at <http://www.forrester.com/ER/Press/Release/0,1769,177,FF.html> (two-thirds of American and Canadian online shoppers feel insecure about exchanging personal information over the Internet).

[8] *Survey Shows Few Trust Promises on Online Privacy,* Apr. 17, 2000, available at <http://www.nyt.com> (citing recent Odyssey survey).

[9] The Commission, of course, recognizes that other consumer concerns also may hinder the development of e-commerce. As a result, the agency has pursued other initiatives such as combating online fraud through law enforcement efforts. *See FTC Staff Report: The FTC's First Five Years Protecting Consumers Online* (Dec. 1999). The Commission, with the Department of Commerce, is also holding a public workshop and soliciting comment on the potential issues associated with the use of alternative dispute resolution for online consumer transactions. *See* Initial Notice Requesting Public Comment and Announcing Public Workshop, 65 Fed. Reg. 7,831 (Feb. 16, 2000); Notice Announcing Dates and Location of Workshop and Extending Deadline for Public Comments, 65 Fed. Reg. 18,032 (Apr. 6, 2000). The workshop will be held on June 6 and 7, 2000. Information about the workshop, including the federal register notices and public comments received, is available at <http://www.ftc.gov/bcp/altdisresolution/index.htm>.

C. The Commission's Approach to Online Privacy—Initiatives Since 1995

Since 1995, the Commission has been at the forefront of the public debate concerning online privacy.[10] The Commission has held public workshops; examined Web site information practices and disclosures regarding the collection, use, and transfer of personal information; and commented on self-regulatory efforts and technological developments intended to enhance consumer privacy. The Commission's goals have been to understand this new marketplace and its information practices, and to assess the costs and benefits to businesses and consumers.[11]

In June 1998 the Commission issued *Privacy Online: A Report to Congress* ("1998 Report"), an examination of the information practices of commercial sites on the World Wide Web and of industry's efforts to implement self-regulatory programs to protect consumers' online privacy.[12] The Commission described the widely-accepted fair information practice principles of *Notice, Choice, Access* and *Security*. The Commission also identified *Enforcement*—the use of a reliable mechanism to provide sanctions for noncompliance—as a critical component of any governmental or self-regulatory program to protect privacy online.[13] In addition, the 1998 Report presented the results of the Commission's first online privacy survey of commercial Web sites. While almost all Web sites (92% of the comprehensive random sample)

---

[10] The Commission's review of privacy has mainly focused on online issues because the Commission believes privacy is a critical component in the development of electronic commerce. However, the FTC Act and most other statutes enforced by the Commission apply equally in the offline and online worlds. As described *infra,* n.11, the agency has examined privacy issues affecting both arenas, such as those implicated by the Individual Reference Services Group, and in the areas of financial and medical privacy. It also has pursued law enforcement, where appropriate, to address offline privacy concerns. *See FTC v. Rapp,* No. 99–WM–783 (D. Colo. filed Apr. 21, 1999); *In re Trans Union,* Docket No. 9255 (Feb. 10, 2000), *appeal docketed,* No. 00–1141 (D.C. Cir. Apr. 4, 2000). These activities—as well as recent concerns about the merging of online and offline databases, the blurring of distinctions between online and offline merchants, and the fact that a vast amount of personal identifying information is collected and used offline—make clear that significant attention to offline privacy issues is warranted.

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

The Commission and its staff have also issued reports describing various privacy concerns in the electronic marketplace. *See, e.g., FTC Staff Report: The FTC's First Five Years Protecting Consumers Online* (Dec. 1999); *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). Recently, 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 (required by the Health Insurance Portability and Accountability Act of 1996). 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. The Commission's comments are available at <http://www.ftc.gov/be/v000001.htm>.

The Commission also has brought law enforcement actions to protect privacy online pursuant to its general mandate to fight unfair and deceptive practices. *See FTC v. ReverseAuction.com, Inc.,* No. 00–0032 (D.D.C. Jan. 6, 2000) (consent decree) (settling charges that an online auction site obtained consumers' personal identifying information from a competitor site and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business); *Liberty Financial Companies, Inc.,* FTC Dkt. No. C–3891 (Aug. 12, 1999) (consent order) (challenging the allegedly false representations by the operator of a "Young Investors" Web site that information collected from children in an online survey would be maintained anonymously); *GeoCities,* FTC Dkt. No. C–3849 (Feb. 12, 1999) (consent order) (settling charges that Web site misrepresented the purposes for which it was collecting personal identifying information from children and adults).

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

[13] 1998 Report at 11–14.

were collecting great amounts of personal information from consumers, few (14%) disclosed anything at all about their information practices.[14]

Based on survey data showing that the vast majority of sites directed at children also collected personal information, the Commission recommended that Congress enact legislation setting forth standards for the online collection of personal information from children.[15] The Commission deferred its recommendations with respect to the collection of personal information from online consumers generally. In subsequent Congressional testimony, the Commission discussed promising self-regulatory efforts suggesting that industry should be given more time to address online privacy issues. The Commission urged the online industry to expand these efforts by adopting effective, widespread self-regulation based upon the long-standing fair information practice principles of Notice, Choice, Access, and Security, and by putting enforcement mechanisms in place to assure adherence to these principles.[16]

Last year, Georgetown University Professor Mary Culnan conducted a survey of a random sample drawn from the most-heavily trafficked sites on the World Wide Web as well as a survey of the busiest 100 sites.[17] The former, known as the Georgetown Internet Privacy Policy Survey, found significant improvement in the frequency of privacy disclosures, but also that only 10% of the sites posted disclosures that even touched on all four fair information practice principles.[18] Based in part on these results, a majority of the Commission recommended in its 1999 report to Congress, Self-Regulation and Privacy Online, that self-regulation be given more time, but called for further industry efforts to implement the fair information practice principles.[19]

This week the Commission issued its third report to Congress examining the state of online privacy and the efficacy of industry self-regulation. *Privacy Online: Fair Information Practices in the Electronic Marketplace* ("2000 Report")* presents the results of the Commission's 2000 Online Privacy Survey, which reviewed the nature and substance of U.S. commercial Web sites' privacy disclosures, and assesses the effectiveness of self-regulation. The 2000 Report also considers the recommendations of the Commission-appointed Advisory Committee on Online Access and Security.[20] Finally, the Report sets forth the Commission's conclusion that legislation is necessary to ensure further implementation of fair information practices online and recommends the framework for such legislation.[21]

---

[14] *Id.* at 23, 27.

[15] *Id.* at 42–43. In October 1998, Congress enacted the Children's Online Privacy Protection Act of 1998 ("COPPA"), which authorized the Commission to issue regulations implementing the Act's privacy protections for children under the age of 13. 15 U.S.C. §§ 6501 *et seq.* In October 1999, as required by COPPA, the Commission issued its Children's Online Privacy Protection Rule, which became effective last month. 16 C.F.R. Part 312.

[16] *See* Prepared Statement of the Federal Trade Commission on "Consumer Privacy on the World Wide Web" before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce, U.S. House of Representatives (July 21, 1998), available at <http://www.ftc.gov/os/1998/9807/privac98.htm>.

[17] The results for the random sample of 361 Web sites are reported in *Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission* (June 1999), available at <http://www.msb.edu/faculty/culnanm/gippshome.html> [hereinafter "GIPPS Report"]. The results of Professor Culnan's study of the top 100 Web sites, conducted for the Online Privacy Alliance, are reported in Online Privacy Alliance, *Privacy and the Top 100 Sites: Report to the Federal Trade Commission* (June 1999), available at <http://www.msb.edu/faculty/culnanm/gippshome.html> [hereinafter "OPA Report"].

[18] *See* GIPPS Report, Appendix A, Table 8C.

[19] *Self-Regulation and Privacy Online* (July 1999) at 12–14 (available at <http://www.ftc.gov/os/1999/9907/index.htm#13>).

* The information referred to has been retained in Committee files.

[20] On December 1999, the Commission established the Federal Trade Commission Advisory Committee on Online Access and Security, pursuant to the Federal Advisory Committee Act, 5 U.S.C. App. §§ 1–15. Notice of Establishment of the Federal Trade Commission Advisory Committee on Online Access and Security and Request for Nominations, 64 Fed. Reg. 71,457 (1999).

The Commission asked the Advisory Committee, a group comprising 40 e-commerce experts, industry representatives, security specialists, and consumer and privacy advocates, to consider the parameters of "reasonable access" to personal information collected from and about consumers online and "adequate security" for such information, and to prepare a report presenting options for implementation of these fair information practices and the costs and benefits of each option. The duties of the Advisory Committee were solely advisory. The Advisory Committee Report and proceedings are available at <http://www.ftc.gov/acoas>.

[21] The Commission vote to issue the 2000 Report was 3–2, with Commissioner Swindle dissenting and Commissioner Leary concurring in part and dissenting in part. Both Commissioners' separate statements are attached to the Report. Copies of the 2000 Report and of the report of the Advisory Committee on Online Access and Security are attached.* The Reports are also available at <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf> and <http://

II. Fair Information Practices in the Electronic Marketplace: The Results of the 2000 Survey

In February and March 2000, the Commission conducted a survey of commercial sites' information practices, using a list of the busiest U.S. commercial sites on the World Wide Web.[22] Two groups of sites were studied: (a) a random sample of 335 Web sites (the "Random Sample") and (b) 91 of the 100 busiest sites (the "Most Popular Group").[23] As was true in 1998, the 2000 Survey results show that Web sites collect a vast amount of personal information from and about consumers. Almost all sites (97% in the Random Sample, and 99% in the Most Popular Group) collect an e-mail address or some other type of personal identifying information.[24]

The 2000 Survey results also show that there has been continued improvement in the percent of Web sites that post at least one privacy disclosure (88% in the Random Sample and 100% in the Most Popular Group).[25] The Commission's 2000 Survey went beyond the mere counting of disclosures, however, and analyzed the nature and substance of these privacy disclosures in light of the fair information practice principles of *Notice, Choice, Access,* and *Security*. It found that only 20% of Web sites in the Random Sample that collect personal identifying information implement, at least in part, all four fair information practice principles (42% in the Most Popular Group).[26] While these numbers are higher than similar figures obtained in Professor Culnan's studies, the percentage of Web sites that state they are providing protection in the core areas remains low. Further, recognizing the complexity of implementing Access and Security as discussed in the Advisory Committee report, the Commission also examined the data to determine whether Web sites are implementing Notice and Choice only. The data showed that only 41% of sites in the Random Sample and 60% of sites in the Most Popular Group meet the basic Notice and Choice standards.[27]

The 2000 Survey also examined the extent to which industry's primary self-regulatory enforcement initiatives—online privacy seal programs—have been adopted. These programs, which require companies to implement certain fair information practices and monitor their compliance, promise an efficient way to implement privacy protection. However, the 2000 Survey revealed that although the number of sites enrolled in these programs has increased over the past year,[28] the seal programs have yet to establish a significant presence on the Web. The Survey found that less than one-tenth, or approximately 8%, of sites in the Random Sample display a privacy seal. Moreover, less than one-half, or 45%, of the sites in the Most Popular Group display a seal.[29]

III. Commission Recommendations

Based on the past years of work addressing Internet privacy issues, including examination of prior surveys and workshops with consumers and industry, it is evident that online privacy continues to present an enormous public policy challenge.[30] The Commission applauds the significant efforts of the private sector and commends industry leaders in developing self-regulatory initiatives. The 2000 Survey, however, demonstrates that industry efforts alone have not been sufficient. Because self-regulatory initiatives to date fall far short of broad-based implementation of effective self-regulatory programs, a majority of the Commission has concluded that such efforts alone cannot ensure that the online marketplace as a whole will emulate the standards adopted by industry leaders. While there will continue to be a major role for industry self-regulation in the future, a majority of the Commission recommends that Congress enact legislation that, in conjunction with continuing self-regulatory programs, will ensure adequate protection of consumer privacy online.

---

www.ftc.gov/acoas/papers/finalreport.htm>, respectively. *The information referred to has been retained in Committee files.

[22] The list of Web sites was provided by Nielsen//NetRatings based upon January 2000 traffic figures. 2000 Report, Appendix A.

[23] 2000 Report at 7, 9 and Appendix A.

[24] 2000 Report at 9.

[25] *Id.* at 10.

[26] *Id.* at 12–13.

[27] *Id.* at 13–14.

[28] *Id.* at 6–7.

[29] *Id.* at 20.

[30] As noted earlier, *supra* n.10, and as illustrated by legislative decisions made in the areas of medical and financial privacy, offline privacy issues are also significant.

The proposed legislation would set forth a basic level of privacy protection for consumer-oriented commercial Web sites.[31] Such legislation would establish basic standards of practice for the collection of information online, and provide an implementing agency with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act.[32]

Consumer-oriented commercial Web sites that collect personal identifying information from or about consumers online would be required to comply with the four widely-accepted fair information practices:

(1) **Notice**—Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (*e.g.,* directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.[33]

(2) **Choice**—Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (*e.g.,* to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).

(3) **Access**—Web sites would be required to offer 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.

(4) **Security**—Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers.

The Commission recognizes that the implementation of these practices may vary with the nature of the information collected and the uses to which it is put, as well as with technological developments. For this reason, a majority of the Commission recommends that any legislation be phrased in general terms and be technologically neutral. Thus, the definitions of fair information practices set forth in the statute should be broad enough to provide flexibility to the implementing agency in promulgating its rules or regulations.

Finally, the Commission notes that industry self-regulatory programs would continue to play an essential role under such a statutory structure, as they have in other contexts.[34] The Commission hopes and expects that industry and consumers would participate actively in developing regulations under the new legislation and that industry would continue its self-regulatory initiatives. The Commission also recognizes that effective and widely-adopted seal programs could be an important component of that effort.

For all of these reasons, a majority of the Commission believes that its proposed legislation, in conjunction with self-regulation, will ensure important protections for consumer privacy at a critical time in the development of the online marketplace. Without such protections, electronic commerce will not reach its full potential and consumers will not gain the confidence they need in order to participate fully in the online marketplace.

---

[31] Legislation should cover such sites to the extent not already covered by the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501 *et seq.*

[32] 5 U.S.C. § 553.

[33] The Commission will soon be addressing the issue of third-party online collection of personal information for profiling purposes in a separate report to Congress.

[34] For example, the program administered by the National Advertising Division of the Council of Better Business Bureaus, Inc. ("NAD") is a model self-regulatory program that complements the Commission's authority to regulate unfair and deceptive advertising. The NAD expeditiously investigates complaints made by consumers or competitors about the truthfulness of advertising. An advertiser that disagrees with the NAD's conclusion may appeal to the National Advertising Review Board ("NARB"), which includes members from inside and outside the advertising industry. The vast majority of disputes handled by the NAD and NARB are resolved without government intervention, resulting in greater respect for and enforcement of the law at a substantial savings to the taxpayer. Those disputes that the NAD and NARB are unable to resolve are referred to the Commission.

The Commission also has a long record of working with industry to develop and disseminate informational materials for the public. *See, e.g.,* Notice of Opportunity to Participate and Obtain Co-Sponsorship in Agency Public Awareness Campaign re: Children's Online Privacy Protection Rule, available at <http//:www.ftc.gov/os/2000/05/index.htm#12>.

IV. Conclusion

The Commission is committed to the goal of assuring fair information practices for consumers online, and looks forward to working with the Committee as it considers the Commission's Report and proposals for protecting online privacy.

The CHAIRMAN. I thank you, Chairman Pitofsky.

I would tell the other Commissioners, your complete statement will be made part of the record and if you could summarize we would very much appreciate it. But at the same time, we do not want to prevent the Committee from receiving all the information you wish to convey.

Commissioner Anthony.

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

Ms. ANTHONY. Thank you, Mr. Chairman. I am delighted to be here today and I am pleased that the Commission is recommending Federal legislation——

Senator STEVENS. Would you pull that mike up to you, please.

Ms. ANTHONY. Sure.

I am pleased that the Commission is recommending legislation necessary to protect consumer privacy. I wish to emphasize four points related to our legislative recommendation:

One, any quality privacy policy should offer true protections to consumers and be presented in a simple format that is clear and understandable;

Two, an enforcement mechanism must be in place that gives consumers confidence that Web sites do what they say they do with consumers' personal data;

Three, a patchwork of State privacy laws will result in confusion both to consumers and businesses, and thus Federal preemption should at least be seriously considered;

Four, implementation of consumer consent via opt-in and opt-out may require making a distinction between market information and sensitive health and financial information.

The 2000 survey reports that 97 percent of the random sample and 99 percent of the most popular group collect personally identifying information, but only 20 percent of the random sample and just 42 percent of the most popular group address, at least in part, all four information practices.

Seal programs and audits can be key enforcement mechanisms. Yet only 8 percent in the random sample and 45 percent of the most popular group display a seal.

Perhaps more troubling to me is that many privacy policies are confusing, contradictory, and ambiguous. I reviewed some of the privacy policies in the most popular group of Web sites in our survey. Frankly, I was disappointed. Almost half of the policies are too long, varying from 3 to 12 pages. Many try to lull a consumer into a false sense of comfort. Despite opening statements asserting the importance of the user's privacy, subsequent paragraphs frequently contain contradictory information.

Consider the following language in an Internet service provider's published privacy policy. The first sentence states: "Your privacy is important to us," but continues several paragraphs later: "The personal information we collect from members during the registration

process is used to manage each member's account. This information is not shared with third parties unless specifically stated otherwise or in special circumstances."

Three pages later, the same policy goes on to say: "We may disclose personal information about our visitors or members or information regarding your use of the services or Web sites accessible through our services for any reason if, in our sole discretion, we believe it is reasonable to do so."

Would you call this a clear, unambiguous disclosure? I do not. Does it inform consumers about whether his or her information will be shared and, if so, with whom? I do not believe it does.

My next example illustrates serious concerns with regard to meaningful consent. I quote from a privacy policy statement from one of the top 100 sites: "When you submit personal information to us, you understand and agree that our subsidiaries, affiliates, and trusted vendors may transfer, store, and process your customer profile in any of the countries in which we and our affiliates maintain offices."

Has the site identified with specificity the parties with whom it will share this consumer's information? Is consent meaningful if consumers do not see this notice or have access to it at the time they supply their personal information?

Even a policy that incorporates all four fair information practices can be ambiguous and contradictory. What do you make of this privacy policy that contains the following disclaimer: "This statement and the policies outlined herein are not intended to and do not create any contractual or other legal rights in or on behalf of any party." This disclaimer seems to absolve the site of any responsibility to protect a consumer's information. It reminds me of a letter I once received from a lawyer which had the following postscript: "Dictated but not read."

I do not think it is difficult to design a standardized, conspicuous privacy notice that informs consumers in an unambiguous, non-contradictory way. The chart, which is attached to my testimony and is what you see here, tells the viewer most of what she needs to know about a Web site's privacy practices and consumer choices. Web sites can take advantage of the interactive nature of the Internet to design effective mechanisms and to provide meaningful notice or privacy policies.

I share Commissioner Leary's view that a comprehensive privacy policy for consumers must extend to the offline world. The business incentive to compete simultaneously in both the offline and online worlds is high. To create a distinction between offline and online is artificial and outdated and in the long run may foster market barriers.

Finally, I want to commend the FTC staff for the hard work they have done on this report. The Bureau of Consumer Protection, with the assistance of the Bureau of Economics, designed and implemented this survey, and the numbers were reported clearly, fairly, and without bias.

Thank you for allowing me to share my views.

[The prepared statement of Commissioner Anthony follows:]

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

Mr. Chairman and members of the Committee, I am delighted to be here this morning, and I appreciate your holding this hearing to address a topic of great importance to the American people and critical to the growth and success of electronic commerce.

I am pleased the Commission is recommending that federal legislation is necessary to protect consumer privacy. Survey after survey demonstrates that public concerns about privacy have been growing and that these concerns have focused on the power of technologies to collect, store, search, and transmit large amounts of personally identifiable information. I not only share those concerns, I note that threats to consumer privacy are increasing with the merging of the offline and online worlds. In short, things may be getting worse for Americans on the privacy front.

I wish to emphasize four points related to the legislative recommendation the Commission makes to you today:

1) Any quality privacy policy should offer true protections to consumers and be presented in a simple format that is clear and understandable.

2) An enforcement mechanism must be in place that gives consumers confidence that Web sites do what they say they will do with consumers' personal data. While the seal of approval programs offer promise, 92 percent of the surveyed sites did not have a privacy seal from one of the industry-established programs. There may be some advantage to building on industry standards that utilize audits.

3) A patchwork of state privacy laws will result in confusion to both consumers and businesses, and thus federal pre-emption should be, at least, seriously considered. People value uniformity and predictability.

4) Implementation of consumer consent, via opt-in and opt-out methods, may require making a distinction between market information and sensitive health and financial information.

A. Fair Information Principles Are Widely Accepted

In the Commission's first Privacy Report in 1998, we summarized four widely accepted principles regarding the collection, use, and dissemination of personal information. These core principles of privacy protection are common to government reports, guidelines, and model codes, and predate the online medium:

- 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 assure that information collected from consumers is accurate and secure from unauthorized use.

B. The Vast Majority of Web sites Collect Personal Data But Do Not Provide Privacy Protections

The percentage of commercial Web sites that collect personally identifying information is very high. The 2000 Survey reports that 97 percent of the Random Sample and 99 percent of the Most Popular Group collect personally identifying information, but the percentage providing aspects of these fair information practices is still quite low. The 2000 Survey reports that only 20 percent of the Random Sample and just 42 percent of the Most Popular Group address, at least in part, all four fair information practices. In fact, these results likely overstate the percentage of sites that truly implement the fair information practices in a meaningful way. Our content analysts credited policies if the stated practices applied to any of the information collected, even if it did not apply to all the information collected.[1]

[1] The 2000 Survey analysis gave Access credit for informational statements about *any* one of three elements (review, correction or deletion). However, the Commission previously stated that fair information practices require that consumers be afforded *both* an opportunity to review in-

Continued

C. Policies Posted By Web sites Are Confusing and Contradictory

Perhaps more troubling to me is that many privacy policies are confusing, contradictory, and ambiguous. What good is a privacy policy that is not understandable by ordinary consumers, is contradictory from paragraph to paragraph, or fails to offer basic protections?

I reviewed some of the privacy policies of the Most Popular Group of Web sites in the survey. Frankly, I was disappointed. Almost half of the privacy polices are too long, varying from 3–12 pages. Many try to lull the consumer into a false sense of comfort by utilizing opening statements regarding the importance of respecting individual privacy or by referring to third parties as "trusted vendors" or those with whom there is an "established agreement to protect your privacy." Despite the opening statements asserting the importance of the user's privacy, subsequent paragraphs frequently contain contradictory information. After reviewing some of these policy statements, I am left to wonder whether:

- these policies truly inform consumers
- the Web sites have something to hide
- the Web sites themselves are confused about their own policies
- the drafting lawyers have run amok.

Consider the following language in an Internet Service Provider's published Privacy Policy.

The first sentence states:

> Your privacy is very important to us.

But, continues several paragraphs later:

> The personal information we collect from members during the registration process is used to manage each member's account. This information is not shared with third parties unless specifically stated otherwise or in special circumstances.

Three pages later, the same policy goes on to say:

> [We] may disclose personal information about our visitors or members or information regarding your use of the Services or Web sites accessible through our Services, for any reason if, in our sole discretion, we believe that it is reasonable to do so, . . .

Would you call this a clear, unambiguous disclosure? I do not. Does it inform the consumer about whether his or her information will be shared and, if so, with whom? I do not believe it does.

My next example illustrates serious concerns with regard to meaningful consent. I quote from a privacy policy statement from one of the top 100 sites:

> When you submit personal information to [us] you understand and agree that our subsidiaries, affiliates and trusted vendors may transfer, store, and process your customer profile in any of the countries in which we and our affiliates maintain offices.

Has the site identified with specificity the parties with whom it will share customer information? Is consent meaningful if consumers do not see this notice or have access to it at the time they surrender their personal information?

Even a policy statement that incorporates all of the four fair information practices may still be ambiguous and contradictory. What do you make of a privacy policy that contains the following disclaimer:

> These policies are effective as of [x date]. [This site] reserves the right to change the policy at any time by notifying users of the existence of a new privacy statement. This statement and the policies outlined herein are not intended to and do not create any contractual or other legal rights in or on behalf of any party.

I wonder through what means consumers will be notified of changes in the policy statement. How will data collected pursuant to one policy be treated under a new policy? Must consumers "check back" from time to time? The disclaimer, quoted

---

formation *and* an opportunity to contest the data's accuracy or completeness. Under this standard, only 11% of the random and 27% of the Most Popular Group would receive credit for providing Access rather than the 18% of the random and 47% of the Most Popular Group calculated using an expansive measure.

above, seems to absolve the site of any responsibility to protect a consumer's information. It reminds me of a letter I once received from a lawyer, which had the following post script: "Dictated, but not read."

D. An Increase in Posted Privacy "Policies" Does Not Correlate with Increased Privacy Protections

Although the survey demonstrates some increase in the percentage of sites posting privacy policies, these policies all too often do not offer privacy protections. While Web sites *should* be offering privacy protections, a whopping 80 percent of the surveyed Web sites in the Random Sample failed to implement aspects of notice, choice, access, and security.

E. No Enforcement Tools Exists to Ensure Sites Do What They Say

For years the Commission has urged industry to engage in meaningful self-regulatory efforts. For self-regulation to be credible, there must be an enforcement mechanism that gives consumers confidence that Web sites do what they say they do with consumers' personal data. Seal programs and audits can be key enforcement mechanisms. Yet, 92 percent of the surveyed Web sites in the Random Group did not have a privacy seal. Our legislative recommendation would reward those sites that have offered meaningful privacy protections and would require all others to meet basic privacy standards. It would also give consumers the assurance that a legal structure is in place to provide confidence that stated privacy polices will be honored.

F. A Standardized Privacy Notice May be Useful: See Chart

How difficult is it to design a conspicuous privacy notice that informs consumers in a standardized, unambiguous, non-contradictory way? Not very difficult. Appended to this testimony is a simple chart that tells the viewer most of what she needs to know about a Web site's privacy practices and consumer choices. Web sites can take advantage of the interactive nature of the Internet to design effective mechanisms to provide meaningful notice or privacy policies.

G. Profiling is Invisible and Threatens Consumer Privacy

Profiling is beyond the scope of this report, and I believe it will be the subject of a later Commission report. Profiling poses a serious privacy threat to consumers because it is largely invisible to them. I am concerned about the passive, surreptitious collection of information about consumers and their browsing habits without their knowledge. Our report notes that third party cookies are placed by ad servers on 78 percent of the sites in the Most Popular Group. Of those sites, only 51 percent disclose to consumers that they have allowed third party cookies to be placed (and they usually locate that disclosure at the end of the policy statement). Unless consumers are technically skilled enough to set their browser to alert them to cookies or to decline all third party cookies, the placement of third party cookies generally goes unnoticed by consumers.

H. Online, Offline: What's the Difference?

Finally, I share Commissioner Leary's view that a comprehensive privacy policy for consumers must extend to the offline world. Traditional brick and mortar businesses no longer store and maintain their customer records on index cards. The data businesses have collected offline are often transferred to computers and can be merged with online databases with a simple click of a button. The business incentive to compete simultaneously in both the online and offline worlds is high. To create a distinction between the offline and online worlds is artificial and outdated and in the long run may foster market barriers.

Finally, I want to commend the FTC staff for the excellent job they have done on this Report. The Bureau of Consumer Protection, with the assistance of the Bureau of Economics, designed and implemented the survey that formed the basis of this report. The survey numbers were reported clearly, fairly, and without bias. My hat is off to them.

I appreciate the opportunity to express my views.

Sample Privacy Policy

We collect Personally Identifiable Information about you	☐ Yes	☐ No	Click *here* to see what kinds of EJNo information we collect
We use your personal information to notify you of our future promotions	☐ Yes	☐ No	Click *here* to opt out/opt in
We share information about you with Third Parties for marketing purposes. Click *here* to see who we share information with	☐ Yes	☐ No	Click *here* to opt out/opt in
You may review and correct or delete information about yourself (with proper authentication)	☐ Yes	☐ No	Click *here* to access our database. Have your Membership # and Pin # ready.
We provide reasonable security to protect your personal information during its transmission and while it is in our possession	☐ Yes	☐ No	

The CHAIRMAN. Thank you very much, Commissioner Anthony. Commissioner Swindle.

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

Mr. SWINDLE. Thank you, Mr. Chairman, Senator Hollings, and members of the Committee.

The CHAIRMAN. You need the microphone.

Mr. SWINDLE. I appreciate this opportunity to be with you today and share some thoughts. I will, at the chairman's request, try to summarize my prepared statement, which we have all submitted.

I have dissented against the Commission's embarrassingly flawed privacy report and its conclusory, yet sweeping, legislative recommendation. In an unwarranted reversal of its earlier acceptance of a self-regulatory approach, a majority of the Commission has recommended that Congress require all commercial consumer-oriented Web sites that collect personally identifying information from consumers to adopt government-prescribed versions of four fair information privacy practices, known as FIPPs. You have heard: notice, choice, access, and security.

The majority has abandoned the self-regulatory approach in favor of an excessive government regulation despite continued progress in self-regulation. Why has a majority of the Commission decided to discontinue relying on self-regulation? The fundamental rationale given is that not enough Web sites are providing the type of privacy protections that the Commission has decided should be provided and this is hindering and will continue to hinder the growth of electronic commerce.

Instead of focusing on consumers' increasing ability to make choices concerning online privacy protection, the majority emphasizes that the survey, the 2000 survey, reveals that only 20 percent of all commercial Web sites and 42 percent of the most popular

Web sites meet the full FIPPs requirement. But the main reason for this relatively low percentage is that commercial Web sites have not disclosed to consumers whether they provide access and security. This failure to disclose is not surprising given the access and security implementation difficulties recently identified by the Advisory Committee on Access and Security, a copy of which I believe is included in our report.

In this regard, it is important to emphasize that the 2000 survey did not attempt to measure whether sites actually provide access and security. Rather, it gauged only whether disclosures address these issues. The 2000 survey certainly did not give any credit for no access, even though the majority indicates it might consider no access to be reasonable access in some instances.

If these access and security disclosure requirements are eliminated, the percentages of all Web sites meeting the FIPPs requirement rises significantly, to 41 percent of all commercial Web sites and 60 percent of the most popular. But even this 41 percent figure is understated because it uses a very strained definition of choice that is more accurately, in my mind, described as mandated choice.

Specifically, there is no choice recognized by the survey unless the consumer is allowed to make two choices: whether or not his information can be used internally by the Web site or the business or, and the second requirement, whether the business is allowed to use that information with third parties.

The report's recommendation that choice be legislated does not mean the kind of choice that informed consumers exercise in a marketplace once they know the terms on which they are dealing with retailers. That is real choice. The effect of mandated choice may be, as Senator Kerry pointed out, to start to eliminate or reduce choices for the consumers.

Legislation, in my mind, should be reserved for problems that the market cannot fix on its own and should not be adopted without consideration of the problems legislation may create by, for example, imposing costs or other unintended consequences that could severely stifle a thriving new economy.

The majority has recommended that Congress give rulemaking authority to an implementing agency, presumably the Commission, to define the proposed legislative requirements. In my judgment, however, the Commission owes it to the Congress and to the public to comment more specifically on what it has in mind before it recommends legislation that requires all consumer-oriented commercial Web sites to comply with breathtakingly broad laws whose details will be filled in later during the rulemaking process.

The privacy report is devoid of any consideration of cost of legislation in comparison to the asserted benefits of enhancing consumer confidence and allowing electronic commerce to reach its full potential.

For the sake of time, I will not cover my entire dissent nor the prepared statement that I have submitted today. But, I would like to make a couple of remarks in conclusion. The privacy report fails to pose and to answer basic questions that all regulators and lawmakers should consider before embarking on extensive regulation that could throttle the new economy. Shockingly, there is absolutely no consideration of the costs and benefits of regulation, nor

of regulation's predictable and unanticipated effects on competition and consumer choice, nor the experience we have to date with government regulation of privacy, nor of the constitutional issues, nor of how this vague and vast mandate will be enforced.

Industry self-regulation is working. Effective privacy protection is more than a numbers game, and the private sector is continuing to address consumer concerns about privacy because it is in industry's best interest to do so. Let us not make the search for the perfect the enemy of the good. The best way to build consumer trust and to ensure the continued growth of the Internet is through a combination of education, strong industry self-regulation, and strong FTC enforcement under existing legal authority. It is premature and counterproductive for the Commission to radically change course and call for broad legislation.

Thank you, sir. I would be happy to answer questions later.

[The prepared statement of Commissioner Swindle follows:]

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

Mr. Chairman and Members of the Committee, I am Orson Swindle, a Commissioner of the Federal Trade Commission. I appreciate the chance to testify today on the issue of online privacy.[1]

I have dissented from the Commission's embarrassingly flawed Privacy Report and its conclusory—yet sweeping—legislative recommendation. In an unwarranted reversal of its earlier acceptance of a self-regulatory approach, a majority of the Commission has recommended that Congress require **all** commercial consumer-oriented Web sites that collect personal identifying information from consumers to adopt government-prescribed versions of four fair information practice principles ("FIPPs"): Notice, Choice, Access, and Security.[2] The majority has abandoned a self-regulatory approach in favor of extensive government regulation, despite continued progress in self-regulation.

Why has the majority of the Commission decided to discontinue relying on self-regulation? The fundamental rationale given is that not enough Web sites are providing the type of privacy protections that the Commission has decided should be provided, and this is hindering and will continue to hinder the growth of e-commerce. The available data do not support this rationale. The 2000 Survey shows that 88% of all commercial Web sites (100% of the most popular sites) displayed at least one privacy disclosure to consumers, up from a mere 14% of all sites (71% of the most popular sites) in 1998. (Privacy Report ["PR"] at 10, Appendix C, Table 2a). Thus, online companies are by and large providing notice to consumers as to their privacy policies, and consumers can choose whether to deal with these companies based on their privacy policies. For those who believe that allowing consumers to make their own choices is the fundamental objective, the results of the 2000 Survey are very encouraging, although more work certainly needs to be done by industry.

Instead of focusing on consumers' increasing ability to make choices concerning online privacy protections, the majority emphasizes that the 2000 Survey reveals that only 20% of all commercial Web sites (42% of the most popular sites) meet the full FIPPS requirements. (PR Appendix C, Table 4). But the main reason for this relatively low percentage is that commercial Web sites have not disclosed to consumers whether they provide access and security. This failure to disclose is not surprising, given the access and security implementation difficulties recently identified by the Advisory Committee on Access and Security.[3]

---

[1] My oral testimony and any responses to questions you may have reflect my own views and are not necessarily the views of the Commission or any other Commissioner.

[2] While this is a reversal for the Commission, Commissioner Anthony has consistently preferred a legislative approach. *See* Statement of Commissioner Sheila F. Anthony, Concurring in Part and Dissenting in Part, *Self-Regulation and Privacy Online* (July 1999), available at <http://www.ftc.gov/os/1999/9907/index.htm#13>.

[3] In 1999, the Commission established an Advisory Committee on Online Access and Security to provide advice and recommendations to the Commission regarding implementation of reasonable access and adequate security by domestic commercial Web sites. That Committee provided

In this regard, it is important to emphasize that the 2000 Survey did not attempt to measure whether sites actually provide Access and Security; rather, it gauged only whether disclosures addressed these issues. And the 2000 Survey certainly did not give any credit for "No Access," even though the majority indicates it might consider no access to be "reasonable Access" in some instances.

If these access and security disclosure requirements are eliminated, the percentage of all Web sites meeting the FIPPS requirements rises significantly to 41% of all commercial Web sites (60% of the most popular sites). But even this 41% figure is understated because it uses a strained definition of "choice" that is more accurately described as "Mandated Choice." Specifically, the 2000 Survey gave credit for choice only when a Web site (1) gave the consumer a chance to agree to or to authorize communications back to the consumer from the Web site and (2) gave the consumer a chance to agree to or authorize disclosure of the consumer's information to third parties. The Report's recommendation that "choice" be legislated does not mean the kind of choice that informed consumers exercise in a marketplace once they know the terms on which they are dealing with retailers. That is real choice. Instead, the majority has recommended Mandated Choice that would require Web sites to continue to do business with consumers who do not agree to the uses the site tells them it will make of their personal information. For sites whose business depends on the use of information to provide consumers with discounts or to reduce the cost of services to consumers, the effect of Mandated Choice may be to mandate their exit from the marketplace or at least the reduction of the choices or products and services now available. Thus, in the name of Mandated Choice, consumers would have less choice.

Not satisfied with the self-regulation's very encouraging progress concerning privacy policy notices and its solid progress with regard to Mandated Choice, the majority recommends that the Congress impose a legislative solution. Legislation could limit consumer choices and provide a disincentive for the development of further technological solutions. Government regulation may actually give consumers fewer choices and, as technology changes, less privacy. Legislation should be reserved for problems that the market cannot fix on its own and should not be adopted without consideration of the problems legislation may create by, for example, imposing costs or other unintended consequences that could severely stifle the thriving New Economy.

The majority has recommended that Congress give rulemaking authority to an "implementing agency" (presumably the Commission) to define the proposed legislative requirements. In my judgment, however, the Commission owes it to Congress—and to the public—to comment more specifically on what it has in mind before it recommends legislation that requires all consumer-oriented commercial Web sites to comply with breathtakingly broad laws whose details will be filled in later during the rulemaking process.

The Privacy Report is devoid of any consideration of the costs of legislation in comparison to the asserted benefits of enhancing consumer confidence and allowing electronic commerce to reach its full potential. Instead, it relies on skewed descriptions of the results of the Commission's 2000 Survey and studies showing consumer concern about privacy as the basis for a remarkably broad legislative recommendation. It does not consider whether legislation will address consumer confidence problems and why legislation is preferable to alternative approaches that rely on market forces, industry efforts, and enforcement of existing laws.

For the sake of time, I will not cover my entire dissent, but I would like to draw your attention to additional points that it makes:

- the Report does not adequately credit self-regulatory efforts and ignores developments in technology;
- the 2000 Survey provides a unique baseline for measuring the quality of privacy disclosures;
- individual FIPPS are widespread;
- measuring success on the basis of full FIPPs is irrational;
- equating self-regulatory enforcement with the prevalence of seal programs is misleading;
- the Report confirms the exponential growth in online commerce but misuses consumer confidence surveys and lost sales projections;

---

the final version of its report to the Commission on May 15, 2000, describing options for implementing reasonable access to, and adequate security for, personal information collected online and the costs and benefits of each option.

- the meaning of surveys showing consumer unease is unclear; and
- the Report ignores or glosses over Constitutional issues, enforcement difficulties, and questions relating to the protection of offline privacy.

In conclusion, the Privacy Report fails to pose and to answer basic questions that all regulators and lawmakers should consider before embarking on extensive regulation that could throttle the New Economy. Shockingly, there is absolutely no consideration of the costs and benefits of regulation; nor of regulation's predictable and unanticipated effects on competition and consumer choice;[4] nor of the experience to date with government regulation of privacy; nor of Constitutional issues; nor of how this vague and vast mandate will be enforced.

Industry self-regulation is working. Effective privacy protection is more than a numbers game, and the private sector is continuing to address consumer concerns about privacy because it is in industry's interest to do so. Let us not make the search for the perfect the enemy of the good. The best way to build consumer trust and to ensure the continued growth of the Internet is through a combination of education, strong industry self-regulation, and strong FTC enforcement under existing legal authority. It is premature and counterproductive for the Commission to radically change course and call for broad legislation.

The CHAIRMAN. Thank you.

Commissioner Thompson.

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

Mr. THOMPSON. Thank you, Mr. Chairman. Good morning to you and members of the Committee. I wanted to thank you for inviting me to appear before you again with my fellow Commissioners to address our most recent report on online privacy.

In 1997 when we began to look at the issue of privacy on the Internet, consumer-based electronic commerce was largely viewed as a place for the most adventurous and technologically savvy. But at the same time, people with vision viewed the Internet as a place that could potentially transform the American consumer marketplace by empowering consumers with access to vast quantities of information and new goods and services.

Since then we have witnessed great progress in achieving that transformation. Yet we still have a long way to go until Americans fully embrace the Internet and accept its technology as integral parts of their daily lives. Today industry, government, and consumers alike share a common goal of making the Internet as meaningful and productive for those at the center of the market bell curve, namely the family in the suburbs of Canton, Ohio, as it is for the technologist in Silicon Valley.

To achieve this goal, we must be led by the voice of users and allow the Internet to become consumer-driven. From the beginning of the Commission's work, consumers have expressed a great con-

---

[4] I note that the regulations promulgated to implement the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501 *et seq.,* require detailed Notice; Access, including the ability to review, correct, and delete information maintained by the site; and a form of opt-in mandated Choice (verifiable parental consent). 16 C.F.R. §§ 312.4, 312.6(a)(1), 312.6(a)(2), 312.5(a), 312.5(b). The regulations went into effect on April 21, 2000, and already press reports state that some small online companies have stopped providing services to children because implementation of COPPA's requirements is too costly. *See, e.g.,* "New Children's Privacy Rules Pose Obstacles for Some Sites," *The Wall Street Journal* at B–8 (April 24, 2000) (reporting one attorney's estimate that it will cost her clients between $60,000 and $100,000 annually to meet COPPA standards); "New privacy act spurs Web sites to oust children," William Glanz, *The Washington Times* (April 20, 2000), available at <http://www.washtimes.com/business/default-2000420233432.htm>. See also "COPPA Lets Steam out of Thomas," Declan McCullagh, *Wired News* (May 16, 2000), available at <wysiwyg://1/http://www.wired.com/news/politics/0,1283,36325,00.html>.

cern about privacy of their personal information on the Internet, and industry has focused its attention on attracting the core of American consumers. The concern that the public has about privacy has only grown louder, so today the issue of data privacy has become a litmus for consumer confidence in the online marketplace.

Back in December 1998, I told industry that we were at a critical juncture, one where industry is asked to self-regulate at the behest of government and public trust. This choice, while daunting, provides an exciting and unprecedented opportunity for industry to take the lead in shaping public policy for this important new medium. Consumers are expecting that industry and government will work together to find new and better ways to make the Internet safe, inspire consumer confidence, and preserve the innovative spirit of e-commerce. But the failure of industry to meet this challenge will not only have a negative effect on the future of e-commerce, but also on the public's confidence in industry's ability to take the lead in solving important public policy problems.

To its credit, the most responsible segments of the online economy recognized the importance of data privacy, both from the public policy standpoint and as a test of their own accountability.

The CHAIRMAN. Commissioner Thompson, could you summarize.

Commissioner THOMPSON. OK.

I think that we are at a critical juncture here. I think that what we are trying to do is propose a model that is not heavy-handed legislation, but provides a means for what some people term as co-regulation. That puts industry in the forefront.

But the problem of Internet privacy may indeed be larger than what we originally envisioned. Industry has a very important role as the lead, but there are holes in the Swiss cheese. A legislative backdrop allows us to get at those holes. You see them in our report when we talk about the quality of what is being provided, and still parts of the Internet industry that are not doing anything at all. Those need attention, and we think it is a critical issue for consumer confidence.

Thank you.

[The prepared statement of Commissioner Thompson follows:]

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

In 1997 when the FTC began looking at the issue of privacy on the Internet, consumer-based electronic commerce was largely viewed as a place only for the adventurous and technologically savvy. At the same time, however, many also viewed the Internet as a place that could potentially transform the American consumer marketplace by empowering consumers with access to vast quantities of information, as well as goods and services. Since then, we have indeed witnessed great progress in achieving that transformation; yet, we still have a long way to go until Americans fully embrace the Internet and accept its technology as integral parts of their daily lives. Today, industry, government and consumers alike share the common goal of making the Internet as meaningful and productive for those Americans at the center of the market bell curve—the family in the suburb of Canton, Ohio—as it is for the technologist in Silicon Valley. To achieve this goal, we must be led by the voice of users and allow the Internet to become "consumer driven."

From the beginning of the Commission's Internet work, consumers have expressed strong concern about the privacy of their personal information on the Internet. And as industry has focused its attention on attracting the core of American consumers, public concern about privacy has only grown louder so that today, the issue of data privacy has become a litmus for consumer confidence in the online marketplace.

In December 1998, I stated:

> [W]e are all at a critical juncture, a point where industry is asked to self-regulate at the behest of government and public trust. This choice, while daunting, presents an exciting and unprecedented opportunity for industry to take the lead in shaping public policy for this important new medium. Consumers are expecting that industry and government will work together to find new and better ways to make the Internet safe, inspire consumer confidence, and preserve the innovative spirit of e-commerce. But, the failure of industry to meet this challenge will not only have a negative effect on the future of e-commerce, but also on the public's confidence in industry's ability to take the lead in solving important public policy problems.[1]

To its credit, the most responsible segment of the online economy recognized the importance of the data privacy issue—both from a public policy standpoint as a test of the technology industry's accountability, as well as from a consumer confidence perspective as a test of industry responsiveness to consumer demand. As a result, the industry leaders have worked with the Commission and consumer groups to provide the market with seal programs, privacy policies and consumer and business education initiatives designed to address the public policy and business challenge posed by the issue of Internet privacy. Furthermore, to date, government has appropriately put industry self-regulatory efforts at the forefront of America's response to the privacy challenge. We recognize the important role that industry plays, and will continue to play, in defining good business practices in electronic commerce. After three years of Internet surveys, public workshops, hearings and reports, however, it has become evident that the public policy challenge posed by the issue of Internet privacy may indeed be larger than any one segment—industry, government or consumers—can address alone.

People in the Internet community are fond of stating that one Internet year is equivalent to three calendar years. The Commission has carefully and cautiously waited over three Internet years before recommending legislative action. During that time, government, industry and consumers have all learned much more about the substantial challenge involved with providing online privacy. In recognition of this complexity and the importance of Internet privacy as a threshold issue for the future growth of electronic commerce, I believe that now is the appropriate time for well-crafted legislation.

In July 1999, I testified before the Senate Commerce Committee where I cautioned that industry faced a formidable challenge in achieving effective self-regulation of Internet privacy. I stated that:

> During the past year, industry leaders have expended substantial effort to build self-regulatory programs. However, I believe that we will not progress further unless industry acts on the specific shortcomings that our report documents. Congress and the Administration should not foreclose the possibility of legislative and regulatory action if we cannot make swift and significant additional progress.[2]

Based upon what I perceived as real progress by industry in having a greater number of Web sites bearing a privacy disclosure, I was willing to withhold calling for legislative action to give industry further opportunities to: (1) maximize privacy coverage by reaching out to spur non-participating companies to adopt and implement effective privacy policies; and, (2) to significantly improve the quality of privacy protections by encouraging participating companies to embrace and implement what the Commission, the Organization for Economic Cooperation and Development and industry groups themselves (See e.g. Privacy Principles of the Online Privacy Alliance) have long recognized as the fair information principles of notice, choice, access, security and enforcement.

Now, three years after the Commission submitted its initial report to Congress and a year-and-a-half after I posed a direct policy challenge to industry, our most recent survey shows that the quality of privacy protections that even the most responsible sites provide, is far from adequate. In fact, our survey shows that forty percent of the most popular (and presumably most sophisticated and responsible) Web sites still do not provide consumers with adequate notice and choice—the most fundamental elements for any privacy policy. I believe these results are especially disappointing because they demonstrate substantial deficiencies in providing what

---

[1] *December 1, 1998, "Managing the Privacy Revolution '98," Remarks Before the 4th Annual National Conference on Privacy & American Business.*

[2] *July 13, 1999, Statement of Commissioner Mozelle W. Thompson in support of "Self-Regulation and Privacy Online," FTC Report to Congress.*

most industry leaders agree should serve as the bedrock of privacy self-regulatory efforts.

So where does that leave us? Based not only on our 2000 Survey results but also our three years of working interactively with everyone interested in the online privacy issue, a majority of the Commission has concluded that Federal legislation is now appropriate because:

> [S]elf-regulatory initiatives to date fall short of broad-based implementation of effective self-regulatory programs, . . . [and] that such efforts alone cannot ensure that the online marketplace as a whole will emulate the standards adopted by industry leaders.[3]

In making my recommendation, I believe that appropriate legislation should not be viewed as a *substitute* for well-crafted industry self-regulatory programs. This point is particularly important because industry self-policing could ultimately provide the public with consumer-driven privacy responses. Instead, legislation incorporating directed rule-making and safe-harbors should provide a principled *backstop* for effective industry efforts. Thus, if basic privacy principles and industry self-regulation define the "Swiss cheese" of online privacy, the Children's Online Privacy Protection Act and our legislative recommendation should be viewed as a means of addressing the holes in the cheese.

I believe the Commission's recommendation is also consistent with my view of the cautious, balanced and responsible approach government should take in the fast-moving Internet environment. Our recommendation incorporates the principles of interactivity, flexibility and innovation. Through safe-harbors and a rulemaking process, government will interact with consumers and industry to implement appropriate solutions to this important public policy problem. Moreover, by recommending legislation that "would set forth a basic level of privacy protection for consumer-oriented Web sites [and providing] an implementing agency with the authority to promulgate more detailed standards,"[4] government would avoid an inflexible "one size fits all" approach that would preclude recognition that consumers vary their view of privacy obligations depending on how they believe their personal information is being used. Finally, by recommending a rulemaking process, it is possible to encourage, and over time incorporate, technological innovation that can provide consumers with better tools to protect their own privacy.

Accordingly, I strongly support the recommendations contained in the Commission's May 2000 Report, *Privacy Online: Fair Information Practices in the Electronic Marketplace.*

The CHAIRMAN. Thank you very much, Commissioner Thompson. As I mentioned, your complete statement will be made part of the record, which I read and I appreciate.

Commissioner Leary.

STATEMENT OF HON. THOMAS B. LEARY, COMMISSIONER, FEDERAL TRADE COMMISSION

Mr. LEARY. Mr. Chairman, members of the Committee: You have my concurring and dissenting statement and, in the interest of time, I would just like to summarize and start with the areas where I think we have broad agreement.

There is a dramatic increase in the number of companies that publicly address privacy one way or the other, but the quality of disclosures varies widely. Too many are confusing, if not misleading, and I think that the examples that Commissioner Anthony has cited for you speak for themselves. More widespread disclosures of this kind could actually do more harm than good. Therefore, I agree with some members of this Committee and with the Commission majority that both business and consumers would benefit from better disclosures.

---

[3] *May 2000, Privacy Online: Fair Information Practices in the Electronic Marketplace,* at 35.

[4] *May 2000, Privacy Online: Fair Information Practices in the Electronic Marketplace,* at iii–iv.

There also seems to be broad agreement that any legislation to address privacy concerns should ultimately apply in the same way to both the online and the offline worlds to the extent the information is the same. There are special capabilities in the online world, which may require special attention, but there is no reasonable basis for treating information that is collected about my purchases on Amazon.com any differently from my purchases at Borders. I think that we have a consensus on that.

There seems to be some difference on the issue of timing and some question as to whether the Commission has enough expertise to recommend broad-based legislation to you because we have studied the Internet only. We have had a lot of experience in privacy issues in the offline world as well, Senators, and if there are any doubts about the issue you have the capability yourselves to investigate and satisfy yourselves that when the information is the same there should be an equal playing field between the online and the offline worlds.

Finally, I would say that I think we all generally recognize that once you get past the issue of notice and disclosure the further elements of the so-called fair information practices become progressively more complicated. There is an even more compelling reason for treating them differently than notice or disclosure. I agree with those members of this Committee who state that ultimately adequately informed consumers should be able to select for themselves the level of privacy protection they want and may be willing to pay for either directly or by foregoing some benefit.

It is not fair to allow consumers who are particularly solicitous about particular elements of privacy and want broad access and broad ability to correct, and so on, to impose costs on those consumers who do not care. So I urge you to consider whether or not the market, as it does in so many other areas of our life, will not work better ultimately than government regulation.

There may be certain special categories of information or special uses, like health information or financial information, that require special treatment in both the online and the offline worlds. But they should not be part of a broad privacy policy imposed on the Internet alone.

Finally, I would just like to say that I think it is in all of our interest to continue to encourage the self-regulatory schemes which are under way and which I believe ultimately hold tremendous promise for improving performance in this industry in a market-based fashion.

Thank you.

[The prepared statement of Commissioner Leary follows:]

PREPARED STATEMENT OF HON. THOMAS B. LEARY, COMMISSIONER, FEDERAL TRADE COMMISSION

Today the Federal Trade Commission recommends that Congress enact legislation to help consumers protect their privacy when transacting business on the Internet. I agree that some legislation is appropriate, but believe that the recommendation in the Report endorsed by a majority is too broad in one respect and too narrow in another. The recommendation is too broad because it suggests the need for across-the-board substantive standards when, in most cases, clear and conspicuous notice alone should be sufficient. The recommendation is too narrow because any legislation should apply to offline commerce as well.

The Report's recommendation is based, in part, on our common belief that the Internet has enormous potential to grow our economy; that this potential is inhibited to some degree by consumers' concerns about their privacy; and that it is an appropriate policy objective to address these concerns and encourage growth. So far, so good. The issue, then, is how best to address these privacy concerns in an even-handed way. If the Internet is subjected to requirements that do not apply *pro tanto* to offline commerce, the regulatory imbalance could itself inhibit the growth of the Internet and undercut our common objective.

We also agree unanimously that, whatever government does or does not do, the private sector will have an important role to play. The majority looks at the 2000 Web Survey data and concludes that the private sector has failed to address privacy concerns rapidly enough. I am not convinced that the Survey supports this conclusion, but agree, for other reasons, that some legally mandated privacy protections would be appropriate.

The Survey does not necessarily demonstrate that the market has failed to respond to consumer demand. It only measures "inputs," the prevalence of privacy policies of various kinds; it does not measure "outputs," the impact that these policies have on consumer confidence and consumer behavior. The Survey numbers could be read to support alternative scenarios. For example, the most popular sites generally have more comprehensive disclosures, and this could mean that some consumers favor them because of the disclosures. The fact that gains are modest overall, however, may also indicate that consumers are not quite as fixated on privacy issues as might appear from the public opinion polls cited in the Report. Marketers generally know more about consumer demand than regulators do.

Marketers know, for example, that consumers' actual buying habits are not necessarily consistent with their expressed preferences. Their stated interest in various ancillary protections like privacy may fade or become more nuanced, once they learn more about them and realize that there are costs attached. Consumer opinion on privacy issues appears to be a complex subject,[1] and public opinion polls simply do not provide an adequate predicate for a legislative recommendation of the scope contained in the Report.

There Is a Need for Better Disclosures

There is one aspect of the 2000 Web Survey, however, that I find particularly disturbing. The Survey results do show a steadily rising trend in the number of companies that address privacy, one way or another, but we cannot therefore conclude that consumers are better informed today or would be even better informed if the numbers rose even further. In fact, a site's mere mention of privacy may lead to a misperception that the consumer's privacy is well-protected, and a plethora of varying and inconsistent privacy claims could add to consumer confusion. The Survey tells us that the scope of the disclosures varies widely (see Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress ("Report") at 38–44) and, in my view, vendors and their customers would both benefit from a legislative initiative to require disclosures of greater clarity and comparability.

Market processes, supplemented by traditional remedies against consumer deception, should ultimately provide the most appropriate mix of disclosures and substantive protections, but these forces sometimes work slowly and I am convinced that privacy concerns have some special characteristics that make it prudent to prompt the market to work more rapidly. Some standardization of the disclosures would allow consumers to compare more easily the privacy practices of different vendors. As we learned when considering environmental marketing claims, for example,[2] varied and inconsistent claims lead to consumer confusion. Consumers may not be able to recognize valid and invalid comparisons when they are dealing with unfamiliar concepts. When terms have uniform meaning and basic equivalent information is disclosed for each site, the marketplace should work more efficiently.

Although consumers' knowledge and understanding of these issues is steadily increasing, it still has a long way to go. Not only is the Internet a recent invention, consumers are just beginning to become aware of the potential for data collection both online and offline. Consumers still do not know much about the possible uses

---

[1] Jupiter Communications, *Proactive Online Privacy: Scripting An Informed Dialogue to Allay Consumers' Fears,* at 3–7 (June 1999).

[2] *See* Guides for the Use of Environmental Marketing Claims (the "Green Guides"), 16 C.F.R. pt. 260 (1999). When the Commission requested public comment on these Guides three years later, commentators generally agreed that they benefit both consumers and industry, *inter alia,* by promoting consistency and accuracy in claims, helping consumers to make accurate decisions, and thereby bolstering consumer confidence. *See* Guides for the Use of Environmental Marketing Claims, Final Rule, 61 Fed. Reg. 53,311 (1996).

of their personal information (and new ones are invented every day), the ramifications of permitting its use, and the costs associated with limiting its dissemination. Because an efficient market presupposes full and accurate information, it is appropriate to mandate more extensive privacy disclosures.

Privacy concerns also differ from concerns about product attributes that consumers may value. An uninformed decision to deal with a vendor that disseminates personal information could have ramifications for years to come, and that decision cannot be retracted. The marketplace may ultimately discipline the less-than-candid vendor, but the potential consumer harm will continue because the personal information may have spread and cannot be retrieved. The privacy loss and consequent harm results from mere participation in the market, with insufficient notice, not from a bad purchase decision. By contrast, if consumers are uninformed about particular product attributes, and regret the purchase, the damage may at most be limited to the value of the purchase.[3]

I therefore agree with the Report insofar as it recommends a legislative prod to ensure better disclosures. Thereafter, I part company.

The Report's Proposal Is Too Broad

The Report's recommendation is framed around the so-called "fair information practices" of notice, choice, access, and security. Notwithstanding references to the need for flexibility (*see, e.g.,* Report at 60–61), the overall thrust of the Report is that any privacy policy should, at a minimum, recognize substantive consumer rights in each of these areas. What the Report does not do is adequately explain why.

In addition to its expertise on consumer disclosures, the Commission is supposed to have some expertise in the operation of competitive markets—when they are likely to succeed and when they are likely to fail. The Report does not explain why an adequately informed body of consumers cannot discipline the marketplace to provide an appropriate mix of substantive privacy provisions. These are matters that Congress can and should investigate on its own, but our Report does not provide any help. It is one thing to recognize that the fair information practices (beyond adequate notice) are laudable goals and to encourage their adoption by various self-certifying industry groups. These certifying programs can make a valuable contribution by reinforcing consumers' confidence and reducing consumer costs of obtaining information. It is quite another thing to urge that the practices, in one form or another, be mandated by legislation and by rules.[4]

When the Commission issued the Green Guides, it expressly disclaimed any authority or intention to achieve a substantive result:

> The Commission does not have a statutory mandate to set environmental policy. It is not the Commission's goal, for example, to require that product [sic] be "recyclable." Rather, any Commission cases, rules, or guides would be designed to address how such terms may be used in a non-deceptive fashion in light of consumer understanding of the terms.[5]

These disclosure-oriented guides did have a substantive effect; later public comments indicated that they did "encourage manufacturers to improve the environmental characteristics of their products and packaging," while "allowing flexibility for manufacturers to improve the environmental attributes of their products and to communicate these improvements to consumers."[6] Better information did lead to a better market outcome. In my view, we should follow the precedent of the Green Guides, and not request the authority to issue substantive standards.

The fact that the fair information practices have been favorably regarded in the regulatory community for almost thirty years (Report at 8–9), does not justify mandatory legislation. A provenance from the 1970s is scant cause for comfort, because government regulators, here and throughout the world, had much less faith in free market institutions then than they have today.[7] Moreover, it cannot be claimed that

---

[3] This limitation may not apply to products that are hazardous to health and safety, and this is one reason why there are also affirmative disclosure requirements to deal with these risks.

[4] I acknowledge that previous Commission reports to Congress, which advocated a "wait and see" policy, have suggested that legislation could be appropriate if the fair information practices were not more broadly adopted. I would not have endorsed that aspect of the previous reports either, had I been here.

[5] Request for Public Comments on Issues Concerning Environmental Marketing and Advertising Claims and Pending Petitions, 56 Fed. Reg. 24,968 (1991).

[6] Guides for the Use of Environmental Marketing Claims, Final Rule, 61 Fed. Reg. 53,311, 53,313 (1996).

[7] *See, e.g.,* Daniel Yergin and Joseph Stanislaw, *The Commanding Heights: The Battle Between Government and the Marketplace that is Remaking the Modern World* (1998).

the fair information practices are "widely-accepted" in the business community (Report at 8). Our own Survey of the Internet world demonstrates the contrary, and there is no indication that the principles are widely accepted in the offline world either. I would not be so quick to conclude that we are right and so many others are wrong.[8]

The Report not only fails to explain why adequate disclosures are insufficient, it passes too lightly over issues of complexity. Granted, these are issues more appropriately addressed in a rule-making proceeding, but Congress needs to have a better understanding of what we mean when we ask for authority to set "reasonable" standards. For example, the Report recognizes that "access" is a complicated matter and indicates that any determination of what is "reasonable" should be informed by the discussion of the Advisory Committee on Access and Security (Report at 30–31, 61). At the same time, however, the Report endorsed by the majority states flatly that "the Commission believes that fair information practices require that consumers be afforded *both* an opportunity to review information *and* an opportunity to contest the data's accuracy or completeness—*i.e.,* to correct or delete the data." (Report at 32). This is an extraordinarily broad claim, which could in many cases lead to vast expense for trivial benefit and which provides an ominous portent for the content of any substantive rules.

Even "choice," which at first glance seems only a natural corollary of "notice" is a complicated subject. The Report recognizes, for example, that it may be appropriate to provide affirmative benefits if a consumer agrees to certain personal disclosures (Report at 61). If the collection of data is one thing that makes it possible for a vendor to offer lower prices, consumers who are particularly tender of privacy would otherwise be able to free ride on the value created by those who are not. (If a supermarket issues a card that offers discounts to people who use it, in exchange for compilation of useful data, consumer "choice" surely does not involve the right to get the discount without supplying the data.[9])

On the other hand, if the premium for permission to use information is too generous, or the penalty for refusal too severe, consumer "choice" really involves nothing more than the "choice" to refuse dealings with the vendor. The issue of what is or is not a reasonable price differential is complicated, but may be too difficult to bother with in a situation where a particular vendor competes with a number of others that have their own policies. Does this mean that reasonableness should depend on the market power of the vendor?

Other examples could be cited to illustrate the difficulties involved in fashioning substantive rules about choice, access and security, but there is no need to burden this statement further. Congress can, and should, explore these issues in detail if it takes up this aspect of the Report's legislative recommendation.

I therefore believe that any across-the-board legislative mandate should be confined to notice alone, although disclosure rules might appropriately provide that notice include information about the other categories. In some cases, involving particular kinds of information or particular uses, the risk of harm may be so great that specific substantive standards are required. This is a legislative judgment. Congress can, and already does pass industry-specific legislation to deal with these situations.[10] In addition, I believe it is entirely appropriate for the Commission to impose more specific restrictions as "fencing-in" relief in a consent settlement, in order to discipline the future behavior of business entities that have misused consumer information in the past.

The Report does recognize (Report at 25) that notice is "the most fundamental of the fair information practice principles," but it recognizes it for the wrong reason. Notice is not fundamental "because it is a prerequisite to implementing other fair information practice principles, such as Choice or Access" (*Id.*); it is fundamental because it helps the marketplace accurately to reflect consumer preferences with respect to the other principles. Consumers, so long as they are informed by clear and

---

[8] The Commission's own Internet privacy policy, which can be readily accessed by a click on the Commission's home page, provides notice only. The Commission does protect consumer privacy. It complies with the Privacy Act of 1974, a statute that applies fair information practice principles to the federal government's collection and use of information. 5 U.S.C. §§ 552a *et seq.* However, the Commission's privacy policy does not provide information about choice, access or security measures.

[9] This use of an offline example is deliberate because the logic is not dependent on the mode of collection. *See* discussion, *infra* pp. 10–12.

[10] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 *et seq.;* Telecommunications Act of 1996, 47 U.S.C. §§ 222 *et seq.;* Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710 *et seq.;* Cable Communications Policy Act of 1984, 47 U.S.C. §§ 551 *et seq.;* Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq.*

conspicuous disclosures, will be able to select the vendors that give them the privacy protections they want and are willing to pay for.

The Report's Proposal Is Too Narrow

I also disagree with the Report's legislative recommendation to the extent that it treats issues of online privacy as wholly different from offline privacy. At times the Report acknowledges the existence of offline privacy concerns and the erosion of the distinction between online and offline commerce (Report at 8 n.26, 55 n.196), but it justifies special treatment of Internet privacy on the ground that the technology of the Internet has "enhanced the ability of companies to collect, store, transfer and analyze vast amounts of data[.]" (Report at 1).

Of course, some privacy issues are particular to the Internet. This new technology has permitted uniquely invasive tracking of consumer preferences by recording not just purchases, but consumers' movements on the Internet as well. This practice of tracking, including third-party profiling, may be particularly threatening and distasteful to many. (*See* Report at 37–38, discussing so-called "cookies"). Any legislative or regulatory scheme can and should ensure that consumers are adequately informed about these Internet capabilities.

However, the majority's recommendation is not focused on the special characteristics of e-commerce or on particular categories of sensitive information collected online. Instead, the majority would apply the fair information practice principles to any personal information collected by any commercial Web site, even though the identical information can be collected offline. The distinction between online and offline privacy is illogical, impractical and potentially harmful.[11] Let me examine each of these points in turn.

Recognition of the privacy concerns specific to e-commerce should not obscure the fact that in significant respects online privacy concerns are identical to those raised by offline commerce. The same technology that facilitates the efficient compilation and dissemination of personal information by online companies also allows offline companies to amass, analyze and transfer vast amounts of consumers' personal information.[12] Offline companies collect and compile information about consumers' purchases from grocery stores, pharmacies, retailers, and mail order companies, in particular.

It is also not possible to distinguish offline and online privacy concerns on the basis of the nature of the information collected. With the exception of online profiling, it is the same information. The Report's recommendation would require Amazon.com to comply with the fair information practice principles but not the local bookstore which can compile and disseminate the same information about the reading habits of its customers. The consumer polls, upon which the Report places such significant reliance, demonstrate that consumer concerns about the disclosure of personal information are not dependent on how the data has been collected.[13]

Moreover, it is impractical to maintain such a distinction. Businesses are likely to have a strong incentive to consolidate personal information collected, regardless of the mode of collection, in order to provide potential customers with the most personalized message possible. Already, companies are seeking to merge data collected offline with data collected online.[14] In light of this reality, the majority's recommendation would result in perverse and arbitrary enforcement. Enforcement actions would depend on the source of and method used to collect a particular piece of consumer data rather than on whether there was a clear-cut violation of a company's announced privacy policy or mandated standards.

Finally, the Report's focus only on online privacy issues could ultimately have a detrimental impact on the growth of online commerce, directly contrary to the Report's objectives. It is clear from the Advisory Committee's Report on Access and Security and from limited portions of the Commission's own Report that implementation of the fair information practices will be complex and may create significant compliance costs. Online companies will be placed at a competitive disadvantage rel-

---

[11] Chairman Pitofsky has expressed some of these views in one of his own speeches. *See* Robert Pitofsky, *Electronic Commerce and Beyond: Challenges of the New Digital Age,* Speech before the Woodrow Wilson Center, Sovereignty in the Digital Age Series, Washington, D.C. (Feb. 10, 2000).

[12] Abacus, a consortium of mail order companies, is a good example of the ability of merchants to compile and share detailed data about consumers' purchasing habits. *See In re Trans Union,* Docket No. 9255 (Feb. 10, 2000), *appeal docketed,* No. 00–1141 (D.C. Cir. Apr. 4, 2000).

[13] *See IBM Multi-National Consumer Survey, prepared by Louis Harris Associates Inc.,* at 22–24 (October 1999).

[14] Dana James, *Synchronizing the Elements; Traditional Companies, Yearning to Catch Up on the Basics, Find Value in Merging Online, Offline Databases,* Marketing News, Feb. 14, 2000, at 15.

ative to their offline counterparts that are not forced to provide consumers with the substantive rights of notice, choice, access and security. Traditional brick and mortar companies that have an online presence or are considering entry into the electronic marketplace will be forced to assess how the cost of regulation will affect their participation in that sector.

A better approach would be to establish a level playing field for online and offline competitors and to address consumers' privacy concerns through clear and conspicuous privacy disclosures. Any privacy concerns that are unique to a particular medium or that involve particular categories of information (however collected) can continue to be addressed through separate legislation.[15]

The Report's recommendation limits itself to online privacy for reasons that seem primarily historical. The Commission first looked at the online world at a public workshop in 1995, followed by subsequent workshops in 1996 and 1997. Then, starting in 1998, Commission staff conducted annual surveys of Internet sites and their privacy policies to measure in a rough way the state of industry self-regulation. Each survey has been reported to Congress. The Report's legislative recommendation flows from that series of surveys. The surveys have provided a lot of useful information, and undoubtedly spurred industry attention to online privacy issues, but the scope of these particular surveys should not dictate the parameters of a legislative proposal.

The Commission has ample information available to support a broader recommendation, and Congress will have ample opportunity to develop its own legislative record. The fair information practices so frequently referenced in the Report were, after all, originally developed to address concerns regarding the collection of information *offline.* And the Commission itself has had significant exposure to offline privacy issues. For example, the Commission has enforced the Fair Credit Reporting Act since its enactment in 1970.[16] This statute addresses consumer concerns about the collection and dissemination of sensitive data by credit bureaus. Although the Act predates the advent of the fair information practices, its provisions mandate some of these same requirements.[17]

The Commission also undertook in 1997 a study of the "look-up" service industry, computerized database services that collect and sell consumers' identifying information. The workshop and subsequent report to Congress focused on the benefits of these services as well as the risks, including consumers' privacy concerns.[18] Although the Internet increased access to these informational products, the information at issue was primarily collected offline. Finally, just last week, the Commission issued its final rule implementing the privacy provisions of the Gramm-Leach-Bliley Act, a rule that focuses on the treatment of consumer information by financial institutions—again without regard to how the information was collected.[19]

Even if the Commission majority, who endorse the Report, determined that our experience was insufficient to assess offline privacy concerns, a better course would have been to invite further Congressional inquiry. As it is, the Report's advocacy of legislation limited to the online world suggests that public remedies should be bounded by the scope of the studies we have chosen to conduct. This is thinking upside down.

Existing Remedies Should Be Actively Pursued

Legislation to mandate more comprehensive and clear privacy disclosures should ensure in the long run that the marketplace provides consumers with their desired level of privacy protection. Legislation and rule-making may take considerable time, however, and in the interim some consumers may suffer long-lasting harm because they have not been adequately informed about privacy issues. In order to reduce these potential harms, I would recommend that the Commission take some immediate steps.

First, the Commission should more actively employ its existing authority under Section 5 to prohibit unfair or deceptive practices. We can not only challenge out-

---

[15] *See supra* note 10.

[16] 15 U.S.C. §§ 681 *et seq.*

[17] The Commission recently issued its decision in *In re Trans Union,* Docket No. 9255 (Feb. 10, 2000), *appeal docketed,* No. 00–1141 (D.C. Cir. Apr. 4, 2000), an enforcement action concerning the dissemination by a credit bureau of certain information to target marketers. The decision considered not only the privacy implications of this practice but also the availability of other information collected offline.

[18] *See Individual Reference Services: A Federal Trade Commission Report to Congress* (Dec. 1997).

[19] *See* Privacy of Consumer Financial Information, __ Fed. Reg.__ (2000) (to be codified at 16 C.F.R. pt. 313).

right violations of express privacy policies,[20] but also challenge policies that deceive because they impliedly offer more protection than they deliver. As noted earlier, although the Survey results demonstrate an increase in the number of privacy disclosures, they also indicate that these disclosures often involve inconsistent or confusing claims. (Of course, enforcement actions should only be brought in cases of clear-cut deception, so that companies which attempt in good faith to provide information, up to now on a voluntary basis, would not be chilled from doing so.) Stepped-up enforcement in this area, as elsewhere, serves a double purpose: it addresses specific situations and sends a message both to consumers and businesses.

Beyond this, the Commission should redouble its efforts to educate consumers directly about the benefits and potential risks associated with the collection and dissemination of their personal information. Without additional authorization, we can help consumers to better understand the meaning of various privacy disclosures. Informed consumers will ultimately be the most effective agents for protection of privacy, online and offline, by rewarding companies that offer the preferred levels of protection.

The CHAIRMAN. Thank you very much, Commissioner.

We have another panel and I know all of our members have questions, so I will just ask one. As has been pointed out, at least statistically it is fairly impressive the number of Web sites that offer privacy policies. But once you get into some of these so-called policies it gets somewhat interesting.

In May, *USA Today* reviewed 10 major Web sites and found their policies to be a confusing jumble of incomprehensible language riddled with loopholes. Yahoo's policy, for instance, is eight pages long, and your survey finds that fewer than half of the sites had clearly worded procedures.

One of the more controversial Web sites, Doubleclick, says that it would use personal information only with your "permission." It does not tell you that it assumes it has permission unless you explicitly opt out. And here is what you have to do: Read the first 1,468 words, click on a link to another page, read 650 more words that tell you why you should not opt out, read 200 more words urging you once again not to opt out, and click onto a final link to opt out of the program.

That is not exactly privacy as some of us understand it. Now, I think this is a matter of real concern, particularly when we look at what Doubleclick was set up for. I wonder if, according to your report, as the numbers of Web sites that provide "privacy protection" are more like Doubleclick's than the kind of thing we assume that would allow us to ensure privacy.

So I guess I would begin with Chairman Pitofsky and go through the witnesses, because I think this is a serious problem, for a Web site to advertise that it will protect your privacy and then have this kind of mumbo-jumbo. When Yahoo, which is one of the most respected and I believe the most used Web site, takes eight pages and 3,405 words and 167 sentences, that is not what we had in mind and I hope it is not your definition of a Web site that allows people to have their privacy ensured.

We will begin with you, Commissioner Pitofsky, and we will go through in order of how the Commissioners spoke.

Mr. PITOFSKY. Mr. Chairman, I went through the same process with Doubleclick that you followed and I have to tell you, if I did

[20] *See FTC v. ReverseAuction.com, Inc.,* No. 00–0032 (D.D.C. Jan. 6, 2000); *GeoCities,* FTC Dkt. No. C–3849 (Feb. 12, 1999).

not have somebody helping me I would never have found out how to get to the third and fourth screen in order to opt out.

The CHAIRMAN. And you are a former university professor.

Mr. PITOFSKY. And I have been doing this consumer protection work for 30 years.

I would have been lost somewhere between the third and the fourth screen. This example is extreme, but I tell you, it is not the only one. I saw one yesterday that was brought to my attention, the headline is: "We protect your privacy. Read on and find out the terms." There are then ten single-spaced pages. Lawyers would have trouble reading it. When you get to the ninth page, you find out you have no rights at all. It is notice, I suppose, but it is a kind of notice that does not do consumers much good.

But on the other hand, 60 percent of the Web sites have notice that we found was quite fair. The question is how you get from that 60 percent all the way to the end. Let me just repeat what I said: I am all for self-regulation, but if the self-regulators cannot say: if you fail to give better notice than that you violate our standards and we will refer you to some law enforcement agency, then I am afraid many of these Web sites who are fairly irresponsible are going to say: Well, why do I not keep making the money selling private identifiable information; so take my seal away from me; I will have to get along without it.

I think there has to be a backup. Effective self-regulation in my experience almost always has that kind of backup of law.

The CHAIRMAN. Did you see the Yahoo Web site?

Mr. PITOFSKY. I did not see that one.

The CHAIRMAN. I am curious whether that would warrant a seal of approval. And I say that not in any bias for or against Yahoo, but the fact is it is the most popular Web site there is.

Mr. PITOFSKY. Let me check it out and I will get an answer for you.

The CHAIRMAN. Thank you.

Commissioner Swindle.

Mr. SWINDLE. I will defer to Commissioner Anthony since she was second—OK, or I will continue.

The CHAIRMAN. I am sorry. Commissioner Anthony, I am sorry. I apologize.

Ms. ANTHONY. That is all right, Senator McCain.

My view is that a uniform standardized notice setting forth in a simple manner, understandable and noncontradictory would be a good thing for consumers to reveal what exactly the Web site's practices are, and then have an opportunity to either opt in or opt out. If there is additional information that needs to be conveyed to the consumer, there could be interactive "click-here" links on a standardized uniform notice that could be utilized to further explain the policy.

But I do not think consumers have any protections if the policy is so confusing that not even a university professor can understand it.

The CHAIRMAN. Well, I will not comment on university professors.

Commissioner Swindle.

Mr. SWINDLE. Mr. Chairman, I think we all agree that these lengthy dissertations that we go through, they are so bad that we do not look at them. That is obviously counterproductive, and I think we can all agree that some form of reasonable English notice—and I do not want to get trapped into saying I am for English only here, since we have other people of other languages——

The CHAIRMAN. How do we enforce that, then?

Mr. SWINDLE. The enforcement of it, I think, comes from the Federal Trade Commission with its existing regulations. We had a case here a couple of years ago called Geocities. It is a very popular site. I personally have never visited it, but I will take the staff's word that it is very popular. They had a privacy statement and they said that, we will do certain things.

We alleged that, contrary to what they said, they turned around and shared the information with a third party in some sense. They settled the case with us. However, once they posted the policy they then came under the umbrella of Section 5 of the Federal Trade Commission Act, and if they are deceiving their customers we have authority to do something.

Now, our surveys, as has been reflected here in some of the numbers that are addressed today, indicate that something on the order of 90 percent of all Web sites have posted some form of notice. Now, if that notice was properly conveyed in a more simple manner than we are seeing now, to express what the site does in the way of collecting information and how it uses it, all those sites would be under the oversight of the Federal Trade Commission under the existing laws.

I might point out that, even though we have a quantum leap in the number of sites that have these notices, we have only handled just a bare handful of cases in which we have challenged the practices that they are implementing, having stated what they do, such as in Geocities. But I think if we continue to expand the numbers of people who have notice, state their privacy policies, and we apply very close scrutiny on what they are doing, I think the effects of FTC action will have a positive effect on seeing more comply with it.

The CHAIRMAN. Commissioner Thompson.

Mr. THOMPSON. Mr. Chairman, I agree with you that—and you are talking about what we consider to be the good guys, because there are people out there who are saying nothing, and that we have very few tools to get at those people. One of the questions that some people raise is what is it that industry cannot fix on its own? As you may remember, last year I was here and I talked to you a little bit about coverage, and I said that there is a core group that you still cannot get to. They are still out there, and consumers deserve better.

Second of all, there is also a benefit to having a level playing field here, so that there are not these wide disparities, so the consumers wind up taking a risk every time they go on the Internet.

The reason I might disagree slightly with some of my colleagues about why online and why now, is because the Internet provides you with an opportunity. The Internet allows somebody to follow you around the shopping mall without your knowledge. It is a little bit different. And because it allows you to aggregate data and col-

lect it on a real-time basis as you put it in, they get it and they use it, means something. So I think there is a slight difference.

One other thing is that I understand that Forrester Research is coming out with a report today that is going to talk a little about this, about some of the pressures on businesses in the dot-com space that make it more advantageous to sell data. They need to do that for economic reasons, and the combination of hyper-partnering, meaning companies doing things with other companies, the pressure to get profits in that way may actually mean that you will see more of this occurring in the Internet space faster.

The CHAIRMAN. Mr. Leary.

Mr. LEARY. Mr. Chairman, I agree with the majority here that there should be some legislation directing us to make rules to assure more consistent and more adequate disclosure. That is something we know how to do and we have done in other areas.

I also agree with a somewhat different majority that you should have the same disclosures when you order by mail or when you open a charge account at your department store to the extent the information is exactly the same.

Thank you.

The CHAIRMAN. Senator Hollings has a question, and we have two votes on the floor and after that we will take a brief recess until we can return from the vote. Thank you. Senator Hollings.

Senator HOLLINGS. There is not any question that the offline should be regulated as online. We gave it to you to do just as you just said, Mr. Leary, that you promulgate rules and regulations for the offline as we have it for the online. Otherwise we have got the proposition, of course, that it is going to be more difficult each day that passes to ex post facto or retroactively do anything. We are into an environment where the best of the best—and I know Fred Yang and Yahoo and they are one of the best, and yet they give little notice. You can see the game that is going on.

I feel like I am in a class where the professor is grading by way of a scale and everybody is cheating. I am going to have to cheat in order to pass, regardless of how much I know about the subject.

Kennedy said years ago, the captain who waited for his ship to be fit never puts to sea. So we put to sea with S. 2606, and we did it with your counsel. There is not any question that you folks are the nearest experts I can find and the most objective folks that I can find. Our staff has done, along with your staff, an outstanding job.

We have drawn a target with S. 2606. Maybe most of you have not had a chance to read it because we waited for you to submit your report and then we of course introduced our bill. We already have ten co-sponsors.

I want each of you in writing to give me criticisms of that particular bill, what is heavy-headed, what is unrealistic, and what is impossible for industry. We have been very considerate of industry. The Internet is not going to stop. All of these folks here act like some day it is going to slow down. It will never slow down. This thing is a dynamic that is running way ahead of all of us, and each day that passes with State's attorneys general all trying to pass their laws, with any and everything coming out of the Congress and nothing real, we have got to really move on this thing. After

5 years, I think we are pretty well in a position to move with your counsel and criticism.

Please do that for me, and we thank you very, very much for what you have done for us so far.

Excuse me. The Committee will be in a brief recess.

[Recess.]

The CHAIRMAN. The Committee will resume. Please, Commissioners, take your seats, and we will begin questioning. I think Senator Wyden by early bird rules is next.

Senator WYDEN. Thank you. Thank you very much, Mr. Chairman. I will let our guests get their seats.

[Pause.]

Mr. Chairman, this question is for you. As you know, Senator Burns and I have been at it for well over a year trying to craft bipartisan legislation. As I have indicated, I happen to think that Senator Hollings, Senator Kerry, and others are making important contributions. I think it would be helpful if you could tell us, in your view are there any dangers in waiting to pass bipartisan privacy legislation?

Mr. PITOFSKY. It is an interesting question. Yes, I think that there are inappropriate invasions of privacy that go on at this time, and they are of a sort that it is difficult for us to get at under present law. Nothing is said about privacy or it is a confusing disclosure, but not really a deceptive one.

So I think there is always a question of protecting consumer rights as promptly as possible. On the other hand, I do think, having worked on this now for 5 years and very energetically for 3, there are differences of view reflected in some of the legislation. There are tough questions that were raised by our advisory committee and in our report. Therefore I think it is more important to do this in a thorough and careful way than to rush to any judgment in this area.

I think we are all aware that it is the end of a Congressional session and there are not that many legislative days left. If it can be done appropriately in a short period of time, fine. But I think it is more important to get it right.

Senator WYDEN. Do you believe that you have existing rulemaking authority under your underlying statute, the organic statute, to protect consumer privacy?

Mr. PITOFSKY. No, we do not. That is the point. It seems to me we need the kind of legislation that we have recommended and that you and Senator Burns have authored in order to engage in rulemaking. We could call invasions of privacy "unfair," but I do not believe that we could sustain that position.

Senator WYDEN. Let me wrap up with this. I do not think what you are talking about now is a radical departure from your previous position, and I do not think you are abandoning self-regulation. I hope that what people will see in this whole effort is that this is not some sinister government power grab. This is an opportunity to empower the consumer; at the end of the day, what we want to do is give consumers control over important information.

We can have this debate about the technical terms, opting out and opting in. In English what we all understand is that explicit permission from the consumer for things like medical and financial

information is clearly their expectation. Senator Kerry has defined that as opt-in.

At the same time, if you subscribe to *Newsweek* for 20 years and they are thinking about contacting you for the 21st year, we should not make them send you one letter in order to get permission to send another letter. I think the approach that you are talking about is very much in line with the bipartisan legislation that Senator Burns has talked. I think it is consistent with the kinds of ideas Senator Hollings and Senator Kerry have expressed, and we appreciate your leadership and look forward to working with you.

Thank you, Mr. Chairman.

The CHAIRMAN. Senator Kerry.

Senator KERRY. I appreciate Senator Wyden's comment. Senator Wyden, Senator Hollings, Senator Rockefeller, and I were chatting on the floor a few moments ago, and it seems to me that there is an opportunity here for us, Mr. Chairman, to try to see if we cannot find a bipartisan meeting ground here that pulls people together. I do not think we are that far off.

Clearly, medical and financial Web sites deserve some kind of special status. I think we can agree on that. We need to find a way to do that.

I still maintain that the degree to which, when you get beyond the notice, the choice, access, and security issues are at this point perhaps left too much to the regulatory process rather than trying to bring the marketplace into it. This would bring the private sector into some perhaps joint resolution that might even result, for instance, in something like an FTC seal of approval, in conjunction with the corporate community in a joint effort to arrive at an agreement as to what the appropriate measure should be.

It seems to me there are some choices in front of us. But I still remain troubled. Let me ask this question first. If we were to pass a fairly significant disclosure and fairly clear disclosure requirement, without mandating in specificity each aspect of choice, access, or security, would you not then be empowered to enforce? And would you not, if you joined together with the community in this sort of FTC seal, be leveraged significantly in your ability to be able to hold people accountable?

Mr. PITOFSKY. In my view, a notice bill is better than the status quo and I would be comfortable with it. But I think we should go further. I believe Congress should go further.

Let me emphasize the choice aspect, because access and security become very complicated. But what would be the consequence of a bill that mandated notice—and we could enforce that, of course—but did not provide choice? Well, first of all I would point out that is not the way we do things in consumer protection. We do not say to consumers: If you go to a store and you are the victim of bait and switch, if you buy a defective product, if you buy a dangerous product, if you are abused in credit terms, then why do you not go to some other store? We say to them: You have a right to be protected against fraud.

Now, if privacy is worthwhile—and I believe it is—then we ought to go the next step and say: First, you should be told what is going to happen with that information; and, second, you should be given an opportunity to say count me out.

Senator KERRY. Sure. But my point is, rather than mandating whether it is going to be opt-out or opt-in in a particular instance, it seems to me you could arrive with the industry at a fair set of options on which you put your approval. And if they vary from that or they are not clear, as Chairman McCain suggested they are not in eight pages—I agree with that. It is clear. You go on the Internet today to some of these sites and it is an exercise in obfuscation. They are clearly trying to not have you opt-out.

So we need to empower consumers. Most people I talk to who are in the industry want to empower consumers. The entire salesmanship of this industry has been based on its democratization impact and consumer empowerment. So it seems to me you could arrive at that, could you not?

Mr. PITOFSKY. I agree and I think we could. I think if we sat down with the responsible people in this industry, from what I have seen of their behavior so far, we could find common ground about what the rules of play ought to be.

Senator KERRY. I also want to say that I think it is far more urgent because of the conglomeration of information on the net and because of the speed with which the net moves and sort of the new awareness of choice. The American public is now becoming far more sensitized to the privacy issue.

But, in point of fact, we cannot just gloss over this offline-online distinction. It sometimes amuses me. Somebody does not want to give their credit card on the Internet, but they will hand it to a waiter at a restaurant they have never been to and they are never going to go to again. He disappears in a back room for 5 minutes and they do not have a clue what happened to the credit card or what may happen in the ensuing days.

Likewise, you can buy, I am told, criminal information records on individuals in the marketplace today. Additionally, information is available on somebody's social security number and through any kind of credit check. I have seen people's personal credit card transactions appear in newspapers based on their private sleuthing through the offline market.

So the notion that there is some new threat really needs to be thought through, because the level of loss of privacy of the average American today is absolutely extraordinary. Marketing takes place in highly specified ways offline, but we are only worried about online, this seems imbalanced.

Do you not agree that these are inconsistencies we have got to try to work through?

Mr. PITOFSKY. I do agree with that.

Senator KERRY. Are there not dangers in the offline issue?

Mr. PITOFSKY. Speaking for myself, I have increasingly come around to the view—I did not start there—that the theory of distinguishing online from offline is really rather weak. I was very influenced by one of our advisory panel people who said: What is the point of treating differently warranty information that is gathered when the consumer files a warranty card—an example of offline private information—when we know some clerk is going to sit there and read it right into an electronic format? Why would you treat one differently than the other? I found that a very powerful argument.

I am also influenced by the fact that we hear that through mergers, joint ventures, and otherwise that online and offline companies are merging their data bases, and that is another reason why we should think about both.

Senator KERRY. But I also say respectfully, and I will terminate on this, that that is another reason why I think we need to approach this thoughtfully and carefully. I suggest simply that if we had at least the first step, where we all could agree on a simple, clear, straightforward form of required disclosure with a set of principles on which each of the acceptable four major principles and enforcement: security, access, choice, notice, and enforcement. If we could establish that in terms of principles, and then you went to work with the industry, it seems to me that you may wind up with a better product. Meanwhile, we can go to work.

Now, I want to emphasize, Mr. Chairman, on financial information and medical information those are places where there ought to be significant rigidity and clarity, and I hope the Committee can come together on it.

Thank you, Mr. Chairman.

The CHAIRMAN. I would remind Committee members we do have another panel after this and it is now quarter to 12. So I hope we can ask sufficient questions and yet exercise brevity.

Senator Burns.

Senator BURNS. Thank you, Mr. Chairman.

I only have one question in listening to the testimony here. It will be very simple. We are pretty much—we agree that the four areas of concern in this are notice, choice, access, and security. Ms. Anthony, I was interested in your recommendation on strong enforcement mechanisms as well as an audit process. Can you give me some detail on what that might look like? I would be interested in that.

Ms. ANTHONY. Well, as I said in my testimony, Senator Burns, there are enforcement mechanisms at hand. The seal programs I think really had a very sensible way to deal with privacy. However, I am unaware of anybody that they have kicked out for not complying, and I do not think everyone has complied.

I think also that government has used, in the past, industry standards in audits, and that is just another suggestion. I am not making any firm recommendation on those fronts. I am just throwing them out as suggestions for you to consider when you devise some enforcement mechanism.

Senator BURNS [presiding]. That is—everybody jumped up and ran away. Oh, are you next? Senator Rockefeller. If you can be brief, please.

[Laughter.]

Senator BURNS. Sorry I asked.

Senator ROCKEFELLER. A couple quick points. A comparison was made between fraud and privacy, and I just want to emphasize the enormity of the issue of privacy. It affects every single American, mostly without their knowledge, as opposed to fraud, which is the usual thing you complain about with Medicare and other things—waste, fraud, abuse, etcetera. These are issues of enormously different dimensions.

Second, if you have voluntary compliance or if you have a regulatory system set up in which you actually get 80 percent or 90 percent of companies that are complying with proper notification that meets all of Commissioner Anthony's specifications, that the 10 percent can undo all of the 90 percent in an instant. So it has got to be 100 percent. That is not offline; that is an online problem.

That is why I think that we tread on dangerous water when we start comparing offline and online and saying, well, if we are going to do one we have got to do the other. They operate under different sets of market rules and they access or make themselves available and dangerous to the American public at very different levels of speed and enormity.

About nine out of ten businesses that start up fail. This means that businesses are starting often. Their accounting rules have changed and now we have discovered they do not have as much money as they thought they did, but people are still into it. It is driving the economy and it is a very good thing for America and for the world.

But again, all it takes is a couple of startups that do not have the money or the time or cannot afford the lawyers to be able to put that proper notification on. All the good work that you enforce or lay out self-regulatory or we lay out other rules for is gone. The 2 percent can undo the 98 percent because once they sell it to the third-party purchaser or they have bought it from a third-party purchaser, it is all gone.

That point needs to be made. That is why I think this is a very different level of problem than talking about online-offline.

The third thing I want to say is that this is a wonderful set of circumstances into which to introduce minutia which distracts, but which is nevertheless important as you listen to it. Witness: Somebody comes in my office yesterday, they do not like what Senator Hollings and I are doing, and so they say, but if you get into access, that means that the consumer might be, as we used to say, a deadbeat dad, until we started getting all the letters from dads who did not consider themselves that way. They go in and then they change information to protect themselves from having to do what they need to do. Or criminals also can access and change their records.

In other words, there are a thousand ways you can come at this to nitpick, to show that there is no perfect software, there is no perfect system. What that does is it tends to throw us on the defensive and say, oh, we cannot do that. We cannot have deadbeat dads changing their records so they do not have to pay child support. Let us just back off and do nothing.

Again, I come back to my original point. We do not have that luxury. I think that is why, Mr. Chairman, you come down with the line of we have to do better. And I think you want to do online and offline together, but my question is are they really of the same dimension? Do they move at the same speed? Do they have the same consequences, offline as online? I think that you would agree with me that they do not.

Mr. PITOFSKY. I do agree with you, Senator. I think the online threats to the privacy of consumers is greater than offline because of the way in which information can be gathered, marshalled, sorted out, accumulated, and then sold. So it is different. But I do not

know about very different. There are threats to privacy that occur in the offline world that deserve our attention.

I know the bill that you are sponsoring suggests that the FTC take a look at that and report back to Congress, and I think that is the right way to go. We did not report on it on this occasion, because we really had not investigated it.

The CHAIRMAN [presiding]. Thank you.

Senator Bryan.

Senator BRYAN. Mr. Chairman, if I might just followup on that. You are not suggesting, however, that because in your own thought process as you describe the evolution of the significance of offline privacy invasion, that we should hold up on these recommendations in terms of developing these base standards of notice, choice, access, and enforcement? I want to be clear on that.

Mr. PITOFSKY. Yes, Senator, exactly right, I am not.

Senator BRYAN. Mr. Swindle, if I might ask you a couple of questions. I believe you were a dissenter in the report that the majority filed. As I understood the thrust of your testimony, you believe that self-regulation ought to be given an opportunity to work its course before we embark upon a legislative course of action. Is that a fair statement of your position, sir? I do not want to mischaracterize it.

Mr. SWINDLE. Yes, sir, that is a fair description of it, but it goes further than that. My concerns with the report were that the report is a misconstruing of information and data. It is the basis for making the recommendation that we have this very broad, all-encompassing legislation on virtually every Web site that exists. And, I think the data is used in a misleading manner and that leads to a recommendation which is illogical. I think we are on the wrong track.

Senator BRYAN. Do you support the concept that consumers ought to be given a notice of what the privacy policies are of online providers?

Mr. SWINDLE. Yes, sir.

Senator BRYAN. Well, let me ask you to respond. Ms. Anthony had an example which she shared with us, where you have got to be referred from one page to another and several hundred intervening words. Our Chairman cited an example of one which I think any fair-minded person would say is not effective notice. I believe that Senator Kerry used the word "obfuscation." I would say that it triumphs form over substance.

Now, why should we not have some legislative standard that requires meaningful notice if this kind of action is being done by some of the major online providers in the country?

Mr. SWINDLE. Senator Bryan, I think you will perhaps recall, in commenting to Senator McCain's comments, I said these things are so ridiculous that I do not even read them. I just click them off.

Senator BRYAN. I apologize, I think I had to leave.

Mr. SWINDLE. I am in the same group, and I think some form of clear and conspicious notice would be most appropriate. I also made the statement that, in effect, our survey indicates that in excess of 90 percent of Web sites now provide some form of notice already. It is not the best of notices because some of them are Yahoo versions and some of them probably do not say anything other than, "we have a privacy policy." So the quality of that statement,

if it were prepared and put into very clear and precise, easy to understand form, would be a very good thing to do.

I think choice naturally follows from being able to understand what is before you. It is like going into a store, it costs a dollar for this ball. If I want to pay a dollar for the ball, I pay it. If the privacy notice says, we want to collect this information if you want to come into our site, then you make a choice. You go or do not go.

Senator BRYAN. I am sure there are other examples other than those that were cited for the record. The notices are misleading and confusing, and I think you are saying that you agree that in effect those are not real notice. Do we not need to have some type of a legislative response that says, look, notice cannot be just some game in which the consumer is moved from one link to another on a web page. It has got to be meaningful.

Is there anything wrong with a legislative standard that requires notice to in fact be——

Mr. SWINDLE. No, sir.

Senator BRYAN. So you would agree with that?

Mr. SWINDLE. My disagreement is with the all-encompassing nature of the recommendation. We are not talking about the same thing here.

Senator BRYAN. So you would have no problem with legislation that talks about notice in a meaningful sense?

Mr. SWINDLE. Yes, sir. And I think in my statement or my dissent I said if the Congress believes we must legislate, let us go no further than notice.

Senator BRYAN. Notice. Let me ask about an aspect of enforcement. Mr. Chairman, this is my last question. You have been patient, but I do not think I have belabored the point.

We had a situation with Chase Manhattan, one of the major banks in America. Those of us that serve on the Banking Committee know. Their privacy policy indicated a course of action in terms of how they would deal with consumer information, with private information. In point of fact, they violated their own consumer policy and sold to third party telemarketers. They received a 24 percent commission for each sale that was ultimately consummated as a result of that third party, the telemarketer, negotiating with the customer.

Now, ultimately what occurred, as you know, is the Attorney General in New York brought suit. But that deals with an enforcement issue. I mean, I do not know the law of every state in the country, and I certainly do not know the particular circumstances of the New York law. But, clearly, that is such a blatant violation of a stated policy there has got to be some enforcement.

Would you agree with that point, Mr. Swindle?

Mr. SWINDLE. Yes, sir, and we can do that under Section 5 of the Federal Trade Commission Act. I made reference earlier to Geocities, which is exactly that case. We would not be involved in the banking industry, as the Senator knows. But in the case of Geocities they had a privacy statement, they said we will do A, B, and C, and we found out later, alleged that they did A, B, C, D, E, and F and did a similar thing, they sold the information to third parties. And we have the power today to take enforcement action against them.

Senator BRYAN. So I take it from your response that it would be within your jurisdiction. Maybe we need to look at that; that is a separate issue. So you would certainly favor a regulation that would clearly provide some sanction for violation of a stated privacy policy such as that?

Mr. SWINDLE. We have that authority today under existing law.

Senator BRYAN. Mr. Chairman, thank you very much.

I appreciate your response, Mr. Swindle.

The CHAIRMAN. Thank you.

I would like to tell the witnesses I appreciate their patience. I apologize for the break while we had a couple of votes. I thank you for helping us address these very difficult issues. We will be in communications with you. In fact, we may ask you to come back if and when there is some proposed legislation concerning this very, very important issue.

So thank you very much.

Mr. PITOFSKY. Thank you, Mr. Chairman.

The CHAIRMAN. The next panel is: Ms. Jill Lesser, Vice President of Domestic Public Policy, America Online; Ms. Christine Varney, senior partner of Hogan and Hartson, testifying on behalf of the Online Privacy Alliance; Mr. Jason Catlett, President of the Junkbusters Corporation; Mr. Jerry Berman, Executive Director, Center for Democracy and Technology; and Mr. Daniel Weitzner, who is Technology and Society Domain Leader of the World Wide Web Consortium.

I would ask those who are departing to expedite their departure and those who are witnesses to please come forward as quickly as possible so we can continue the hearing.

I want to thank all the witnesses for their patience. Obviously, your complete statement will be made a part of the record. Welcome, Ms. Lesser.

STATEMENT OF JILL A. LESSER, VICE PRESIDENT OF DOMESTIC PUBLIC POLICY, AMERICA ONLINE, INC.

Ms. LESSER. Thank you, Chairman McCain, and I will try to be brief. Chairman McCain——

The CHAIRMAN. Could I emphasize, of course, we want you to be brief, but it is most important that we receive the information you have to impart. If there is any appearance of impatience on the part of the chairman and members of the Committee, please disregard that. The most important thing——

[Laughter.]

Ms. LESSER. I will take that under advisement.

The privacy report issued this week by the Federal Trade Commission shows in many ways that we have reached a crossroads in the development of the online medium. It is clear that the Internet is revolutionizing our society, dramatically changing the way we learn, communicate, and do business. People are migrating to the Internet to meet their commerce and communications needs at an extraordinary rate because it is convenient and fast and offers unprecedented selection of information, goods, and services.

Yet, despite this enormous growth the Internet has enjoyed over the past few years, or perhaps because of it, we have seen a heightened awareness of online privacy and security issues, consumer

protection, and a whole host of issues related to online safety. And even though the medium continues to grow at an enormous rate, online companies are realizing that it is their responsibility to address these issues for their consumers.

Of course—and I think this has perhaps been underemphasized today—this medium offers to users an ability unprecedented to customize and personalize their experiences. Consumers can, and do on a regular basis, communicate specific preferences that will allow them to receive information tailored to their own interests.

No other commercial or educational medium has ever afforded such tremendous potential for personalization, and we are seeing consumers take advantage of these opportunities at an incredible rate. But we know that the power of the Internet can only be fully realized if consumers feel confident that their privacy is properly protected when they take advantage of these benefits, and therefore we, along with many other companies, are protecting privacy. We view it as an essential aspect to earning their trust, and this trust is, in turn, essential to building the medium.

That is why we and other companies have devoted so much time and energy to creating strong policies that provide meaningful protection. As we have discussed much this morning, there are several important elements of those policies and I believe many, particularly the industry leaders, have policies that address all of those elements.

Our own commitment is based on the lessons we have learned and the input we have gotten from consumers, policies that clearly notify our users what information will be collected, why, how it will be used, and the opportunity to exercise choice and disclosure. Indeed, we intend to fully implement those notice and choice principles across all of our brands when we hope our merger with Time-Warner is finally consummated.

We also make sure that our policies are well understood with respect to our employees, and I think this is an important point as well. Implementation throughout a company of a privacy policy is critical to making sure that it is really truly within the ethos of all of our companies.

We do try to keep users informed about the steps they can take. That is, do not give out your password and certainly do not give information out to companies or anybody you do not know and you do not trust.

Finally, with respect to children, we have worked with many of you, Senator Bryan and Senator McCain in particular, supporting the Online Privacy Act related to children in the 105th Congress and do believe it was an area where additional steps were needed.

In adopting and implementing our own policies, we are committed to fostering best practices within the industry, and you will hear from the Online Privacy Alliance and many other trade associations and others we have worked with, and we have done a lot to make sure that our business partners are also following important privacy policies.

So after all of that background, where are we now? The FTC report concludes that, despite this progress, industry has not done enough and that broad privacy legislation is necessary in order to ensure that consumers are protected. Does this mean in their view

that self-regulation is a failure, and what are we as industry therefore supposed to do?

As the Committee and other Congressional leaders begin to sift through the FTC's recommendations, I would just like to offer a few thoughts as you do that. First, it is important for all of us in industry and government to stop thinking about this issue as a zero sum game, as self-regulation versus government regulation. Instead, we must remember that the crux of the issue is about consumer confidence, consumer protection, safety, and security, and since all of us have the same end goal, to ensure that consumers trust the online medium, we do not need to set ourselves up as opponents in a privacy battle.

One way to approach this joint responsibility is to allow the market to lead, as it has, in developing up-to-date and innovative initiatives for protecting privacy, but give the government its important enforcement activities. Indeed—and I think this is important to note in light of all the numbers we have heard today—the government's existing enforcement powers are greatly expanded simply by the proliferation of privacy policies, now numbering almost 90 percent.

If you look at the examples used by Chairman McCain, by Commissioner Anthony and others this morning about perhaps unfair or deceptive privacy policies, I would note that the FTC does have broad enforcement authority in those areas. So if you compare 90 percent of sites having privacy policies with the enforcement authority of the FTC, I think there is an enormous amount of coverage that we are underestimating.

Second, I would say that it is critical that neither the government nor industry view this issue as simple. On the contrary, when we as businesses ask our consumers what they are most concerned about, we get a variety of different answers. For some consumers, it is really security rather than privacy—identity theft, hacking—and certainly this is an area where the industry has every incentive to do the right thing, but the government must make clear that bad behavior is unacceptable.

For other consumers, the primary concern relates to sensitive information, an issue we have talked about a lot this morning. Individuals want to take advantage of online health-related services, for example, without worrying about embarrassing or compromising releases of their health information. Indeed, Congress has addressed these issues through financial services legislation enacted last Congress and the Health Insurance Portability and Accountability Act of 1996, neither of which, I would note, have been fully implemented. So we do need to make sure we understand what is out there.

Such examples and others underscore the intricacy of the privacy issue and the difficulty in pinpointing the actual problems that need to be addressed through industry or government action. Unfortunately, I would say the FTC's recommendation for a sweeping regulatory regime for online privacy does not take into account either the complex dimensions of this issue or the need for industry-government partnership on privacy.

The Commission purports to recognize the important role that industry leadership on self-regulation has played, yet it recommends

broad legislation with expansive regulatory authority that could actually discourage industry-led initiatives and market-driven solutions by outlawing consumer-oriented methods of privacy protection and personalization.

We would therefore simply ask that members of this Committee look at privacy with a high regard for the benefits of personalization and the efficacy of industry action to date. You may find there are gaps in industry enforcement where government must step in to ensure compliance. Nevertheless, it is clear that companies are responding to increasing marketplace demand for online privacy, and the tremendous growth of e-commerce reflects a positive trend on a variety of consumer protection issues, including privacy.

The challenges that lie ahead will give us a chance to prove that industry and government can work together, but ultimately it is the consumer who will judge whether those efforts are adequate because, no matter how extraordinary the opportunities for e-commerce may be, the marketplace will fail if we cannot meet consumers' demands for privacy protection and gain their trust.

We as a company are committed to doing the right thing. We believe our colleagues in the industry are as well. We appreciate the opportunity to discuss these important issues with you this morning. Thanks.

[The prepared statement of Ms. Lesser follows:]

PREPARED STATEMENT OF JILL A. LESSER, VICE PRESIDENT OF DOMESTIC PUBLIC POLICY, AMERICA ONLINE, INC.

Chairman McCain, Senator Hollings, and Members of the Committee, I would like to thank you, on behalf of America Online, for the opportunity to discuss online privacy with you today. My name is Jill Lesser, and I am the Vice President for Domestic Policy at AOL.

The privacy report issued this week by the Federal Trade Commission shows that, in many ways, we have reached a crossroads in the development of the online medium. It is clear that the Internet is revolutionizing our society—dramatically changing the way we learn, communicate, and do business. People are migrating to the Internet to meet their commerce and communications needs at an extraordinary rate because it is convenient and fast, and offers an unprecedented selection of information, goods and services. AOL subscribers can sign on to our service and do research, shop for clothing, obtain health information, and buy airline tickets—all in a matter of minutes. And every day we are seeing new online opportunities arise, and new users flocking to take advantage of these opportunities.

Yet despite the enormous growth that the Internet has enjoyed over the past few years—or maybe because of it—we have seen a heightened awareness of online privacy and security issues. Every day we are faced with new reports, studies, and statistics—many of which seem to contradict each other—about how Internet users feel about the medium and how online privacy is, or isn't, being protected. And even though the medium continues to grow at an incredible rate, online companies are realizing that they have to sit up and pay attention to privacy if they want to stay in business.

Of course, one of the most attractive benefits that this medium offers to users is the ability to customize and personalize their online experience. Consumers can communicate specific preferences online that will allow them to receive information tailored to their own interests. For instance, AOL members can set their online preferences to get sports scores or stock quotes, read news stories about their own hometown, or receive notices about special discounts on their favorite CDs. No other commercial or educational medium has ever afforded such tremendous potential for personalization, and we are seeing customers take advantage of these opportunities at an incredible rate—through our own services and through countless other business models for personalization, from online bookclubs to discount ticket agencies to special offers from the local supermarket.

But we know now that the power of the Internet can only be fully realized if consumers feel confident that their privacy is properly protected when they take advan-

tage of these benefits. If consumers do not feel secure online, they will not engage in online commerce or communication—and without this confidence, our business cannot continue to grow. For AOL, therefore, protecting our members' privacy is essential to earning their trust, and this trust is, in turn, essential to building the online medium. That's why AOL and other companies have devoted so much time and energy to creating strong privacy policies that provide meaningful protection and are backed up by compliance and enforcement programs.

AOL's own commitment is based on the lessons we've learned over the years and the input we've received from our members. We've created privacy policies that clearly explain to our users what information we collect, why we collect it, and how they can exercise choice about the use and disclosure of that information. AOL's current privacy policy is organized around 8 core principles:

- We do not read your private online communications.
- We do not use any information about where you personally go on AOL or the Web, and we do not give it out to others.
- We do not give out your telephone number, credit card information or screen names, unless you authorize us to do so. And we give you the opportunity to correct your personal contact and billing information at any time.
- We may use information about the kinds of products you buy from AOL to make other marketing offers to you, unless you tell us not to. We do not give out this purchase data to others.
- We give you choices about how AOL uses your personal information.
- We take extra steps to protect the safety and privacy of children.
- We use secure technology, privacy protection controls and restrictions on employee access in order to safeguard your personal information.
- We will keep you informed, clearly and prominently, about what we do with your personal information, and we will advise you if we change our policy.

We give consumers clear choices—which are easy to find and easy to exercise—about how their personal information is used, and we make sure that our users are well informed about what those choices are. For instance, if an AOL subscriber decides that she does not want to receive any tailored marketing notices from us based on her personal information or preferences, she can simply check a box on our service that will let us know not to use her data for this purpose. Because we know this issue is so critically important to our members and users, we make every effort to ensure that our privacy policies are clearly communicated to our customers from the start of their online experience, and we notify our members whenever our policies are changed in any way.

We also make sure that our policies are well understood and properly implemented by our employees. We require all employees to sign and agree to abide by our privacy policy, and we provide our managers with training in how to ensure privacy compliance. We are committed to using state-of-the-art technology to ensure that the choices individuals make about their data online are honored, and that such data is protected and secured.

And we try to keep users informed about the steps they can take to protect their own privacy online. For instance, we emphasize to our members that they must be careful not to give out their personal information unless they specifically know the entity or person with whom they are dealing, and we encourage them to check to see whether the sites they visit on the Web have posted privacy policies and to review those policies.

Furthermore, AOL takes extra steps to protect the safety and privacy of children online. One of our highest priorities has always been to ensure that the children who use our service can enjoy a safe and rewarding online experience, and we believe that privacy is a critical element of children's online safety.

We have created a special environment just for children—our "Kids Only" area—where extra protections are in place to ensure that our children are in the safest possible environment. In order to safeguard kids' privacy, AOL does not collect personal information from children without their parents' knowledge and consent, and we carefully monitor all of the Kids Only chat rooms and message boards to make sure that a child does not post personal information that could allow a stranger to contact the child offline. Furthermore, through AOL's "Parental Controls," parents are able to protect their children's privacy by setting strict limits on whom their children may send e-mail to and receive e-mail from online.

As you know, AOL supported legislation in the 105th Congress to set baseline standards for protecting kids' privacy online—precisely because of the unique concerns relating to child safety in the online environment. We worked with Senator Bryan, Senator McCain, the FTC, and key industry and public interest groups to help bring the Child Online Privacy Protection Act (COPPA) to fruition. We believe the enactment of this bill—which took effect last month—was a major step in the ongoing effort to make the Internet safe for children.

In addition to adopting and implementing our own policies, AOL is committed to fostering best practices among our business partners and industry colleagues. One of the strongest examples of this effort is our "Certified Merchant" program, through which we work with our business partners to guarantee our members the highest standards of privacy and customer satisfaction when they are within the AOL environment. AOL carefully selects the merchants we allow in the program, and requires all participants to adhere to strict consumer protection standards and privacy policies. The Certified Merchant principles are posted clearly in all of our online shopping areas, thereby ensuring that both consumers and merchants have notice of the rules involved and the details of the enforcement mechanisms, which help to foster consumer trust and merchant responsiveness.

Through our Certified Merchant program, we commit to our members that they will be satisfied with their online experience, and we have developed a money-back guarantee program to dispel consumer concerns about shopping online and increase consumer trust in this powerful new medium. We believe that these high standards for consumer protection and fair information practices will help bolster consumer confidence and encourage our members to engage in electronic commerce.

We at AOL are proud of the steps we've taken to create a privacy-friendly environment online for our members and encourage our industry colleagues to do the same. But we haven't done these things to prove a point or to discourage government regulation—we've done them because we *must* do them, because our business, more than ever, requires us to respond to consumer demands and take privacy seriously in order to build more consumer trust in the medium. And we know that many other online businesses feel exactly the same way. That's why AOL joined with other companies and associations two years ago to form the Online Privacy Alliance (OPA), about which you will hear more this morning from another witness. And that's why through NetCoalition, a group representing some of the largest and most active online companies, we recently sent a letter to 500 CEOs encouraging them to post good privacy policies on their Web sites that contain the key fair information principles, and to fully implement these policies within their companies. The progress that industry has made is *real*—one thing the FTC report clearly shows is that the proportion of commercial Web sites posting privacy policies has skyrocketed in less than three years from less than 14% to over 90%—unbelievable progress for an industry that barely existed just a few years ago and which today is demonstrating the most rapid growth in the history of media.

So where are we now? The FTC report concludes that, despite this progress, industry hasn't done enough, and that broad privacy legislation is necessary in order to ensure that consumers are protected. Does this mean that self-regulation is a failure? What are we supposed to do next?

As the Commerce Committee and other Congressional leaders begin to sift through the FTC's recommendation and face the issue of whether to take action in this area, I would like to offer just a few thoughts on how you might approach answering these difficult questions:

First, it is important that all of us in industry and government stop thinking about the privacy issue as a "zero sum game"—as self-regulation versus government regulation. Instead, we must remember that the crux of the issue is really consumer confidence, consumer protection, safety and security. And since all of us have the same end goal—to ensure that consumers trust the online medium—we do not need to set ourselves up as opponents in a privacy "battle." Clearly the industry has an enormous incentive to make consumer protection a fundamental part of doing business, but there is also an important role for government in protecting consumers. One way to approach this joint responsibility is to allow the market to lead the way in developing up-to-date and innovative initiatives for protecting privacy, but let the government step up its enforcement activities. Indeed, the government's existing enforcement powers are greatly expanded simply by the proliferation of privacy policies, now numbering 90 percent. This type of partnership allows for maximum flexibility and technological innovation, so that the "good guys" can set the stage for best practices while the "bad guys" pay the price for bad behavior.

Second, it is critical that neither the government nor industry view privacy as a simple issue with a simple answer. On the contrary, when we as businesses ask our

consumers what it is they are most concerned about we get a variety of different answers:

- For some consumers it is security rather than privacy that is the greatest concern. They care more about whether their credit cards can be safely "submitted" online than about whether their ISP will send them a tailored advertisement. In reality, the risks of identity theft may actually be greater in the offline world than in the online world, where fewer humans actually touch or handle an individual's credit card, for example. Yet the prospect of personal information being compromised through hacking and theft is likely keeping many consumers from going online. This is certainly an area where the industry has every incentive to do the right thing but the government must make clear that bad behavior is not acceptable.
- For other consumers, the primary concern relates to sensitive information like health and financial data. Individuals want to take advantage of online health-related services, for example, without worrying about embarrassing or compromising releases of their health information. For these types of information, industry and government will need to determine what privacy standards need to be in place for particular businesses to succeed, and indeed Congress has already addressed these issues through financial services legislation enacted last Congress and the Health Insurance Portability and Accountability Act of 1996, neither of which have yet been fully implemented.
- Still another group of consumers is concerned about whether their online behavior is being "tracked." Yet when the technologies behind such activity are explained and consumers are able to understand that there are both positive and negative uses of these types of tools, it may turn out that consumers simply want to know what a particular Web site is doing so they can make their own decisions about how to use these services.

Such examples underscore the intricacy of the privacy issue and the difficulty in pinpointing the actual problems that need to be addressed through industry or government action.

Unfortunately, the FTC's recommendation for a sweeping regulatory regime for online privacy does not take into account either the complex dimensions of this issue or the need for an industry-government partnership on privacy. The Commission purports to recognize the important role that industry leadership on self-regulation plays in any privacy solution; yet the report recommends broad legislation that would provide "flexibility to the implementing agency in promulgating its rules or regulations . . . [that could] define . . . fair information practices with greater specificity." Such expansive regulatory authority could actually discourage industry-led initiatives and market-driven solutions by outlawing consumer-oriented methods of privacy protection and personalization. Furthermore, such sweeping legislation would not take into account all of the more targeted proposals that have either been enacted or are pending—from the new children's privacy law, to rules for health and medical data, to financial privacy regulations.

We at AOL would therefore ask the Members of this Committee to develop its policies in the privacy area with high regard for the benefits of personalization and the efficacy of industry action to date. You may find that there are gaps in industry enforcement where government must step in to ensure compliance. Nevertheless, it is clear that companies are responding to the increasing marketplace demand for online privacy, and that the tremendous growth of e-commerce reflects positive trends on a variety of consumer protection issues, including privacy. Sweeping regulatory action could very likely curb such market innovation and competition and discourage creative and flexible approaches to privacy protection.

The challenges that lie ahead will give us the chance to prove that industry and government can work together to promote online privacy. But ultimately, it is the consumer who will be the judge of whether these efforts are adequate. Because no matter how extraordinary the opportunities for electronic commerce may be, the marketplace will fail if we cannot meet consumers' demands for privacy protection and gain their trust.

We at AOL are committed to doing our part to protecting personal privacy online. Our customers demand it, and our business requires it—but most importantly, the growth and success of the online medium depend on it. We appreciate the opportunity to discuss these important issues before the Committee, and look forward to continuing to work with you on other matters relating to the Internet and electronic commerce.

The CHAIRMAN. Ms. Varney, welcome.

STATEMENT OF CHRISTINE VARNEY, SENIOR PARTNER, HOGAN AND HARTSON, ON BEHALF OF THE ONLINE PRIVACY ALLIANCE

Ms. VARNEY. Thank you, Chairman. It is a pleasure to be here. Thank you for inviting me. Mindful of your admonition, I am just going to talk for a few minutes. I have got longer remarks that we have submitted for the record and I would like to address some of the issues that have been raised this morning.

First of all, we can sit here all day and argue about numbers—88 percent, 60 percent, 40 percent, back out access, back out security, whatever. I think that it is fairly clear that there has been enormous progress. If you look over time, the increase in the numbers of Web sites that are making some type of privacy disclosures, providing some types of choices, is going up. I think that is something that this Congress can take a lot of credit for because they have shown a lot of leadership in working with the industry on it.

The complexity that we get to, that Commissioner Anthony and others have mentioned, when you read these notice policies should not be underestimated. Both Yahoo and Doubleclick have very large, very complex businesses and, Chairman, both those companies have been working very hard in the last month to completely revamp their privacy policies and make them easier to use, easier to read, and both those companies would like to come and talk to you, perhaps next week if you have time, to show you what they are planning on doing and get your feedback and your thoughts about it.

The CHAIRMAN. I would be glad to do that.

Ms. VARNEY. Thank you.

If privacy policies, if notices are misleading, I think as Ms. Lesser said, the FTC has the authority. Maybe what they need is more resources. They ought to prosecute those people. To put a statement up that says we protect your privacy policy and somewhere in the statement say we do whatever we deem reasonable with your data and you do not get any choice about it, I think is deceptive on its face and it ought to be prosecuted.

Senator Kerry talked a lot——

The CHAIRMAN. Yahoo? Yahoo ought to be prosecuted?

Ms. VARNEY. Well, Yahoo's is not deceptive, Senator. Yahoo's is complex. Yahoo is a very large company with an enormous Web site offering a wide array of services and products. When I read Yahoo's privacy policy, what I think they tried to do was be completely comprehensive, tell you everything. And it is not easy to read, they will agree with you.

The CHAIRMAN. Why do you have to be comprehensive? Can you not just say, this information will be private? What is the comprehensiveness?

Ms. VARNEY. You may absolutely say, we will never disclose this information to anyone under any circumstances, if that is what you do. When you run a Web site where you have content provider partners, where you have chat rooms that you link to that are run by other companies, where you have ask-a-doctor questions, where you e-mail a doctor who does not work for a company but works for somebody else, that information is in fact going to someone else.

It might be clear to you, it might not be clear to you. But to say we never give your information to anyone under any circumstances is flat out deceptive, unless that is precisely what you do. I would submit to you, Senator, unless you are dealing with a very small Web site, that is not the case today.

These Web sites, why are they so complex and comprehensive——

The CHAIRMAN. So we need a how many sentence——

Ms. VARNEY. I think that what you see——

The CHAIRMAN. Ms. Varney, that is not appropriate. It is not appropriate for most Americans not to be able to understand a Web site's privacy policy.

Ms. VARNEY. I agree, I agree.

The CHAIRMAN. Now, can you understand the Yahoo statement?

Ms. VARNEY. I do not think that is a fair test, Senator.

The CHAIRMAN. Well, we just had a university professor who could not.

Ms. VARNEY. I will leave that one.

I think that you are right, it is too complicated, and the companies are really working on how to make it less complex. Why is it so complicated? Because they are big companies with lots of business units. They are publicly traded companies that face shareholder lawsuits if they are not completely accurate in every regard. That is not to say that they cannot do it better and that they should not and that they will. I think they all will, which goes to my next point.

The CHAIRMAN. I apologize for interrupting you, by the way.

Ms. VARNEY. Not at all. Always better to have an exchange, I think, a dialog than a monologue.

What you have seen, what you have identified here this morning, I think is a real problem in making these notices easy to find, read, and understand. How do you do that? That is a problem we ought to address and perhaps ultimately it may need to be addressed legislatively.

Do you need to delegate what I consider to be broad, sweeping regulatory authority to the FTC to do that? No. This Congress has not delegated to any Federal agency broad regulatory authority over the Internet and I do not think this is the time to start.

Senator Kerry mentioned the financial data, data related to health and medical information, data related to kid-sensitive data. That may need a more complex regulatory scheme. In fact, as Ms. Lesser said, you passed the Financial Services Modernization Act. Now, we can argue about whether or not the privacy protections in that are adequate, but you passed it and it is just now going into effect.

You passed the Health Insurance Portability and Accountability Act. Those regulations dealing with privacy are not even done yet. We need to look at them. We need to figure out if there is loopholes. We have to give Americans the highest level of protection for their health and medical data.

The kids law, the Children's Online Privacy Protection Act, which this Committee birthed, has been wildly successful in my view, but it has had some unintended consequences, maybe not bad but unintended. Let us take a look and see where the gaps are.

The question I think is, whether it is 80 percent or 90 percent or 60 percent, how do you get this last mile to get every Web site that is collecting personal information to tell consumers in a straightforward way what they are doing and what their choices are? I do not believe the answer is delegating broad regulatory authority to the Federal Trade Commission at this time.

Thank you, Senator.

[The prepared statement of Ms. Varney follows:]

PREPARED STATEMENT OF CHRISTINE VARNEY, SENIOR PARTNER, HOGAN AND HARTSON, ON BEHALF OF THE ONLINE PRIVACY ALLIANCE

Mr. Chairman:

Thank you very much for inviting me to testify this afternoon on behalf of the Online Privacy Alliance. My name is Christine Varney. I am a former Federal Trade Commissioner and am currently a partner at Hogan & Hartson where I chair the Internet Practice Group. In addition, I am an advisor to the Online Privacy Alliance—a coalition of over 100 industry and trade associations who came together two years ago to formulate and advocate for best privacy practices online. With your permission I have submitted for the record extensive descriptions of privacy practices developed by the Online Privacy Alliance that can be used for future reference. I would like to take a few minutes here to discuss the FTC's report and the Commission's call for regulatory authority.

First, let me congratulate and thank the Commission for their ongoing work in examining the issues of privacy in the information age. It was not that long ago when I was a Commissioner in 1995 and I was told by some of my colleagues, none of whom are still at the FTC, that privacy was not a consumer protection issue. I think we have all come to realize that privacy is *the* consumer protection issue of the information age.

It is important to remember that the FTC's study is not and cannot be considered an evaluation of the state of privacy on the Internet. The FTC's analysis that only 20 percent of Web sites comply with all four fair information practices, and therefore, provide inadequate privacy is fundamentally flawed. As Commissioner Leary points out in his statement, the Commission's own Internet privacy policy does not meet the Commission's own test for an adequate privacy policy. In fact, in many many Web sites, both commercial and otherwise, some of the fair information practice elements, such as choice, security, or access, may not be at all relevant.

Let me give you a few examples as to when or why some of these criteria may not be relevant. If a site only uses your data *only* to complete a transaction, no choice is necessary. A site that does not disclose its security precautions doesn't mean they don't exist. Many experts testified in front of the Federal Trade Commission's Advisory Committee on Security and Access that security measures and precautions should not be disclosed on Web sites as it can lead to increased attempts at unauthorized access. Finally, the FTC's own Advisory Committee could not come to any agreement on what, if any, level of access is appropriate for non-sensitive data, under what circumstances, and at what costs.

While the FTC report does provide metrics, it clearly does not nor should it be interpreted as evaluating the state of privacy on the Internet. Thus, I entirely disagree with the conclusion that privacy in cyberspace is woefully inadequate and that legislation is necessary to empower the Federal Trade Commission to regulate data practices in e-commerce.

Two years ago, close to 10% of all Web sites posted some type of privacy policy or described their privacy practices in some way. Today that number is close to 90%. That is astonishing! Consumers are now better able than ever to determine whether a Web site's data practices match their own preferences. The ability of consumers to make meaningful privacy choices likewise doesn't guarantee privacy on the Net. We clearly need to do more work to make those choices clear and easy.

When asked "do you care about your privacy?" an overwhelming 90% of Americans will respond that yes, they do. But when you push down on those numbers, what you find out is that Americans care deeply about the abuse and misuse of their personal financial information, personal medical or health information, and information about their children. Additionally, Americans are very concerned about identity theft and credit card fraud on the Internet. In each of these arenas, Congress has either already acted or the FTC already has sufficient authority to enforce existing law. You have dealt with collection of data, from or about children in the Children's

Online Privacy Protection Act which went into effect just last month. Last year, you passed the Financial Services Modernization Act. While we may argue about the adequacy of the financial privacy protections in the Act, clearly the Congress has begun addressing financial privacy in that Bill and the FTC has, just last week, released its regulations implementing that Act. The regulations implementing the Health Insurance Portability and Accountability Act are still being drafted. These regulations clearly address health and medical privacy. Credit card fraud and identity theft are already illegal and should be prosecuted to the fullest extent.

Thus, I believe the FTC's conclusion that privacy on the Internet is inadequate is not supported by the facts in their report. That is not to say that we, industry and government, can't do a better job empowering consumers to protect privacy on the Internet. What is needed, I believe, is a commitment by government and industry to continue the work started several years ago to make privacy policies easy to find, read and understand. To make the promise of meaningful choice and control over personal data real—whether through technology solutions like P3P, software solutions like Privida and Privaseek, enforcement actions under existing law, or filing specific legal gaps. What we do not need are sweeping regulations governing the collection and use of data, the conditions and methods under which that data use can be consented to, the dimensions of access that must be provided to data and the level and design of web security. Rather, what I would suggest is that Congress continue its work with consumers and industry representatives in order to determine how best to reach the last 10 percent of Internet sites that do not disclose their data practices and perhaps begin consideration of a means to create a coherent and simple standard for privacy disclosures across all Internet sites. Congress has wisely refrained from delegating to any agency enormous regulatory authority over the Internet. When Congress has seen a problem, it has specifically addressed the problem. If there is any problem with privacy for non-sensitive data on the Internet, it is the lack of ubiquity in the posting of privacy policies and inconsistent and often complicated disclosure statements. Neither of these problems is successfully addressed through an enormous regulatory undertaking. Whatever solutions Congress, industry and consumers come to that will make privacy choices on the Internet ubiquitous, the solutions must be technology neutral, market driven, and hospitable to the online environment.

Those who sit before you and talked about self-regulation as a failure and legislation as the answer, or self-regulation as a panacea and legislation as repugnant, are in my view, clearly missing the point. The point in the information age has to be how can American consumers, whether they are consuming medical information, financial information, or other commercial information, protect themselves and their privacy desires. In some instances, there will be technological solutions. In some instances, there may be best practices, and in other instances, there may be loopholes in existing law that need to be closed or an absence of law altogether that must be filled.

Too often the privacy debate has been polarized between those who wish to prohibit the use of personal information for any and all purposes, and those who wish to exploit the use of personal information for any and all purposes. Neither of these postures addresses the increasing concerns of Americans regarding the protection of their personal privacy while allowing for its beneficial use. Neither of these polar positions realizes that there are benefits and limits to the use of personal information. Neither of these positions frankly can bring a balanced economically viable and societally appropriate conclusion to the privacy debate.

The CHAIRMAN. Thank you very much.

Mr. Catlett, for the benefit of the Committee perhaps you could tell us what Junkbusters is about.

STATEMENT OF JASON CATLETT, PRESIDENT AND CHIEF EXECUTIVE OFFICER, JUNKBUSTERS CORPORATION, AND VISITING SCHOLAR, COLUMBIA UNIVERSITY DEPARTMENT OF COMPUTER SCIENCE

Mr. CATLETT. I would be pleased to, Senator. Junkbusters is a Web site where people go for information about how to stop junk communications, such as junk e-mail, junk telemarketing calls, junk faxes, unwanted junk mail, and so forth.

The CHAIRMAN. It sounds to me like you are doing the Lord's work, Mr. Catlett.

[Laughter.]

Mr. CATLETT. Thank you, sir.

Senattor BURNS. Maybe we do not have to pass the spamming bill then?

Mr. CATLETT. I strongly recommend that you do pass something like H.R. 3113 without the provision of labeling. I think that is very much needed.

There are those who say that technological solutions for, for example, filtering out junk e-mail will suffice. But I can tell you, after running this Web site for 4 years and publishing software to help people protect their privacy, publishing information about how to remove cookies, how to stop junk phone calls and so forth, I can tell you that technology is not going to stop the death of privacy in this country.

Furthermore, self-regulation is also not alone or with technology going to stop the erosion of privacy. It is necessary to have laws that give individuals the right to protect their own interests.

The CHAIRMAN. You do not believe that the FTC has existing authority?

Mr. CATLETT. I do not believe they have sufficient authority to require sites to, for example, stop selling your telephone number to telemarketers when you tell them if the site's policy is stated as they will do that or they do not state that. There is nothing you can do, and we get e-mail at Junkbusters from harassed mothers in West Virginia who say, how can I get these telemarketers to stop calling me?

Mere notice is not enough. The doctrine that all actions can be taken on the basis of fraud is simply mistaken, I think.

There has been a lot of discussion about online and offline worlds and I would like to relate a little experience when I used to work at AT&T Bell Labs. I came here in 1992 to work on research on marketing and data bases. That work was governed by very strict laws about what could be done with people's phone call records. Suppose that Congress had not passed those laws to protect the privacy of people when they use the phone system.

Well, we would have a situation similar to what we have today on the Internet, where we are reading headlines about the terrible things that phone companies are doing. Instead of Doubleclick, it would be some company—I will fictionally call it Orwell Long Distance—that is spying on the phone customers.

For example, it might have speech recognition technology that listens to the key words that you speak in your phone conversations with business and uses them to target more interesting telemarketing calls to you. It might analyze the telephone numbers that you call, look them up in the Yellow Pages categories, and see what kind of categories of products you are interested in, and sell that information to cataloguers.

Now, if they did that people would be outraged and it would be simply illegal. But analogous practices on the web are prevalent from companies such as Doubleclick.

The Federal Trade Commission's report has been criticized by some people as understating the amount of progress that has been

made. But if you look at the analysis of, say, Forrester Research, an independent industry analysis firm, they actually paint a much bleaker picture of the amount of privacy protection that has been provided by industry. Forrester called many of these policies a joke and said that they serve to protect the interests of the companies rather than consumers. The Electronic Privacy Information Center has also done a series of excellent reports that come to the same conclusion.

So to my mind the FTC's conclusion that legislation is necessary is absolutely unassailable. We need legislation. What kind of legislation is needed? Well, the Online Privacy Alliance's four principles are not sufficient. Merely having notice, offering choice, some sort of weak access, and some sort of security is not enough. What is needed is in many cases to ask the consent of the person concerned before using his or her information.

That is one of the great principles of the bill before you, the Consumer Privacy Protection Act. It furthermore establishes, would establish, standing institutions that look to the privacy issue beyond the trade issue. Most importantly, it gives individuals a private right of action so that they can defend their own interests when their privacy is violated.

My own major criticism of the bill is that it preempts State law. I think it is entirely proper to allow the States their traditional role of laboratories of legislative innovation.

Privacy is a fundamental human right and Congress with this bill now has the opportunity to head off the demise of that right. It is really clear to me that, looking at the U.S. as someone who was not born here, that the world looks to the U.S. as a Nation that deeply respects human rights and individual liberties, and the citizens of this country do not have enough rights to defend their own privacy in cyberspace.

So I think that you all bear a great responsibility for determining whether the United States' leadership will extend into cyberspace and whether American citizens' rights will be preserved into the twenty first century.

Thank you.

[The prepared statement of Mr. Catlett follows:]

PREPARED STATEMENT OF JASON CATLETT, PRESIDENT AND CHIEF EXECUTIVE OFFICER, JUNKBUSTERS CORPORATION, AND VISITING SCHOLAR, COLUMBIA UNIVERSITY DEPARTMENT OF COMPUTER SCIENCE

My name is Jason Catlett, and I am President and CEO of Junkbusters Corp., a for-profit dot com company working to promote privacy. I'm very grateful to the Senate for this opportunity to discuss with you how to protect privacy in the Internet age.

I came to this country from Australia eight years ago to join the computer science research staff at AT&T Bell Laboratories. Since I founded Junkbusters in 1996, the company has published advanced software and provided services and information to help people defend their own privacy. These resources have been used by hundreds of thousands of Americans. Based on feedback from people across this country, and my own investigations, I have been led to the conclusion that technical solutions to the challenges of privacy will not prevent the death of American privacy online. It is clear to me that legislation is appropriate and necessary to protect privacy on the Internet.

My work in marketing and databases at AT&T Bell Labs was governed by strict laws to protect the privacy of telephone subscribers. The Internet still has few cor-

responding laws, so companies are engaging in practices that would be regarded as unacceptable and illegal on a phone network.

Collectively, this commercial surveillance is having the tragically perverse consequence of scaring off consumers from the entire medium rather than attracting them to a particular site. The Harris/Business Week polls and many others since 1998 have found that fear for privacy is a major or primary reason consumers give for not going online, and for not participating in e-commerce. Their 2000 poll showed a strong majority of Americans favoring new privacy legislation. Forrester Research, a highly regarded firm of technology analysts whose reputation has been built by providing accurate research and advice to companies, has harshly criticized the poor standards of privacy protection online, finding in September 1999 that 90 percent of Web sites fail to comply with basic privacy principles. Forrester called most privacy policies "a joke" and concluded that "the vast majority of such policies, like those of the Gap, Macy's and JC Penney, use vague terms and legalese that serve to protect companies and not individuals." These are not the words of some bleeding heart privacy advocate, but of hard-nosed analysts working for a company whose long-term success heavily depends on understanding and promoting the growth of Internet commerce. In October 1999 Forrester published a report finding that "Nearly 90% of online consumers want the right to control how their personal information is used after it is collected. This desire for online anonymity cuts across consumers from a broad range of demographic backgrounds, including gender, income, and age. Surprisingly, these concerns change very little as consumers spend more time online." It is not ignorance that is causing Americans to worry. It is a rational assessment of the lack of control over their personal information, and the paucity of recourse available to them if it is misused.

This privacy problem will not go away by itself because the economic incentives of individual companies work against it. As an example, providing customers with an opt-out from a list of phone numbers being sold to telemarketers means both forgoing future revenue and incurring a capital cost to set up an opt-out system. Companies can ill afford to unilaterally jump ahead of their competitors, even though the sums of money are minor compared to the increase in participation that would result from a market where privacy rights are widely respected. The idea that consumer demand will force companies to offer privacy protections is naive and simply not supported by empirical evidence in surveys. What company is going to produce advertising copy like the following? "Buy books from us and we will give you a choice in whether we sell your phone number to telemarketers." As Commissioner Anthony wisely observed in a statement Monday, legislation of the kind recommended by the FTC "would reward those sites that have offered real privacy protections and require all others to meet basic privacy standard."

We are facing a tremendous loss of both economic opportunity, and of our fundamental human right to privacy. The only way to stop this tragedy is to require all companies to respect the privacy of their customers and prospects. And that is an entirely proper thing for the federal government to do.

On the Internet this loss is particularly acute, but is obscured by technical complexity. Let me describe one example by analogy.

Online advertisers build up profiles based on where people go, what they look for, and how they behave on the Net. Imagine if Congress had not passed laws to protect the privacy of telephone users. The headlines would be full of the kind of privacy horror stories we see today about the Internet. We might see a telco that I will fictionally name Orwell Long Distance using speech-recognition technology to spot keywords in your conversations with businesses in order to target you with more interesting telemarketing calls. OLD might look up the yellow pages categories of the numbers you frequently call, and sell that information to junk mailers to decide the kinds of catalogs you're less likely to throw away. This sounds absurd to us now, but on the Web, equivalent practices abound, unrestrained.

Banner ad companies get to see the specific Web pages people visit, plus the keywords they type into search engines and other forms. They track individual PCs using unique identifiers called "cookies" placed on Web browsers. Most people haven't heard these companies' names, but some of them have started identifying people by name. Large profiles that were previously gathered with just an anonymous identifier are being linked to a street address, and phone number, and e-mail address.

If Orwell Long Distance were unencumbered by present phone privacy laws, its lobbyists would be telling Congress that any attempt to restrict the free flow of information on the international phone system would be futile, and could result in the collapse of toll-free ordering. But you would wisely dismiss that claim and judge that the greater economic good requires that people have confidence that their privacy is protected by law when they do business by phone.

It would be silly to expect consumers to defend themselves from Orwell Long Distance by using their own voice scramblers and payphones, or indeed technology from OLD itself. Suppose OLD designed a device that could be held up as a technological solution to the privacy concerns of phone subscribers. The result might be rather like a caller ID box, but in addition to displaying to the name and number of the calling party, it would indicate the degree of privacy being offered by the various carriers involved in the call. The called party would then supposedly be given "choice" on whether to pick up and speak to her mother for example, or have her call automatically rejected because it doesn't meet her daughter's privacy "preferences." This scheme would not protect privacy on the phone, and its Internet equivalent, P3P, will not protect privacy online.

What people need are simple, predictable standards, not more complexity, just as businesses need simple predictable copyrights. Both privacy and copyright law accommodate more complex arrangements whenever needed, with the consent of the parties involved.

The comparison with copyright is useful in dismissing many commonly-heard objections to privacy legislation. "We mustn't impede the free flow of information, so privacy/copyright laws are bad." On the contrary, such laws promote participation in the information economy, by protecting the rights of the participants. "The Internet is international, so privacy/copyright laws are useless." On the contrary, that is no reason to permit domestic abuses, and international treaties can be developed. "Technology changes quickly, so copyright/privacy laws are useless." On the contrary, such laws should be technology-independent; it is the data that needs protecting, not the means of transmission. "It's impossible to enforce copyright/privacy laws completely, so we shouldn't have them." Of course incidental violations will occur, but organizations will not base their businesses on piracy/privacy violation, or at least not for long.

Finally, imagine if Recording Industry Association of America were assessing the results of a fictional survey by the Department of Commerce showing that more than 80% of U.S. households do not infringe music copyrights, and concluding that copyright law should therefore be repealed. Preposterous, the RIAA would say. Even 95% of households respecting copyright would still leave 5% free to infringe copyrights. We must have a law. Won't new technology for preventing the unauthorized duplication of CDs provide the answer, a lobbyist against one-size-fits-all legislation might ask? No, the RIAA would say. We need a law, and we need substantial criminal and civil penalties. The Digital Millennium Copyright Act of 1998 was Congress's response to this issue.

In general, information technology produces many more opportunities for enabling undesired uses of information than it does for preventing it. As someone who has personally designed, coded, documented and published privacy-enhancing software, I would be the last to try to impede such technologies. The argument by some lobbyists that legislation would dampen technological innovation to protect privacy is specious. On the contrary, legislation would give companies an incentive to adopt technologies that promote privacy. Services for assuring anonymity become more valuable in a world where data protection is required, because anonymity is an infallible way of obviating the misuse of personal information.

The Report and Recommendation of the Federal Trade Commission

The FTC's report has been criticized by some trade associations as understating the level of privacy protection being provided by major Internet sites. I believe exactly the opposite is the case. Three years of surveys by the Electronic Privacy Information Center plus Forrester's assessment in September provide far stronger evidence that the average site provides substandard privacy. As an illustration, take the issue of access by consumers to information collected about them. The Online Privacy Alliance's spokesperson Christine Varney said in a press release Tuesday that "There is no agreed-upon standard for access, so how can the FTC measure it?" They can't. The answer was on page 23 of the FTC's report: "With respect to Access, a site received credit if it offers the ability to review, correct, or delete at least one item of personal information it has collected—oftentimes simply an opportunity to update an e-mail address—without regard to what other information a site may have actually collected or compiled." Plainly the FTC can measure access, and they did. It is significant that the FTC were very easy graders, and yet most sites still failed. As to the consumer's view of access, a study in April 1999 by AT&T Laboratories asked respondents about "importance of whether the site will allow me to find out what info about me they keep in their databases." 57% replied saying it was very important, 27% somewhat important, 4.2% not important, with the rest not responding. The FTC's conclusion that legislation is needed to improve consumer confidence in a world where most sites are not providing sufficient privacy is simply

unassailable. What is remarkable is that the majority of Commissioners waited so long before recommending legislation.

The four privacy principles of the Online Privacy Alliance and the FTC (namely notice, choice, access and security) are necessary but not sufficient to adequately protect privacy. Orwell Long Distance, for example, would post a privacy policy (notice), offer an 800 number where people can opt out of surveillance (choice), let consumers fill out their own change-of-address forms (access), and deliver all its lists to telemarketers encrypted (security). Missing are affirmative consent and purpose specificity: not using information gathered for one purpose (to complete the phone call) for another purpose (to give to telemarketers) without gaining affirmative permission. These are among the principles endorsed the OECD in 1980 and used as the basis of privacy laws in most developed countries, including recently Canada.

The Consumer Privacy Protection Act of 2000

The Consumer Privacy Protection Act from Senator Hollings and his colleagues is a landmark work, making giant strides towards the wide application of all these principles, across technologies and across market sectors, within a legal framework that will really protect privacy in this country.

The CPPA addresses the problem that privacy policies have become "moving targets" that are constantly subject to change. Requiring consent for material changes in use an important part of the principle of purpose specificity. In line with this goal, the requirement for notice might be waived when the policy change merely narrows the purposes to which information is put, rather than widening them.

The CPPA moves toward addressing the urgent need for standing institutions that consider privacy and security policy issues not merely in the context of commerce, but also of government, society and human rights.

Very importantly, the bill provides a private right of action, which is essential if people are to have the means to protect their own interests. Some, but not all enforcement power should vest in agencies such as the FTC. Experience with the Telephone Consumer Protection Act of 1991 dispels the scare mongering claim that a vast government bureaucracy would be needed to curtail privacy violations. The FTC has restricted its enforcement actions to cases of fraud (which are indeed widespread and severe in that industry). State Attorneys General occasionally take action. But it is the precious few individuals who file suit in small claims court that have done the most to discourage the telemarketing industry from routinely violating the law.

Finally, to allow further progress, federal laws should not preempt state law. A good federal law that allows state Attorneys General sufficient enforcement powers will reduce the need for new state-specific legislation, but the states should not be deprived of their traditional role as laboratories of legislative innovation.

Congress now has before it a comprehensive proposal to head off the demise of privacy in this country. It is time for each member of Congress to decide whether the right to privacy is worth defending, or whether it should be allowed to lapse into a 20th century memory.

Throughout this nation's history, the world has looked to the United States as a bastion of liberty, and to its elected governments as defenders of individual rights. Congress now bears a great responsibility for determining whether that leadership will extend into cyberspace, and whether the American citizen's right to privacy—a fundamental liberty—will endure into the 21st century.

I appreciate the opportunity to speak before you today. I would be pleased to answer your questions.

[A list of references is available at *http://www.junkbusters.com/testimony.html* on the Web.]

The CHAIRMAN. Thank you, Mr. Catlett.

Mr. Berman.

STATEMENT OF JERRY BERMAN, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. BERMAN. Thank you, Mr. Chairman and Members of the Committee. It is a privilege to be here.

My organization is a civil liberties organization, but also an Internet policy organization, and we are trying to maximize the democratic potential of the Internet to build a bill of rights in cyberspace. We have worked with all of you on different issues af-

fecting the Internet, whether it is objectionable content and indecency and how to protect the rights of adults versus how to protect our children, encryption, communications privacy, and here data privacy.

In every one of those areas we have recognized that the Internet is a different paradigm, it is global, it is decentralized, and that we need to focus in every one of those areas on empowering users and caretakers to protect their rights. That is the thrust of every model piece of legislation.

There is consensus between Senator Burns' effort with Senator Wyden a year ago, and the Boucher and Goodlatte effort that something needs to be done. All four chairs of the Internet Caucus who share that vision of the Internet are supporting privacy legislation.

It is very important to understand that none of that legislation is saying government takes over the Internet. All the thrust of that legislation is to empower users to protect their rights on the Internet. And users cannot protect their rights if they have a crazy quilt of notice and obfuscation on the net where they do not know what the information policies are of those nets, of those Web sites, and they cannot exercise the right to choose or opt-in or opt-out of particular practices, and there has to be flexibility in that area.

The legislation I see that has been introduced not only provides that baseline information, that information will not be provided by 100 percent of the sites until Congress acts, because everyone can be a publisher on the Internet. There are so many net sites that do not know that privacy is even an issue. It is not the last mile, as Christine Varney says, because if Yahoo does not know what notice is required and they may be suffering from a potential prosecution over their eight pages, what about the little Web site?

Is it not important for the government to set some standard so that people on the Internet, the Web sites and consumers, know where they are? That is the key part of this legislation.

You do not have to rely on the heavy hand of government, particularly in trying to figure out on the web what notice means. You can also rely on self-enforcement and some of the web, TrustE and BBBOnLine, they can become safe harbors under the legislation. But to move it from 8 percent takeup by the industry to 100 percent is going to require some push that they know that is a safe harbor, and only Congress can do that.

If Congress does not act in this area, you are facing 270 bills in the States, and we have recognized in many areas that a crazy quilt of State laws is counterproductive, a burden on the Internet, a burden on commerce, a burden on speech, and not in the interest of the Internet.

I think that the companies like AOL and IBM and Microsoft and others that we have worked with on their online privacy guidelines have done a terrific job and they have moved forward and they should be commended for it. But they cannot bear the burden and they do not have the resources or the time to drag the other Web sites along or to subsidize them or to pick them up. That is a role for government, and it is balancing and making their practices the best practices as part of legislation which will build legislation which maps onto the decentralized Internet and preserves and protects and enhances the values that we share.

Thank you.
[The prepared statement of Mr. Berman follows:]

PREPARED STATEMENT OF JERRY BERMAN, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. Chairman and members of the Committee, the Center for Democracy & Technology (CDT) is pleased to have this opportunity to speak to you about the important subject of privacy on the Internet. CDT is a non-profit, public interest organization that is dedicated to developing and implementing public policies to protect civil liberties and democratic values on the Internet. CDT has been at the forefront of efforts to establish and protect the very high level of constitutional protection that speech on the Internet has been afforded by the United States Supreme Court in the *Reno* v. *ACLU* [1] decision, and to develop sound public policies and technical solutions to protect individual privacy.

Mr. Chairman, the Internet is at a critical junction in its evolution. Although as a popular mass medium the Internet is less than ten years old, it is already entering into a period of significant transformations. Ensuring privacy on the Internet requires a multi-faceted approach that draws upon the strengths of technology, self-regulation, and legislation to deliver to the American public the ability to exercise control over their personal information.

I wish to emphasize four key points this morning:

- Privacy is not a partisan issue. Privacy is a deeply held American value. It is broadly supported by the American public and has frequently been the subject of bi-partisan legislative efforts.
- Privacy and the Internet are ill served by a crazy quilt of standards. Consistency is critical to consumers, businesses, and the character of the Internet. In an environment where everyone is a publisher and a business it is impossible to develop a consistent standard for privacy without legislation. While self-regulatory efforts, auditing, and self-enforcement schemes work for some businesses, on its own it will result in an inconsistent framework of privacy protection.
- Industry leaders should not ignore or carry bad actors or outliers, but rather participate in a system of self-regulation and legislation that ensures a level playing field and predictable standards. Industry leaders would be ill advised to ignore the cost to privacy of bad actors and newcomers. Bad actors will not self-regulate: the clueless or new on the scene may not have the resources or wherewithall to participate in regulating their own behavior. Law is critical to spreading the word and ensuring widespread compliance with fair, privacy protective standards. By building a system of self-regulation and legislation we can create a framework of privacy and instill consumer trust.
- Legislation can and should support self-regulation and technical developments. The tired debate over self-regulation versus legislation does not serve our mutual interest in privacy protection. It is our collective task to develop a legislative privacy proposal that fosters the best industry has to offer through self-enforcement and privacy enhancing tools. Realizing privacy on the Internet demands that we develop a cohesive framework that builds upon the best all three of these important tools offer.

I. Privacy

The critical starting point on the privacy questions is the current state of privacy (and citizens' expectations of privacy) and the ways in which the evolution of the Internet may threaten privacy principles.

CDT believes that a key privacy consideration should be individuals' long-held expectations of autonomy, fairness, and confidentiality, and policy efforts should ensure that those expectations are respected online as well as offline.[2] These expectations exist vis-à-vis both the public and the private sectors. By autonomy, we mean the individual's ability to browse, seek out information, and engage in a range of activities without being monitored and identified. Fairness requires policies that provide individuals with control over information that they provide to the govern-

---

[1] *American Civil Liberties Union* v. *Reno,* 929 F. Supp. 824, 844 (E.D. Pa. 1996), aff'd, *Reno* v. *American Civil Liberties Union,* 521 U.S. 844 (1997).

[2] For a fuller exploration of these issues see, e.g., Testimony of Deirdre Mulligan, Staff Counsel of the Center For Democracy & Technology, Before the Subcommittee on Communications of the Senate Committee on Commerce, Science, and Transportation, July 27, 1999.

ment and the private sector. In terms of confidentiality, we need to continue to ensure strong protection for e-mail and other electronic communications.

As it is evolving, the Internet poses both challenges and opportunities to protecting privacy. The Internet accelerates the trend toward increased information collection that is already evident in our offline world. The trail of transactional data left behind as individuals' use the Internet is a rich source of information about their habits of association, speech, and commerce. When aggregated, these digital fingerprints could reveal a great deal about an individual's life. The global flow of personal communications and information coupled with the Internet's distributed architecture presents challenges for the protection of privacy.

II. The Expectation of Fairness and Control Over Personal Information: What the FTC's Report Reveals

When individuals provide information to a doctor, a merchant, or a bank, they expect that those professionals/companies will collect only information necessary to perform the service and use it only for that purpose. The doctor will use it to tend to their health, the merchant will use it to process the bill and ship the product, and the bank will use it to manage their account—end of story. Unfortunately, current practices, both offline and online, foil this expectation of privacy. Much of the concern with privacy in electronic commerce stems from a lack of robust privacy rules in various sectors of the economy, such as financial and health, that handle a treasure trove of sensitive information on individuals. Whether it is medical information, or a record of a book purchased at the bookstore, or information left behind during a Web site visit, information is routinely collected without the individual's knowledge and used for a variety of other purposes without the individual's knowledge—let alone consent.

The online environment facilitates the collection of information about consumers that offline entities can only dream of. To paraphrase Chairman Pitofsky, "Not only do they know I ordered the steak, but they know I considered the salmon and how long it took me to make up my mind." Recent months have witnessed detail reports, investigations, and law suits about the surreptitious collection of personal information by businesses—some completely unknown and invisible to the consumer. From network advertisers to fraud detection systems, profiling Web site visitors is routine. Using a mix of "cookies," "web bugs," and other monitoring techniques consumers are routinely being watched, their activities assessed, and their experience of the Internet altered.

The FTC report released on Monday is the third study to assess the state of privacy on the World Wide Web. This year's report is by far the most comprehensive study of consumer privacy online. Not only did the FTC tally raw numbers, but also, finally, the FTC explored the important question of whether improved numbers equal improved privacy for consumers. The good news is that progress, in terms of sheer numbers, continues. The disappointing news is that the sum is less than the parts.

- **The head count is improving.**

The constant call by industry, the FTC, and consumers for privacy policies has been heeded. Today, consumers are more likely than not to find a privacy statement of some sort at Web sites. The number of sites sporting a "privacy policy"—a comprehensive description of a Web site's information practices that is located in one place—has risen from 2% in 1998 to 62% in 2000. Similarly, more Web sites are providing consumers with some information about how they use information (referred to as "information practice statement" or "privacy disclosure"). In 1998 only 14% of surveyed sites made any statement about their use of personal information. This year 79% of the surveyed sites posted at least one information practice statement. While progress was more modest in other areas, every area witnessed some improvement over previous years.

- **Notice, choice, access, and security remain the exception not the rule.**

While progress continues, the Web has not witnessed the widespread implementation of the Fair Information Practice principles of notice, choice, access, and security. (The principles are set forth in detail in Appendix A.) While the number of sites meeting this standard has doubled—from 10% in 1999 to 20% in 2000—the number represents a small portion of total Web sites. It is troubling to note that even at those sites that sport a privacy seal from a self-regulatory program adherence to these four fair information practices hovers at 52%. And of the sites surveyed, 8% participate in a seal program—leaving the critical area of self-regulatory enforcement unsettled.

- **A lack of clear rules has led to the proliferation of confusing privacy notices that are beyond the reading comprehension skills of the majority of the American public.**

This year the FTC delved into the difficult realm of substantive analysis of privacy policies. What they found mirrors CDT's experience—and based on reports and e-mail those of consumers as well. (Appendix B* includes several examples of Web site privacy policies that contain confusing and contradictory statements.) Privacy policies can be exceedingly difficult to decipher. Several articles have documented the difficulties faced by consumers seeking to understand the protections a Web site affords them by reading privacy policies.[3] As Chairman Pitofsky stated in a recent USATODAY.com story, "Some sites bury your rights in a long page of legal jargon so it's hard to find them and hard to understand them once you find them. Self-regulation that creates opt-out rights that cannot be found (or) understood is really not an acceptable form of consumer protection."[4]

While some sites may be actively attempting to confuse consumers—for example CDT identified several privacy policies that use common terms in a misleading fashion and others that contain contradictory statements. In general, we believe that Web sites are in the unenviable position of trying to assuage legitimate public concern with privacy and ensure their attorneys that in doing so they will not unintentionally create a liability disaster. The rock and the hard place that many Web sites find themselves in creates a tendency toward legalese, over and under disclosure, and hedging. When doing the right thing creates liability that those who sit still don't face, notices resemble legal disclaimers rather than vehicles for consumer education and empowerment.

Regardless of the intent, consumers interests are ill served by policies that are written in complex, vague language. Guidelines on the essential elements for inclusion in a notice would help both consumers and businesses. It would likely result in shorter more direct statements for consumers, and, for businesses, it would take some of the risk out of the process of writing a privacy policy notice.

- **Surreptitious data collection techniques continue to grow.**

Over the past twelve months privacy concerns surrounding the use of technology to track and profile individuals has taken center stage. From the joint FTC and Department of Commerce workshop on Online Profiling, to the massive online consumer protest of Doubleclick's withdrawn proposal to tie online profiles to individuals' offline identities, to the private lawsuits against Realnetworks, to State Attorneys' General actions against Doubleclick—it is clear that policy-makers and the public are concerned with the use of technology to undermine privacy expectations.

There is reason for concern. Third-party cookies, as the FTC Web sweep reports, are routinely found at commercial Web sites. In fact, consumers visiting 78% of the 100 most popular Web sites will be confronted with cookies from entities other than the Web site. While the growth of third-party cookies continues, less than 51% of the top 100 sites that set third-party cookies tell consumers about this practice.

Similarly, the use of "web bugs" or clear gifs—invisible tags that Internet marketing companies use to track the travels of Internet users—has grown exponentially over the past year. Richard Smith, a well-known computer security expert, in his presentation to the Congressional Privacy Caucus stated that in January 2000 approximately 2000 "web bugs" were in use on the Web (according to a search using Alta vista), but in just 5 months that number multiplied ten-fold to 27,000.[5] While the FTC did not look for "web bugs" or for statements about them, it is unlikely that Web sites are telling consumers about this new tracking device.

III. Bringing Privacy to the Internet

Privacy as discussed above is a complex concept. It encompasses our right to withhold information, our interest in maintaining confidences in information we willingly choose to disclose, as well as our right to walk—or surf—the streets without having every step captured, analyzed and tied to our identity forevermore. Protecting these three interests—autonomy, fairness, and confidentiality requires a

---

*Appendix B has been retained in the Committee files.

[3] See, Will Rodger, "Privacy isn't public knowledge: Online policies spread confusion with legal jargon," USATODAY.com, May 1, 2000 <http://www.usatoday.com/life/cyber/tech/cth818.htm>; The Industry Standard, March 13, 2000, at 208–9.

[4] Will Rodger, "Privacy isn't public knowledge: Online policies spread confusion with legal jargon," USATODAY.com, May 1, 2000. <http://www.usatoday.com/life/cyber/tech/cth818.htm>

[5] Richard M. Smith, Statement at the Congressional Privacy Caucus briefing, May 18, 2000. See, *http://www.tiac.net/users/smith* for additional information on "web bugs" and other privacy and security issues.

wise use of resources in the public and private sector. Of utmost importance it demands that we empower individuals with the information, tools, and protections necessary to exercise meaningful control over their personal information. To deliver privacy we must build a program of self-regulation and legislation, and support the widespread deployment of privacy enhancing technology.

A. Enforceable Fair Information Practices are Essential in the Online Marketplace

The Federal Trade Commission's latest report confirmed what advocates, industry representatives and the public knew: privacy on the Internet is far from a reality. The Federal Trade Commission's five year focus on privacy has raised the level of attention and concern, but has not delivered anything close to comprehensive compliance by businesses operating online. Despite commendable efforts such as BBB Online and TrustE, judged by the full set of agreed upon privacy principles the overwhelming majority of Web sites have not delivered privacy to the marketplace.

Numerous surveys have documented the public's overwhelming concern with privacy online. Many responsible industry actors are engaged in efforts to craft privacy rules; unfortunately many other companies have yet to take the actions necessary to protect privacy. We have the opportunity to develop privacy rules that establish strong protections for individuals, a fair baseline for a competitive marketplace, and a framework of trust for electronic commerce. Embedding these rules in federal legislation will not be easy, but it can, and ultimately must, be done.

If Congress fails to act on the FTC's recommendation, there is no doubt that the states will fill the gap. At last count over 200 privacy bills were introduced at the state level. While many do not directly deal with online privacy, several do. The states have become increasingly active in protecting consumer privacy and if left with a vacuum it is likely that they will step in. A strong federal law is in the interest of consumers, industry and the Internet. If the rules provide strong protections for privacy, consumers and businesses would both benefit from the certainty that a federal approach affords. In addition, the borderless nature of communication and commerce on the Internet is best approached with common rules. A patchwork of inconsistent and conflicting standards could increase consumer confusion, burden businesses, and interfere with the relatively seamless operation of the Internet.

B. Delivering on Technology's Promise: Ubiquitously Available, Tools that Empower Consumers to Make Real-Time, Flexible Decisions About Their Personal Information.

1. Technology is critical to consumer privacy on the Internet.

The specifications, standards, and technical protocols that support the operation of the Internet offer a new way to implement policy decisions. By building privacy into the architecture of the Internet, we have the opportunity to advance public policies in a manner that scales with the global and decentralized character of the network. As Larry Lessig repeatedly reminds us, "(computer) code is law."

Accordingly, we must promote specifications, standards and products that protect privacy. A privacy-enhancing architecture must incorporate, in its design and function, individuals' expectations of privacy. For example, a privacy-protective architecture would provide individuals the ability to "walk" through the digital world, browse, and even purchase without disclosing information about their identity, thereby preserving their autonomy and ensuring the expectations of privacy. A privacy-protective architecture would enable individuals to control when, how, and to whom personal information is revealed. It would also provide individuals with the ability to exercise control over how information once disclosed is subsequently used. Finally, a privacy-protective Internet architecture would provide individuals with assurance that communications and data will be technically protected from prying eyes.

While there is much work to be done in designing a privacy-enhancing architecture, some substantial steps toward privacy protection have occurred. Positive steps to leverage the power of technology to protect privacy can be witnessed in tools like the Anonymizer, Crowds, and Onion Routing, which shield individuals' identity during online interactions, and encryption tools such as Pretty Good Privacy that allow individuals to protect their private communications during transit.

The World Wide Web Consortium's Platform for Privacy Preferences ("P3P") is also a promising development. The P3P specification will allow individuals to query Web sites for their policies on handling personal information and to allow Web sites to easily respond. While P3P does not drive the specific practices, it is a standard designed to promote openness about information practices, to encourage Web sites to post privacy policies, and to provide individuals with a simple, automated method to make informed decisions. Through settings on their Web browsers, or through

other software programs, users will be able to exercise greater control over the use of their personal information.

An important milestone is June 21. On that day, major Internet companies will offer the first public demonstration of a new generation of Web-browsing software based on P3P, designed to give users more control over their personal information online. We are hopeful that P3P products will provide consumers with increased control over their personal information. Technologies must be a central part of our privacy protection framework, for they can provide protection across the global and decentralized Internet where law or self-regulation alone may prove insufficient.

2. Tools must reflect the diversity of consumers' privacy needs.

Privacy is not the same as secrecy. Tools must support individuals' needs to shield their identity, reveal certain information to a limited set of entities, ensure information is not compromised in transit, and protect information stored on their own computer. While tools are coming to market that reflect consumers' varied needs for privacy, there is much work to be done.

The Internet Engineering Task Force (IETF) is undertaking a critical privacy effort. IETF is working on two standards that would create new guidelines for the appropriate use of cookies. While cookies are helpful for Web sites looking to maintain relationships with visitors, they have been implemented in ways that give users very little control and have been used by some to subvert consumers' privacy. On most browsers, users are given only the option to either accept or reject all cookies or to be repeatedly bombarded with messages asking if it is OK to place a cookie.

The IETF is considering two complementary "Internet drafts" that would encourage software makers to design cookies in ways that give users more control. These drafts lay out guidelines for the use of cookies, suggesting that programmers should make sure that:

- the user is aware that a cookies is being maintained and consents to it,
- the user has the ability to delete cookies associated with a Web visit at any time,
- the information obtained through the cookie about the user is not disclosed to other parties without the user's explicit consent, and
- cookie information itself cannot contain sensitive information and cannot be used to obtain sensitive information that is not otherwise available to an eavesdropper.

The drafts say that cookies should not be used to leak information to third parties nor as a means of authentication. Both are common practices today. The IETF is expected to make its decision to move forward with these, and perhaps other cookie specifications, before the end of the summer and will invite public comments at that time.[6]

The recent report of the Federal Trade Commission's Advisory Committee on Online Access and Security recommended that steps be taken to improve security. The Committee's report highlighted the need for Internet businesses to develop robust security practices that protect data from both internal and external threats and protect customer data during both transit and storage. Specifically the Advisory Committee recommended that:

- Each commercial Web site should maintain a security program that applies to personal data it holds.
- The elements of the security program should be specified (e.g., risk assessment, planning and implementation, internal reviews, training, reassessment).
- The security program should be appropriate to the circumstances. This standard, which must be defined case by case, is sufficiently flexible to take into account changing security needs over time as well as the particular circumstances of the Web site—including the risks it faces, the costs of protection, and the data it must protect.

It is critically important that standard setting bodies support the development of privacy enhancing technologies and robust security standards. It is equally important that businesses bring these important developments to the mainstream market in products that are accessible and user-friendly for individual consumers and the myriad of small shop-keepers establishing Web sites.

---

[6]The draft can be found at: http://www.ietf.org/internet-drafts/draft-iesg-http-cookies-03.txt and http://www.ietf.org/internet-drafts/draft-ietf-http-state-man-mec-12.txt.

3. Tools must be widely available and easy to use.

In the area of child protection, industry and the public interest community have collaborated on efforts to bring tools and information to consumers through common resources, educational campaigns and other efforts. Similarly, privacy enhancing tools must be widely deployed if they are to truly benefit all consumers. While experienced Internet users may avail themselves of today's tools, it is unlikely that newcomers can find them, let alone use them effectively. As privacy enhancing technologies come to market ensuring their wide-spread availability and use should be a priority.

IV. Conclusion: Protecting Privacy on the Internet Requires a Multi-pronged Approach that Involves Self-regulation, Technology, and Legislation.

On self-regulation, we must continue to press the Internet industry to adopt privacy policies and practices, such as notice, consent mechanisms, and auditing and self-enforcement infrastructures. We must realize that the Internet is global and decentralized, and thus relying on legislation and governmental oversight alone simply will not assure privacy. Because of extensive public concern about privacy on the Internet, the Internet is acting as a driver for self-regulation, both online and offline. Businesses are revising and adopting company-wide practices when writing a privacy policy for the Internet. Efforts that continue this greater internal focus on privacy must be encouraged.

On the technology front, while the Internet presents new threats to privacy, the move to the Internet also presents new opportunities for enhancing privacy. Just as the Internet has given individuals greater ability to speak and publish, it also has the potential to give individuals greater control over their personal information. We must continue to promote the development of privacy-enhancing and empowering technology, such as the World Wide Web Consortium's Platform for Privacy Preferences ("P3P"), which will enable individuals to more easily read privacy policies of companies on the Web, and could help to facilitate choice and consent negotiations between individuals and Web operators.

On the public policy front, we must adopt legislation that incorporates into law Fair Information Practices—long-accepted principles specifying that individuals should be able to "determine for themselves when, how, and to what extent information about them is shared." [7] Legislation is necessary to guarantee a baseline of privacy on the Internet, but it is not one-size-fits-all legislation. Congress must do more to protect privacy in key sectors such as privacy of medical records. For consumer privacy on the Internet—and we believe more broadly—there needs to be baseline standards and fair information practices to augment the self-regulatory efforts of leading Internet companies, and to address the problems of bad actors and uninformed companies. We also stress that legislation is needed to raise the standards for government access to citizens' personal information increasingly stored across the Internet, ensuring that the 4th Amendment continues to protect Americans in the digital age.[8]

Several proposals are circulating in Congress today. Members of this Committee have introduced two important bills: Senator Hollings "Consumer Privacy Protection Act" (S. 2606); and, Senators Burns and Wyden "Online Privacy Protection Act" (S. 809). We believe that the outlines of sound privacy protection for the online environment have taken shape and look forward to working with this Committee on these efforts.

The history of the Internet is that policy regimes are first created by consensus among a broad cross section of the community. CDT is committed to participating in any process that helps to build a new social contract embodying democratic values in the emerging online world. The work of the Federal Trade Commission—through its public workshops, hearings, and its recent Advisory Committee on Online Access and Security—provides a model of how to vet issues and move toward consensus. We look forward to working with this Committee, as well as others, the industry and the public interest community to build a cohesive system of privacy protections for the online environment. Thank you for the opportunity to participate in this timely hearing.

---

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

[8] See, Testimony of Deirdre Mulligan, Staff Counsel of the Center for Democracy & Technology, before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary, March 26, 1998, at 11–13 (concerning disclosure of subscriber information to the U.S. Navy).

Appendix A

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The CHAIRMAN. Thank you, Mr. Berman.

Mr. WEITZNER. Is that the proper pronunciation?

STATEMENT OF DANIEL J. WEITZNER, TECHNOLOGY AND SOCIETY DOMAIN LEADER, WORLD WIDE WEB CONSORTIUM

Mr. WEITZNER. That is exactly correct.

The CHAIRMAN. Welcome, Mr. Weitzner.

Mr. WEITZNER. Thank you, Chairman McCain. It is an honor to be here and I am very pleased to be part of this discussion.

My testimony, which I have submitted and I will not read all of, makes three very basic points. First, and I think based on the discussion we do not even have go to through this any further, the increasing sophistication of web technology enables the collection of large volumes of personal information, both directly from users and in the background in some way or another. Some characterize it as surreptitious, others characterize it as convenient. But there is an increasing volume of information collected.

Second, the World Wide Web Consortium, the organization I work for, which is the group that sets technical standards for the web and includes over 420 members from industry, academia, research, consumer organizations all around the world, recognized the increasing consumer concern over privacy and we therefore launched a project called P3P, the Platform for Privacy Preferences, which will enable the marketplace to deliver software tools and services that enhance users' knowledge of Web sites' information practices and give users more control over their personal information.

Finally, I hope that we can dispense with the false dichotomies, the false choices, presented between law, regulation, technology, industry practices, or self-regulation. I think it should be clear to us that some balance of all of those factors is needed. No one of those is going to solve the problem—not law, not self-regulation, not technology. So we do not need to worry about any one of them being sufficient. I think we should all just stipulate that we need to find the right combination.

I am going to——

The CHAIRMAN. You are saying right combination of legislation and regulation? Is that what you are saying?

Mr. WEITZNER. Well, I suppose that is a further distinction that I would probably leave to you. I think we need some kind of legal baseline. Whether that is implemented solely in statute or through regulation is something I would leave to you. But I think we need a legal framework in which to operate here along with technology tools and responsible industry practices.

Let me dispense with the discussion of all the myriad ways that information, personal information, can be collected online because I think there is a general appreciation for that point, and I want to talk directly about W3C's efforts to build technology tools that will help enhance users' privacy experiences and particularly, given all the discussion we have had, we have heard already, about the complexity of privacy policies, the difficulty of finding them, the number of words that one has to get through to get to the bottom line of the policy, let me talk in a little bit more detail about W3C's Platform for Privacy Preferences.

Through this project, which is really a project to develop technical standards that address privacy, we hope to enable the development of a variety of tools and services, produced by the market-

place, that give users greater control over personal information and thereby enhance trust between web services and individual users.

P3P enables services, whether they are in web browsers, in web servers, in other pieces of software or services that users come across, that will enhance user control by putting privacy policies where users can find them, by presenting the policies in a form that users can understand, and, most importantly, by enabling users to act on the policies that they see more quickly.

For e-commerce services there are benefits as well. P3P can be used to make the browsing experience more seamless. Any web designer who is concerned about offering a product or a service to someone who visits their site has a difficult balancing task, even if they want to provide the maximum information about their privacy policy to that user. It is not easy to present, and I think it is a fair point that it is sometimes complicated to articulate in prose, especially prose readable to the non-experts out there, exactly what information practices sites are engaged in, and I think it is quite fair to say that, whether it is Yahoo or any of the other really sophisticated, exciting services, they do a lot of different things with your personal information in a lot of different places, and to try to catalogue all that in one single place is bound to be complex.

So with P3P what we have tried to do is to enable the association of particular web pages and privacy policies that apply to what is going on at that point on the web, so that when you are asked to fill out a form right there your browser will be able to tell you, not necessarily in prose terms but with graphical icons or some other means, exactly what is going to happen there when you submit that form data.

Think if you will for a minute about the experience we have had with security on the web. Several have referred to the fact that there was great concern about providing credit card numbers on the web by a number of users. How was that concern alleviated? In some part it was alleviated by, I think, a very broad education campaign. In some part, though, it was alleviated because browsers added tools that told users that their transaction was secure.

No one on this Committee may know the acronym SSL. That is the technology that secures the communication between a user and a Web site. But I think vast numbers of people who use the web recognize the little lock or the little key icons and know when that lock or that key is closed they should feel comfortable putting their credit card number onto that page.

We are looking to do the same kind of thing for privacy, to be able to represent to users exactly what is going on at exactly the point in the Web site they are at, rather than forcing them to go back and read through the Web site and click through. I was amused at the description of the number of clicks. I have never actually counted them, and the number of words, but I think that is exactly the problem that we are trying to address with P3P.

Finally, P3P can help to assist with three of the four information practices that the FTC report has outlined. Obviously, notice; it provides a capable for presenting easy-to-understand notice to users. It helps users to make a choice.

Finally, it tells—it has the vocabulary to tell users exactly where they can go, what they have to do, to get access to their personal information. Security is dealt with in other parts of web standards, so we have not addressed it directly in P3P.

I would say that the question of access is complex and P3P does not pretend to provide a mechanism to enable access, but we do provide a way for users to understand how to go and get access.

I want to just close by saying that I think that this Committee does face very difficult questions regarding what legal or regulatory framework, if any, is best to address privacy on the web. There are obviously a variety of options before you and I am not here to support or oppose any particular approach. I would urge, though, that with or without legislation, with or without regulation, web users both in the United States and around the world need more powerful technical tools to give them greater control over their online privacy relationships and greater information about what kinds of relationships they enter into.

Even with the most stringent privacy laws in place, I would submit, so much of individual users' practical privacy rights on a day to day basis depends on being able to make individualized choices about what they want done with their personal information in a particular interaction. The web is getting so complex that we are going to need technology tools to help with that.

We certainly also need some way or another to encourage and in some cases most likely require Web sites that offer those choices. But we are going to need the tools to make those choices effective choices and make sure that they are not buried four or five clicks and thousands of words down in some policy.

So I hope that, whatever action this Committee takes, it will be consistent with encouraging the development of these tools and unleashing the innovative forces in the marketplace which, whether or not they have an incentive to provide privacy regulation, privacy protection, the innovation that we see in this marketplace can help to solve these problems and we should make sure that it is able to do that.

Thank you very much.

[The prepared statement of Mr. Weitzner follows:]

PREPARED STATEMENT OF DANIEL J. WEITZNER, TECHNOLOGY AND SOCIETY DOMAIN LEADER, WORLD WIDE WEB CONSORTIUM

Introduction

Good Morning. My name is Daniel J. Weitzner. I thank the Committee for holding this hearing on online privacy and am honored to be able to contribute to your consideration of this critical issue. I am head of the World Wide Web Consortium's (W3C) Technology and Society activities, responsible for development of technology standards that enable the Web to address social, legal, and public policy concerns. W3C, an international organization made up of over 420 members from industry, academe, users organizations and public policy experts, is responsible for setting the core technical standards for the World Wide Web. W3C was founded in 1994 by Tim Berners-Lee, inventor of the Web, who serves as the Director of the Consortium. In addition to my work at W3C, I also hold a research appointment at MIT's Laboratory for Computer Science, teach Internet public policy at MIT, and am a member of the Internet Corporation for Assigned Names and Numbers (ICANN) Protocol Supporting Organization Protocol Council.

Today I will touch on three major points:

- The Online Privacy Environment: Increasing sophistication in Web technology enables the collection of large volumes of personal information, sometimes with

the explicit knowledge of the user, and sometimes in the "background." While this information may often be collected for purposes considered positive by the user, most users are unable to exercise meaningful control over data collection and in many cases will have little control over subsequent use of personal information.

- The Platform for Privacy Preferences (P3P): W3C's P3P project will enable the marketplace to deliver software tools and services that enhance users knowledge of Web sites' information practices and give users more control over their personal information. A wide cross-section of the Web community has contributed to the development of P3P and is now beginning to test early implementations of the draft standard.
- Balancing Law, Technology, and Industry Practice: All three of these elements are required to give users the privacy protections they need in the online environment. Whatever the mix of law and self-regulation, we should assure that it creates an environment that encourages the development of innovative privacy-enhancing tools.

I. The Online Privacy Environment

The Internet and the World Wide Web have put extraordinary power over information in the hands of people and institutions around the world. With unprecedented ability to both publish and access information in the hands of hundreds of millions of people, centuries old barriers to knowledge and exchange of ideas have vanished. Yet this same interactivity, the bi-directional ability to exchange information from any point to any other point on the Net has brought about significant threats to individual privacy. For the same communications mechanisms that give individuals the power to publish and access information can also be used, sometimes without the user's knowledge or agreement, to collect sensitive personal information about the user and his or her information usage behavior. At W3C, our goal is to use the power of the Web, and enhance it where necessary with new technology, to give users and site operators tools to enable better knowledge of privacy practices and control over personal information.

Urban legends of the Web's imagined surveillance capabilities abound. Nevertheless, Web technology has evolved quite sophisticated data collection techniques which have caused alarm and distrust among many users. State-of-the-art Web sites are able to collect personal information about users both directly, by presenting online forms to be filled out by users, and in the background, through use of various technologies such as access logs, cookies and, in some cases, the placement of small programs that run on users computers collecting information and delivering it back to the site. The background techniques are often used to offer more customized, personalized and easy-to-use services, many of which users appreciate. Yet, all but the most technologically sophisticated users have no practical ability to understand what sort of background data collection is taking place on their computers, much less limit such collect when they wish.

Powerful data collection techniques, users inability to know what is being collected or how to stop it, together with occasional highly publicized abusive privacy practices, all combine to generate a significant level of fear and distrust on the part of many Web users. Three of the most notable online privacy incidents in the last year illustrate how strongly users and the general public react when users discover that data collected about them may be used for a dramatically different purpose, or that personal information will be disseminated without their control.

- Intel Processor Serial Number: Just before it released its new Pentium III processor, Intel had to turn off access to the unique serial number inside each processor because users objected to the inability to block transmission of this serial number to Web sites. Though Intel believed this ID would actual enhance security by providing better transaction verification, users felt that it would be used to track their browsing and buying habits without giving sufficient control to users.
- Doubleclick personally-identifiable web usage tracking: Widespread outcry arose earlier this year when Doubleclick announced plans to use user information previously collected to track surfing habits of users for the purpose of targeting banner ads. User objected to the fact that information previously collected was to be used for a different and more invasive purpose, and because it was not clear to many people how to opt-out of such tracking. Doubleclick has subsequently withdrawn the tracking plans and mounted an education campaign to inform users, among other things, how to control the information collected by Doubleclick.

W3C and its members became concerned about privacy on the Web because people won't use the Web to its full potential if they have to face such uncertainty. The majority of users are perfectly willing to share some information on the Web. At the same time, basic human dignity demands the we have meaningful control over which information we chose to expose to the public. Our goal is to include in the basic infrastructure of the Web the building blocks of tools that can provide each user this basic control.

II. P3P Enables Greater User Control

To help address growing concerns about online privacy, W3C launched the Platform for Privacy Preferences (P3P) project to enable the development of a variety of tools and services that give users greater control over personal information and enhance trust between Web services and individual users.

P3P-enable services will enhance user control by putting privacy policies where users can find them, present policies in a form that users can understand them, and, most importantly, enable users to act on what they see in policies more easily. For e-commerce services and other Web sites, P3P can be used to offer seamless browsing experience for customers without leaving them guessing about privacy. Moreover, P3P will help e-commerce services develop comprehensive privacy solutions in the increasingly complex value chain that makes the commercial Web such a success. On today's Web, when a consumer buys a product or service from one Web site, completing the transaction may well involve numerous individual services linked together, each of which has some role in the ultimate delivery to the user and each of which has some responsibility for honoring the privacy preferences expressed by the user at the beginning of the transaction.

Consider all of the steps involved in the increasingly common processing, printing, distributing, and archiving a digital photo. After the user takes a digital image with a common digital camera, one site may be the point to which the photo is first uploaded, from there the user follows a link to another site that performs special image processing, after which the next site created prints, which are then delivered by yet another service to family members. Finally, yet another site may offer archival services for the photos. At each step along the way, these sites are dealing with sensitive information (the names of the people in the photos, their location, etc.).

Setting the stage where such flexible combinations of services can be offered to users requires widespread agreement on standards, including the means of communicating from one service to another about how personal information should be handled. Standards have a vital role in the operation of the Web in general. The Web is not run by any single organization, but it does enable people to share information around the world because everyone who operates a piece of the Web agrees to follow shared technical standards. In the same was as the HTML standard ensures that everyone who looks at a Web page will see it as the author intended it to look, regardless of what computer or software is used, the P3P standard will enable every user and site operator on the Web to communicate in a common language about privacy.

Can users find P3P in their browsers today? Not yet, as the standard is only just being completed. P3P has been under development over the last two years at the World Wide Web Consortium in a design effort that has included software vendors, large commercial users, privacy advocates, and government data protection commissioners from around the world. Participants in the effort include

- America Online/Netscape
- American Express
- AT&T
- Center for Democracy and Technology
- Commission Nationale de l'Informatique et des Libertes
- Citibank
- Electronic Frontier Foundation
- Microsoft
- NCR
- NEC
- Nokia
- Information and Privacy Commission/Ontario, Canada
- PrivacyBank
- Privacy Commissioner of Schleswig-Holstein, Germany
- Phone.com
- Geotrust

With the standard definition nearly complete, we are now entering the testing and implementation phase. Our last step in finalizing the design of the standard is to

host a series of interoperability testing events, one in June and one in September. We are encouraged that a number of large Web software developers as well as innovative smaller services have committed to implementing P3P in their products. Following this testing phase, we will issue a final standard for the Web community.

III. Conclusion: Role of Law, Technology Tools, and Industry Practice in Privacy Protection

This Committee faces hard questions regarding what regulatory framework, if any, will best address the serious privacy issues on the Web today. Congress may choose to enact a general privacy baseline, or may consider targeted legislation focused on certain sensitive sectors, such as has already been done with respect to children's privacy. Or, those who seek more time for self-regulatory efforts may take hold. I am not here to support or oppose any particular approach, but rather to suggest that with or without legislation, Web users in the United States and around the world need more powerful technical tools to give users greater control over their online privacy relationships. Similarly, e-commerce service providers need tools to enable them to build innovative, flexible, customizable services that respect users' privacy rights and preferences.

Even with the most stringent privacy laws one might imagine, so much of practical privacy rights depends on users being able to make individualized choices about the privacy relationships that want to have with the growing number of Web-based services with which the interact. Effective exercise of informed choice, whether under legislative mandate or enlightened self-regulation, can only be accomplished in the increasingly complex Web of personal information with the help of tools that users can use. So whatever the final outcome of this debate, we should all be committed to see that the innovative and entrepreneurial energy that abound in the Internet are able to develop innovative tools to help users and vendors.

The CHAIRMAN. Thank you.

Ms. Lesser, Ms. Varney, do you have a response to Mr. Catlett's allegations?

Ms. LESSER. Well, I would say the following. Obviously, we sort of fundamentally disagree with Mr. Catlett on approach, but we fundamentally agree with Mr. Catlett on the need to protect consumers' privacy.

The CHAIRMAN. Do you disagree when he says that there is no technology that will solve this problem nor does the FTC have sufficient authority?

Ms. LESSER. Let me take the first and then the second. On the technology question, I think it is certainly not technology alone. As Mr. Weitzner has laid out, there are lots of efforts going on in terms of technological development in helping consumers and businesses have that conversation and making it easier for consumers to get notice and make choices, and that is critical.

However, in order for technology to solve some of these problems, you have to rely on implementation and in many ways you need to rely on how businesses are going to deal with their consumers. So I would say, in answer to some of the questions raised about whether there are large companies or small companies having complicated, incomplete, misleading privacy policies, I would submit, based on our own data with our customers, those companies will not ultimately succeed in getting consumers' trust and they will see a decrease in their business.

So I do not think that technology can do it alone, but we have never relied on technology to do anything alone. It needs to be coordinated with good business practices.

In terms of legislation, I think that, as I said, it is not a zero sum game. There may be areas where we need to see standards set by this Committee to guide the industry and to make sure that we are all headed in the right direction, particularly those of us who are

not at this particular point. However, we need to do this in a deliberative way and make sure that we have identified what issues need to be addressed and who best to address them.

I strongly believe that the FTC has an important role to play. I believe this Committee has an important role to play and that industry and consumers engaged in a dialog have an important role to play.

I will say there is one important thing I disagree with in Mr. Catlett's remarks that I think it is important to emphasize, and that is the issue of preemption. However you folks begin to look at this issue, it is critical as we look at this medium, which we know is national but we also know is global, that we do not seek out a multiplicity of confusing and inconsistent standards, that whatever road we go down we make sure that companies, every single company, be it the smallest company in any of the States represented here, go online and serve customers, they may be serving customers from all 50 States very quickly and from all over the world, and they simply, both large and small companies, cannot comply with a multiplicity of laws that are inconsistent around the globe and around this country.

So I would strongly urge you, as you look at standards, to think clearly about the need to respect the global and national nature of the Internet online medium.

The CHAIRMAN. Ms. Varney.

Ms. VARNEY. Yes, Senator. As to the second question, the FTC authority, clearly the Federal Trade Commission has the authority to prosecute anybody who posts a privacy policy that is deceptive or misleading, and they should do it and perhaps they need more resources to do it.

Do they have the authority to compel Web sites that do not post privacy policies to do so? Probably not. Do they have the authority to compel Web sites to post privacy policies using certain language or in a certain way? Probably not.

The Chairman of the Federal Trade Commission and I, as a former Federal Trade Commissioner, have had a longstanding argument, which I think you have heard before, about whether or not the FTC's unfairness authority, as opposed to their deception authority, would be a sufficient basis for them to prosecute those who collect and use personal information for purposes other than it was provided without adequate notice and consent.

The Chairman believes he does not have—that the Section 5 unfairness standard does not give him that authority. I think it does. But he is a professor and a former dean of a university and he is the Chairman.

The CHAIRMAN. Mr. Catlett.

Mr. CATLETT. Thank you, sir. On the issue of preemption, if Congress moves promptly and passes a good law that gives strong rights to individuals, then the States will not need to move in to address particular needs of their citizens.

As to the question of inconsistent legislation, companies deal globally with this problem all the time. For example, Doubleclick does not set cookies in Germany because of laws that relate to privacy. Therefore Germans are getting better privacy protection from an American company than Americans are. So companies do deal

with these large differences and a nation gets the level of privacy protection that it demands.

The CHAIRMAN. Mr. Berman.

Mr. BERMAN. I think some companies can deal with the crazy quilt of regulations. One of the arguments for legislation is to get away from that and to have some uniformity. I agree with Jason that it ought to be a high standard—and a standard that protects privacy, but it also has to protect the free flow of information over the Internet. And if our companies or our small Web sites have to figure out the laws and design their sales and their approaches to be consistent with every country in the world, I think that will be an enormous burden on commerce.

So one of the reasons why I think that it is important for the United States and for us to work these things out now is to establish we are a leader in the Internet and what the regulatory regime that makes sense for the Internet makes sense also internationally. A traditional large regulatory role over every Web site, which some Europeans advocate, I think is inconsistent with the way the web is designed and will not work. So it is part of providing leadership.

One last point. These issues are complex and I think that in order to work them out it does require drilling down on what do we mean by notice, what do we mean by access, what do we mean by a remedy. What is fair when L.L. Bean sends your shoe size to the wrong company? Do they go to jail? Those are not easy questions, what access do you have and what is the security, those issues.

But—and I think that in order—and a regulatory agency should not be given an enormous amount of discretion. In order to limit that discretion, one of the things that Congress can do is when it writes its legislation, which is to make clear in legislative history and go and really use staff time and drill down on how its legislation is going to work, the explain to the FTC and explain to the public and to the companies what they have in mind.

That is not easy legislation, but it is absolutely I think critical in this area or you will see too much discretion and you will not have the confidence of the Internet community.

The CHAIRMAN. So, Mr. Catlett, along those lines, I like many others buy books online. Now when I go on one of these Web sites they say: Hi, John; we just got in a new biography of Napoleon we know you would like—which is true. They know, they know what my preferences are. So actually they are helping me by informing me of books that I would like to read. What is wrong with that?

Mr. CATLETT. That is a wonderful service, sir, and I use it myself.

The CHAIRMAN. You know what I am getting at here, OK. Where does the line stop where they are informing me and helping me and they are invading my privacy?

Mr. CATLETT. Everybody wants the benefits of personalized technologies and the Internet is wonderful at providing that, provided that the personal information is treated fairly. That means several things: only using the information for the purpose that they collected it for, in the case of say making book recommendations, and not for selling to, giving to journalists who want to get a psychographic profile of the individual who buys the books.

Second, the individual should have access to that complete profile that is built up so that they can be sure for themselves——

The CHAIRMAN. Like a FOIA, like a Freedom of Information Act.

Mr. CATLETT. Precisely, sir. And those laws should apply very broadly to all commercial entities that maintain personal information. It is the right of people to determine information that is held about them. That information is being used by companies supposedly for their benefit and so people have the right to see that information.

The CHAIRMAN. Do they now?

Mr. CATLETT. No, they do not, sir. You have the right to see your credit report, but you do not have the right to see the vastly greater profiles about you that marketing companies have.

The CHAIRMAN. Is that fair, Ms. Lesser?

Ms. LESSER. I think it is a fair articulation of the current law. I do not think it is necessarily a fair articulation of all business practices. So for example——

The CHAIRMAN. Now wait a minute. Is it fair for me not to know what——

Ms. LESSER. Oh, I am sorry, I misunderstood your question.

The CHAIRMAN. Should I be able to see what Amazon.com's profile of me is?

Ms. LESSER. I imagine that if Amazon.com is creating, is giving you, for example, as we do, an opportunity to have a member profile——

The CHAIRMAN. Is it fair for me to know what the profile is, Ms. Lesser?

Ms. LESSER. Sure, absolutely, it is fair for you to know.

The CHAIRMAN. But right now I do not have that right.

Ms. LESSER. You will probably be given a right to know what your profile says by a lot of companies, because it is smart business practice.

The CHAIRMAN. But if they do not choose to——

Ms. LESSER. Now, the level of—there is a difference between understanding access, i.e., do you access directly into the data base or do you have an ability to basically say——

The CHAIRMAN. You are complicating the issue.

Ms. Varney, do I have the right to know what profile is compiled on me by an Internet corporation?

Ms. VARNEY. Do I get to ask you a question back, to further this?

The CHAIRMAN. Yes.

Ms. VARNEY. OK, thank you.

The CHAIRMAN. Tragically, yes.

[Laughter.]

Ms. VARNEY. Do you want to know—the company is going to take what you have purchased on their Web site to develop their profile. Do you want access to everything that you have purchased?

The CHAIRMAN. No, what their profile of me is.

Ms. VARNEY. So you do not care about getting access to your past purchases? You want to see what they do with that information?

The CHAIRMAN. I want to know what the profile is because obviously they are letting other people know that profile.

Ms. VARNEY. Why are they letting other people know the profile?

The CHAIRMAN. I do not know why. For profit and fun.

[Laughter.]

Ms. VARNEY. Not yours, Senator, I can assure you.

The CHAIRMAN. I am sorry, Conrad.

Ms. VARNEY. If they are not sharing the profile, does that matter to your question?

The CHAIRMAN. Even if they are not sharing the profile. The FBI has a file on me and I hope they are not sharing it, and yet I have the ability—well, I do not care if they are.

[Laughter.]

The CHAIRMAN. Most citizens would not want that. So through the Freedom of Information Act I can find out, I can get my FBI file. Should I not be able to, through some kind of Freedom of Information Act, know the profile that is kept on me?

Ms. VARNEY. Having been through the Senate confirmation process, I do have an FBI file and I have reviewed it, and what is in my FBI file are facts and summaries of conversations——

The CHAIRMAN. Should every American have the same right as they do with the FBI file?

Ms. VARNEY. But Senator, that is what I am getting at, what is in the FBI file. If the FBI has a psychographic profile on me, I have not seen it, I cannot see it.

The CHAIRMAN. They may and they may not. I have seen all kinds of FBI files.

Ms. VARNEY. Can you see what they have on me?

The CHAIRMAN. You are evading my question. Should they have the right to know the profile—should I have the right to know the profile that is kept on me?

Ms. VARNEY. Senator, I do not mean to be evasive. I am trying to——

The CHAIRMAN. So you are not going to give me an answer?

[Laughter.]

Ms. VARNEY. I am going to give you an answer.

The CHAIRMAN. Then say it.

Ms. VARNEY. I am trying to draw a distinction——

The CHAIRMAN. If you want to ask me a question, you have got to give me a yes or no answer.

Ms. VARNEY. I will, I will. You will not let me, though. I am trying to draw a distinction between the data that is used by a company to create a profile and the profile. Obviously you have a right to all the data, the transactional data. What some of the companies will say back to you, whether or not you accept this argument, is: We spend a lot of time and a lot of money and hire a lot of people and do algorithms and all kinds of things to come up with what we think is the profile. It is our proprietary property.

Is it good business sense to share it with you? Sure. Do you want to legislate it? Talk to the companies that do it. I do not know.

The CHAIRMAN. So your answer is "I do not know." Now, what is your question for me?

Ms. VARNEY. I asked the question, whether you wanted access to the underlying data or to the profile that the data was used to generate.

Mr. WEITZNER. Well, my question is I want to see your profile.

The CHAIRMAN. I think I should have access—very frankly, I think I should have access to any information that is collected

about me and conclusions that are drawn about me. I think that is the right of citizens, and I do not understand how it could be—well, go ahead.

Mr. WEITZNER. Could I suggest we just take one step back. I do not have a quick answer to this question, but the right of access——

The CHAIRMAN. By law I can have my credit profile.

Mr. WEITZNER. That is right, and the reason that you can have your credit profile is because important decisions are made affecting your life based on that credit profile. So you have a right to see it really in order to correct it if there are mistakes.

The CHAIRMAN. Suppose that this company that makes a profile of me that portrays me as an axe murderer is then sold and distributed to others, all over the Internet. Is that good?

Mr. WEITZNER. I think that what you certainly have a right to know is what are they disseminating to others. I am not sure that I am comfortable with the notion that any single Web site that has any kind of commercial activity has to have a mechanism for disclosing all of the information that it compiles that is in some way personally identifiable. That really goes pretty far and I think, as the FTC Advisory Committee recently pointed out, you get into a whole other set of privacy problems.

How does Amazon know that you are you when you are coming to look at your profile? A lot of people are going to be trying to figure out every Senator's password.

The CHAIRMAN. They have got my credit card. They get my credit card when I make a purchase, so they are pretty darn sure that it is me.

Mr. WEITZNER. Well, they insure against the risk that it actually is not you and they protect themselves. And the credit card companies charge you whatever interest they charge you.

The CHAIRMAN. They do not know that I like history books just because of one purchase.

Go ahead, Mr. Berman.

Mr. BERMAN. I think the answer is—I raised it before—this is not an easy question. There has been a committee now on access which has drilled down and made a distinction between proprietary information, information which you should have which might be exempt information. So it depends. That is one of the critical factors in writing legislation like this. In order to decide the access——

The CHAIRMAN. You are making an argument we better be very careful about writing——

Mr. BERMAN. You better be very careful and go through the hypotheticals about what you mean by access and who has access. You might also raise the question which we raise: If you have total commitment from the private sector to both only give you that profile and keep it for themselves and never use it for anyone else because they are the only ones that want to sell you Napoleon books, what is the right of the FBI to get access to that information, that profile?

What we have done is we are making an enormous transfer of third party information, personal sensitive information, to the net without also examining what the government access standards are

to that information. I mention the Monica Lewinsky example. A colleague of mine at CDT is testifying over in another——

The CHAIRMAN. We try not to mention that.

Mr. BERMAN.—committee dealing with government access. I would urge that at some point the committee try and look at them together because they are of a piece.

The CHAIRMAN. Well, this is fascinating. This is a fascinating issue. I mean, it is really a remarkable issue, and I would argue that 5 years ago if we had said we would be having this kind of discussion, it simply was not on the screen. I believe that Mr. Catlett is right, though. I think this is a very rapidly growing issue rather than one that is diminishing.

I apologize to my friend and colleague for the length of time I took, but it is a fascinating dialog.

I thank the witnesses.

Senator BURNS. I have never missed a meal and I do not plan to.

[Laughter.]

Mr. BERMAN. You have never missed a meal while I have been up here.

Senator BURNS. In light of the conversation and the dialog with the Chairman, give me your assessment—and I would ask you, Jerry. Give your assessment of the safe harbor approach.

Mr. BERMAN. Well, I think that the safe harbor approach offers a real opportunity in dealing with the Internet. One of the things that the FTC has built up is a considerable amount of experience in dealing with that there are a whole myriad—it is not one-size-fits all on the Internet. We want to encourage a lot of different experiments in enforcement and trying to get companies to do audits and so on.

If the safe harbors encourage that experimentation so that good practices can find their way into that safe harbor, then after developing a data base and factual basis on how those work you can make decisions about whether you need to go further and deal with criminal penalties and all the other paraphernalia. But I would not start at that end, which is with big penalties and high standards for what is a safe harbor, because there is so much experimentation, so many new people on the Internet.

But I think that what is the problem with the self-regulatory regime now is not that people are not trying these experiments, but that they do not know what a safe harbor is. So they do not know what to spend, whether it is worth it, whether if they join E-Trust or BBBOnLine whether they are going to be safe from prosecution or safe from legislation. So I think that that uncertainty is something that your legislation begins to address. I mean, we need to work on it, and Senator Hollings——

Senator BURNS. In other words, we do not want to abandon the safe harbor approach?

Mr. BERMAN. I do not think so.

Senator BURNS. Now let us go, let us go one step further then. Does the simple posting of privacy policy amount to actual privacy to the end user? I mean, once they make——

Mr. BERMAN. It does not amount to privacy if the statement is not complete or it says in some circumstance we do this, in some

circumstance, and it is conflicting. We have examples in our testimony. It has to be a complete statement covering the fair information practices. It has to give you adequate information so that you know what the scope of collection and use is.

Senator BURNS [presiding]. That is all I have today. I have listened to the testimony and the questions. I do not know what happened to the Chairman, but I will tell you this, that we thank you for coming today. There will be other Senators with questions. If you could respond to the individual Senators and to the Committee, that would be helpful.

Right now, this hearing is adjourned. The record will remain open for 2 weeks.

[Whereupon, at 12:51 p.m., the Committee was adjourned.]

APPENDIX

RESPONSE TO QUESTION SUBMITTED BY HON. MAX CLELAND TO JASON CATLETT

Question 1. As you know, I am a co-sponsor of S. 2606, which was introduced this week by Senator Hollings and nine other Senate colleagues. This bill allows for "opt-in" provisions for Web sites using and sharing personally identifiable information, and "opt-out" for non-personally identifiable information. I would like to get your thoughts on these provisions, specifically addressing the implemenatation of these provisions by Web sites and the possible effects it may have on online commerce.

Answer. This responds to Senator Cleland's question to me about S. 2606.

I believe the bill makes broadly the right decision on both opt-in for personally identifiable information (PII) and opt-out for non-personally identifiable information (non-PII), subject to the following qualifications.

For PII, opt-in should certainly be required, since to have personal data distributed without the consent of the person concerned on a data transmission medium as powerful as the Internet would mean the death of privacy online. It may further be necessary to set and evolve a high standard to ensure that the consent is both well-informed and affirmative.

For non-PII, at least an opt-out should certainly be required, but it is possible that in some cases that may arise in the future, the standard should be raised to opt-in. The use of pseudonymous identities is expected to greatly increase in the next few years, and it may be necessary to protect the privacy of these identities, even if they are not personally identified with any natural person.

Accordingly, I would recommend proceeding with the broad standards as they are in this bill, but remove the language preempting state law. If changes become necessary following experience with the law, states should be free to act accordingly.

On the implementation for Web sites, I can speak from direct experience, having operated for about four years a Web site that collects personal information on a purely opt-in basis. The Internet makes the process of opting-in and opting-out very inexpensive, at near zero marginal cost.

This contrasts with the relatively high cost of processing opt-transactions in the physical world. As to the cost of establishing the opt-processing systems, it would be only a very small percentage of the total development cost of a typical e-commerce site. It is entirely reasonable to require this.

The major effect on e-commerce would be to increase consumer participation due to improved consumer confidence. This could be as much as 20 or 40 percent over several years, compared to the ugly scenario where no protections are in place, and consumer confidence continues to decline. People who are scared offline at their earliest encounters with the Internet may be reluctant to return.

Online advertisers might complain that they have to ask people's permission before using or selling information about them, and that therefore they would have to forgo some revenue. This is a very poor reason to lower the standards proposed in the bill, because (i) online advertisers still have a fine business selling ads that are targeted not based on personal information, using the so-called old-fashioned "print model" of putting ads for golf clubs in the sports section: this constitutes the vast majority of their existing revenues; (ii) online advertising is only a tiny percentage of e-commerce revenues; and (iii) it is unfair to permit the advertisers to maximize their revenues at the expense of reducing the total size of the market.

If it is not out of place here, I would like to commend the Senator and his cosponsors on the Consumer Privacy Protection Act, and to express my admiration for the plain common sense of his remarks about online privacy during the hearing.

If I can be of any further assistance to you or the Committee, please free to ask.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MAX CLELAND TO JILL A. LESSER

Question 1. Do you believe people should be able to know what information is collected about them by third parties, how that information is used, and the ability to correct incorrect information?

Answer. Yes. We at America Online believe strongly that "notice" and "choice" with respect to personally identifiable information are essential elements of online privacy protection. In other words, consumers should be given clear notice about what personally identifiable information is collected about them and why it is being collected, and should be given the opportunity to exercise choice about how such information is used. In addition, we believe that organizations that collect personally identifiable information from consumers should take steps to protect the security of that information and should establish a process for correcting inaccuracies in important information, such as account or contact information. AOL's privacy policy is based on these essential principles.

Question 2. As you know, there are several privacy seal programs that Web sites can earn by their privacy practices. Several of the "good players" attempt to influence their business partners to adopt stronger privacy protections and earn the endorsement of these seal programs. AOL works with its partner companies to ensure good privacy practices. However, how do you explain the fact that the FTC report found only 8% of randomly selected sites participate in these programs?

Answer. AOL supports the development of privacy seal programs to help encourage good business practices, build public awareness, and increase consumer confidence in the online medium. AOL helps to promote sound privacy practices through its Certified Merchant Program, which requires AOL merchants to post a comprehensive privacy policy that is consistent with the principles outlined in AOL's privacy policy and the industry guidelines developed by the Online Privacy Alliance.

While we do not know the precise reason for the low level of seal program participation found in the FTC report earlier this year, one factor may be simply that more public education is needed to make both consumers and businesses more aware of the importance of such programs. As public awareness about online privacy issues continues to grow, participation in these programs will likely increase. Furthermore, it is possible that the FTC survey focused narrowly on strict "seal" programs, and perhaps did not take into account the wide variety of compliance and certification programs that currently exist, such as AOL's Certified Merchant program, to help ensure good privacy practices and increase consumer confidence. We believe that the proliferation of all such programs will help to build consumer trust in the online medium.

Question 3. What evidence have you seen to indicate that the average, not necessarily Web-savvy, American Web surfer is knowledgeable about information-gathering practices of Web sites? Especially among groups coming online more and more, like older Americans?

Answer. It is clear that online privacy issues have taken center stage in the public debate over the past year, and that Americans generally are more aware than ever before about both the tremendous benefits of electronic commerce and the potential privacy implications of doing business online with sites that do not protect their privacy. This year's FTC report shows a dramatic increase in the number of commercial Web sites that have posted privacy policies describing their information-gathering practices. Despite this incredible progress, we believe that the average user's knowledge and understanding of how his or her personal information is collected and used online is still not at the level where it needs to be in order to ensure that consumers' privacy is being fully protected.

AOL believes, therefore, that companies doing business online have a responsibility to reach out to Internet users to help educate them about what they can do to protect their privacy online. AOL makes it a priority to clearly inform our members about our privacy policies and about the steps they can take to ensure that their personal information is protected wherever they go online. In addition, we have participated in a number of industry-wide efforts to raise public awareness about online privacy, such as the "Privacy Partnership 2000," an ongoing grassroots initiative created by TrustE and leading online companies like AOL to promote privacy education on the Internet, as well as the recent media consumer education campaign sponsored by the members of Netcoalition.com, a public policy organization comprised of leading online consumer companies. We believe that industry, government, and consumer groups must continue to work together to promote public education about online privacy and bring consumer education to the level where it needs to be.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MAX CLELAND TO THE FEDERAL TRADE COMMISSION

Dear Senator McCain:

Thank you for transmitting Senator Cleland's post-hearing questions related to the Federal Trade Commission's report, *Privacy Online: Fair Information Practices in the Electronic Marketplace* ("Report"). The Commission's responses are as follows.[1]

Question 1. Some people have called for the creation of a privacy commission to establish future privacy guidelines and "add flesh" to laws that may be passed by Congress. Do you feel as though this role could be effectively performed by the Federal Trade Commission? And, what is your opinion on the creation of such a commission?

Answer. Yes, based on the proposals we have seen about the anticipated role of a privacy commission, we believe that the FTC could effectively perform the duties associated with such a commission. As you know, the FTC has been involved with data privacy issues since 1995, and has in fact performed many of the same functions that a privacy commission would perform. The Commission has held a series of widely-attended public workshops, which included participation by industry, advocates, and academics, and has produced numerous reports focusing on a variety of privacy issues, including the collection of personal information from children, self-regulatory efforts and technological developments to enhance consumer privacy, consumer and business education efforts, and the tale of government in protecting online privacy. Moreover, at Congress's direction, the Commission has promulgated a well-received rule pursuant to the Children's Online Privacy Protection Act. The agency will continue to examine privacy issues and we believe the Commission could effectively fill the role of implementing any additional laws Congress may enact. Moreover, the FTC also has a competition mission that gives the agency a unique ability to consider the competitive implications of any privacy regulations.

We generally believe that additional resources can be brought to bear on the evaluation and development of effective privacy protection for Americans. We are concerned, however, that the creation of a separate privacy commission might be inefficient given the FTC resources already devoted to privacy issues. Furthermore, a number of states are moving forward with their own form of online privacy legislation. Thus, such a commission also could have the counter productive effect of delaying thoughtful consideration and development of otherwise appropriate and timely legislation to protect privacy.

Question 2. Do you feel Internet business has the potential to grow with clear, concise privacy policies in effect?

Answer. Yes. As described in our recent report, "Privacy Online: Fair Information Practices in the Electronic Marketplace," (May 2000, available at *http://www.ftc.gov/os/2000/05/index.htm#22)*, some survey research suggests that the vast majority of online consumers are concerned about the misuse of their personal information online, and that large numbers of consumers do not trust online companies to keep their personal information confidential. Alleviation of these concerns should prompt more consumers to use the Internet. Sites with clear and concise privacy policies that implement the fair information practices outlined in the Commission's Report have the potential to appeal to consumers who are concerned by providing a "privacy-friendly" marketplace in which consumers can shop. Moreover, a majority of the Commission believes that if Congress enacts legislation requiring a baseline of privacy protections, consumers could benefit from the knowledge that they would be entitled to at least a uniform level of protection wherever they visit online. This knowledge should also result in a concomitant increase in consumer confidence in the online marketplace.

Question 3. What evidence have you seen to indicate that the *average*, not necessarily web savvy, American Web surfer is knowledgeable about information gathering practices of Web sites? Especially among groups coming online more and more like older Americans?

Answer. As noted in our recent Report, although consumers may not be conversant in the specific information-gathering practices of Web sites, survey evidence indicates that consumers are increasingly concerned about their privacy online. (Report at 2–3.) Some evidence also suggests that older Americans are concerned about shopping online because of their privacy concerns. (Report at 2 n.15, referring to *AARP National Survey on Consumer Preparedness and E-Commerce: A Survey of*

[1] The Commission vote to issue this letter was 4–1, with Commissioner Swindle dissenting. His views are expressed in a separate letter, which is attached.

Computer Users Age 45 and Older (March 2000), available at <http://www.aarp.org/press/2000/nr033000.html>) The Commission unanimously believes that all consumers, including older Americans and others new to the online medium, would benefit from clear and conspicuous privacy disclosures online.

In addition, consumer education about online information gathering is still badly needed. The FTC will continue its efforts to educate consumers about the online marketplace and its information practices and will encourage self-regulatory groups to focus on consumer education as well. Educating businesses about the need to implement privacy protections has and continues to be an important complement to these consumer education efforts.

Question 4. As you know, the Better Business Bureau and other companies have online "seals" for which Web sites can apply if the site believes it meets the privacy standards of those seal programs. The FTC report states that only 8% of the Random Sample of sites and 45% of the Most Popular sites in the survey display a privacy seal. Could each of you comment ou these seal programs and their influence on the Internet industry and its privacy practices?

Answer. The Commission has long supported the development and implementation of seal programs as part of industry self-regulatory efforts. We believe online privacy seal programs can play an important role in advancing the implementation of fair information practices in the online marketplace. They educate both online businesses and online consumers about online privacy protections, and they can serve as a key enforcement component of industry self-regulation in this area. The established programs are to be commended for their efforts to date, and the emergence of several new, competing seal programs is a welcome development.

If widely adopted, seal programs promise an efficient way to alert consumers to licensees' information practices and to demonstrate licensees' compliance with program requirements. Although the number of sites enrolled in seal programs has increased in absolute terms over the past year, with 45% of the Most Popular sites participating, the seal programs have yet to establish a significant presence on the Web. Therefore, their impact on online commerce remains limited. The Commission believes that seal programs' efforts would be bolstered by legislation requiring online companies to adhere to core fair information practice principles.

Question 5. Several Internet companies claim that privacy policies will "kill the goose that laid the golden egg" by being too burdensome on this fledgling industry. The FTC report references concerns of FTC staff and the Advisory Committee an Online Access and Security that some of these recommendations to protect consumer privacy should not be overly burdensome to the company. Do you have any further guidelines on what is "overly burdensome" for the Committee?

Answer. The Commission has specifically recognized that implementation of the fair information practices of Access and Security raise complex issues. As you note, many of these issues were highlighted in the Report of the Advisory Committee on Online Access and Security. The majority of the Commission does not believe that providing Access and Security would necessarily create unreasonable burdens or costs to online businesses.[2] Furthermore, the issue of burden, particularly with respect to small businesses, could be fully and fairly addressed in a rulemaking proceeding. Such a proceeding, with input from online businesses and consumers would greatly assist any implementing agency in crafting a rule that implements online privacy protections in a flexible and reasonable manner.

Please let me know if the Commission can provide any additional information on this important matter.

By direction of the Commission.

ROBERT PITOFSKY,
Chairman.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MAX CLELAND TO ORSON SWINDLE

Dear Chairman McCain:

Thank you for transmitting Senator Cleland's post-hearing questions related to the Federal Trade Commission's report, Privacy Online: Fair Information Practices

[2] Commissioner Leary opposes mandated access and security at this time because he believes that the Commission has insufficient information about the relative costs to businesses and benefits to consumers in this area, and because, if notice is adequate, the competitive marketplace should provide a better solution than regulation.

in the Electronic Marketplace ("Privacy Report"). For the most part, I do not share the views expressed in the Commission majority's response to Senator Cleland's questions. Accordingly, for the Senator's consideration, I am providing my individual responses to his questions.

Question 1. Some people have called for the creation of a privacy commission to establish future privacy guidelines and "add flesh" to laws that may be passed by Congress. Do you feel as though this role could be effectively performed by the Federal Trade Commission? And, what is your opinion on the creation of such a commission?

Answer. A Congressionally established privacy commission could add measurably to the general understanding of online privacy. A serious examination of all the issues surrounding online privacy should add significantly to a better understanding of the possible unintended consequences of the laws that may be passed for the online economy. Such an examination should look at the costs and benefits of various options, including legislation, industry self-regulation, government guidelines regarding industry best practices, etc. As I pointed out in my dissent from the Privacy Report, an analysis of this type should have preceded any recommendation of legislation by the FTC and certainly should precede enactment of legislation mandating privacy protections.[1]

Having some experience and certainly a reservoir of knowledge about privacy online, competitive issues, how to make clear and conspicuous disclosures online, and implementation of the Children's Online Privacy Protection Act, the FTC theoretically could perform this function. However, the recent FTC Privacy Report indicates to me that a more objective, probing analysis and less pro-regulatory bias are desirable. Perhaps it would be best for an independent, non-partisan commission to take on this task, in a manner similar to the Advisory Commission on Electronic Commerce.[2]

Question 2. Do you feel Internet business has the potential to grow with clear, concise privacy policies in effect?

Answer. Yes, although it is obviously growing exponentially now with less than perfect privacy policies in effect. To my knowledge, no one has empirically established the impact of privacy policies on consumer behavior. Industry self-regulation is making good progress. I suspect that the degree to which privacy concerns are impeding the growth of online commerce has been vastly overstated. The FTC's efforts to evaluate online privacy have not included any empirical study of the effects on online commerce of the existence of privacy policies, whether consisting of simple notice or comprehensive statements implementing all four FTC-suggested fair information practice principles. Instead, the FTC, relying upon consumer opinion surveys showing that many consumers are concerned about online privacy, has asserted that online commerce will not reach its full potential without legislation ensuring full fair information practices.[3] Consumer opinion polls showing a generalized concern about-privacy, however, should not be relied upon as the basis for concluding that legislation is required for the optimal growth of online commerce.[4] There is no reason to conclude that legislation will necessarily increase consumer confidence in the online marketplace.

For example, a study conducted by Jupiter Communications in mid-1999,[5] concluded that "consumers do not see government regulation as the solution to the online privacy issue. The vast majority of respondents to a Jupiter Consumer Survey—86%—said that they would not trust a Web site with their privacy even if the government regulated it."[6] The same study asked consumers to identify the top two factors that would increase their trust in Web sites regarding privacy. "The posting of privacy policies eased the concerns of 36 percent of consumers surveyed."[7] Government regulation was "not a popular option" for increasing consumers' confidence:

---

[1] Privacy Report, Dissenting Statement of Commissioner Orson Swindle at 2, 21–24.

[2] This Commission was created by Congress when it enacted the Omnibus Appropriations Act of 1998, Pub. L. No. 105–277, to study and make recommendations about taxation on transactions using the Internet. The Commission's final report is available at http://www.ecommercecommission.org/report.htm.

[3] Privacy Report at iv.

[4] See *generally* Concurring and Dissenting Statement of Commissioner Orson Swindle to Statement of the Federal Trade Commission on Online Profiling; see also Privacy Report, Dissenting Statement of Commissioner Orson Swindle at 10–16.

[5] This study predates the noteworthy increase in the display of privacy policies online and in online sales in late 1999 and the first quarter of 2000.

[6] Michele Slack, Jupiter Communications, *Proactive Online Privacy, Scripting an Informed Dialogue to Allay Consumers' Fears* at 19 (June 1999).

[7] *Id.* at 4.

"only 14 percent indicated that they would more likely trust a Web site on privacy issues if the site were subject to government regulation."[8]

Question 3. What evidence have you seen to indicate that the *average*, not necessarily Web savvy, American Web surfer is knowledgeable about information gathering practices of Web sites? Especially among groups coming online more and more like older Americans?

Answer. To my knowledge, the research cited in the Commission's Privacy Report does not directly address this issue. One study mentioned in the Report, a telephone survey of adult computer users conducted in March 2000 by Harris Interactive for *Business Week,* found that 40% of computer users had heard of cookies and, of these, 75% understood them to be "files downloaded onto your computer that track your online habits."[9] The Harris poll also found that 55% of computer users while surfing online had seen a privacy notice or other explanation of how personal information collected by a Web site will be used. Of those who had seen a privacy notice, 35% always read it, 42% sometimes read it, 18% rarely read it, and only 4% never read it.[10]

Surveys that indicate that consumers are increasingly concerned about online privacy are not evidence that consumers are knowledgeable about the information gathering practices of Web sites. Simply stated, once again the FTC is presenting misleading interpretations of opinion survey results, including the AARP survey.

The AARP report shows that the majority (54%) of older Americans who use the Internet *make purchases online.*[11] Three out of four of these online purchasers describe themselves as either very or somewhat concerned about the privacy of the information, yet they make purchases.[12] This confirms my sense that consumers who express concerns about privacy in the abstract find that their concerns are outweighed in practice by the convenience and other benefits of shopping online.

The Privacy Report, relying only on the press release and not the full AARP Report, cited the press release as support for the proposition that "many consumers who have never made an online purchase identify privacy concerns as a key reason for their inaction."[13] In fact, the AARP study itself does not permit any conclusions to be drawn about the degree to which privacy concerns or any other reason influenced consumers' decisions not to purchase online.

Instead, the study used an open-ended question followed by probing to determine why those respondents who stated that they never purchased over the Internet have not made such purchases).[14] The resulting tabulation of reasons offered by consumers in response shows only how frequently these consumers identified particular reasons for not purchasing, not whether a particular reason was "key" to their decision not to purchase. Of the Internet users who have never made an online purchase, 43% "simply are either not interested in online shopping (28%) or do not like online shopping (15%)."[15] Another 20% indicated that they like to shop and/or examine products in person. Twenty-four percent cited "concerns about privacy" and an additional 6% stated they were concerned about "safety of payment."[16]

Question 4. As you know, the Better Business Bureau and other companies have online "seals" for which Web sites can apply if the site believes it meets the privacy standards of those seal programs. The FTC Report states that only 8% of the Random Sample of sites and 45% of the Most Popular sites in the survey display a privacy seal. Could each of you comment on these seal programs and their influence on the Internet industry and its privacy practices?

Answer. The "seal programs" are a good idea. However, the fact that a company does not use a seal program does not mean that it has unsatisfactory privacy policies and practices. No conclusions should be drawn from not belonging to a seal pro-

---

[8] *Id.*

[9] Business Week Online, *Business Week/Harris Poll: A Growing Threat* (March 2000), available at <*http://www.businessweek.com/2000/0012/b3673010.htm*>. Interestingly, of those computer users that are aware of cookies, many set their computers to reject them, either always (21%) or sometimes (21%), while an even larger group either never (43%) or only rarely (10%) did so.

[10] *Id.*

[11] *AARP National Survey on Consumer Preparedness and E-Commerce: A Survey of Computer Users Age 45 and Over* ("AARP Report") at 32, 62 (March 2000), available at <http://research.aarp.org/consume/e-commerce__1.html>.

[12] *Id.* at 54.

[13] Privacy Report at 2 n.I5.

[14] AARP Report at 64.

[15] *Id.* at 34.

[16] *Id.* A variety of other reasons are also identified in the AARP Report, but only reasons mentioned by at least 3% of those surveyed are reported.

gram. Seal programs are but one of many practices that can be used to give consumers confidence. Companies with good business practices that satisfy consumers accomplish that confidence-building without necessarily having to employ seal programs.

I disagree with the majority's conclusion that seal programs have yet to establish a significant presence on the Web. As I mentioned in my dissent from the Privacy Report, seal programs are not the only enforcement mechanism that backs up self-regulation).[17] In any event, 45% of the most popular sites—the ones that attract the greatest number of individual visitors—use a privacy seal, and that is not an insignificant presence by any stretch of the imagination.

Question 5. Several Internet companies claim that privacy policies will "kill the goose that laid the golden egg" by being too burdensome on this fledgling industry. The FTC report references concerns of FTC staff and the Advisory Committee on Online Access and Security that some of these recommendations to protect consumer privacy should not be overly burdensome to the company. Do you have any further guidelines on what is "overly burdensome" for the Committee?

Answer. I do not know what privacy policies will be "overly burdensome," although I suspect that mandating Choice, Access, and Security may be burdensome for many small Internet companies, as well as for larger companies whose business models rely on the sale or use of consumer information to offset the costs of providing benefits and services to consumers. No one, at the FTC or elsewhere, has made an assessment that answers your question. This was my sharpest disagreement with the majority's legislative recommendation in the Privacy Report.[18] It is critical to look at the costs and burdens that proposed legislation might impose *before imposing them,* and it is just as critical to realistically assess the likely benefits of such legislation.

Regulations have a long history of not accomplishing their original, well-intended purposes, and unintended adverse consequences are a well known, oft-occurring fact of life. No one at the FTC has made a cost-benefit analysis of either the legislative/regulatory approach or the industry self regulation approach.

In its response to this question, the majority basically says, as it did in the Privacy Report that, regardless of the costs of legislatively imposed privacy requirements, Congress should impose them anyway, and we will work out the problems later. This could have a chilling effect on the New Economy, and the damage could be difficult to repair.

Please let me know if I can provide additional information on this important matter.

Sincerely,

ORSON SWINDLE

CENTER FOR DEMOCRACY AND TECHNOLOGY
Washington, DC, September 8, 2000

Hon. JOHN MCCAIN,
Chairman,
Senate Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Chairman McCain,

Thank you again for inviting the Center for Democracy and Technology (CDT) to testify at the May 25, 2000 oversight hearing on Internet privacy. We are happy to answer the Committee's additional question on CDT's view of current practices in Internet advertising.

The ability to personalize and customize content for the individual is one of the main features drawing a vast number of individuals and businesses to the Internet. Individuals can be empowered by this personalization. For example, tailoring information to a person's needs could help a citizen more easily find details about their local elections or a consumer could aggregate advertisements in order to compare prices. In both of these cases, some sort of personal information or preference data may be needed. All of these and other similar activities should be encouraged, but in each case the companies providing the personalization service must make decisions about how they plan to protect the individual's privacy in the process. Too often, CDT has seen common Internet business practices that surreptitiously collect

[17] Privacy Report, Dissenting Statement of Commissioner Orson Swindle at 9–10.
[18] *Id.* at 21–24.

information. These practices should not be blamed on a particular technology, but on how tracking technologies are utilized.

Simply put, individuals should be told when decisions are being made about them.

CDT is not a business organization and therefore we cannot offer a comparison or analysis of the effectiveness of a particular business or marketing plan, but we can offer an assessment of ways to personalize while protecting privacy. Despite the polls showing that as many of 96% of Americans are concerned about privacy, many companies still do not take privacy into account or purposely ignore privacy when creating new business models. These companies are left to defend bad practices that could have been avoided at an earlier stage if privacy had been a consideration.

The good news is that the tide has begun to turn. Everyday CDT meets with companies that want to make sure that they are protecting privacy or have created new privacy enhancing technologies that put users in control. Two members of the CDT staff have recently written a short article entitled "Your Place or Mine: Privacy Concerns and Solutions for Client and Server Side Storage of Personal Information"* detailing some of the legal and technical concerns that business should take into consideration when making decisions about how to personalize. I have also included a recent law review article with a broader overview.*

I would be happy to answer any remaining questions that you may have. Please feel free to contact me.

Sincerely,

JERRY BERMAN,
Executive Director.

cc: Senator Max Cleland

ASSOCIATION OF NATIONAL ADVERTISERS, INC.
Washington, DC, June 12, 2000

Hon. JOHN MCCAIN,
Chairman,
Committee on Commerce, Science, and Transportation,
United States Senate
Washington, D.C.

Dear Mr. Chairman:

The Association of National Advertisers (ANA) commends you for holding the May 25th hearing on Internet privacy issues and the FTC's report on the most recent privacy "sweep." We continue to believe that the most effective way to protect privacy in the online environment is through a combination of strong industry self-regulation, consumer empowerment and strong FTC enforcement under existing legal authority. While much more remains to be done, we believe that industry self-regulation has made substantial progress in the past few years. Also, the FTC has been an active, effective "cop on the beat" in this area. Therefore, ANA believes it would be counterproductive and premature for Congress to adopt broad privacy legislation at this point.

We would appreciate it if you would include these comments in the official record for the May 25, 2000 hearing.

In last year's "report card" to Congress on the state of online privacy protection, the FTC stated: "The Commission believes that self-regulation is the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology." We agreed then and strongly believe now that those sentiments continue to be correct.

The most recent FTC survey found significant progress in the number of sites that posted privacy policies, 88% of a random sample and 100% of the most popular sites. This is truly a major improvement from the FTC's first sweep in 1998, when only 14% of Web sites had any disclosure about privacy policies.

We agree with you that the privacy disclosures on many Web sites are too long and complex. We have urged our member companies to take another look at their notices to make sure that, to the maximum extent possible, the disclosures are clear and conspicuous and in language that ordinary consumers can understand.

According to the FTC report, only 20% of the busiest commercial sites implement all four of the fair information principles of notice, choice, access and security. We believe that the 20% finding must be placed in the proper context.

While most sites have policies on notice and choice, many are still developing policies on the complex issues of access and security. These issues are very challenging,

---

*The information referred to has been retained in the Committee files.

as demonstrated by the report of the Commission's Advisory Committee on Online Access and Security (ACOAS). Even the FTC admits in its report that it has not been able to establish clear standards on how to implement these policies. Yet the FTC's report graded down Web sites for not fully addressing access and security.

Everyone agrees on the concepts of access and security, but these issues are the true Gordian Knot of privacy. Implementing these concepts is a difficult and complex process. Providing consumers with broad access to information, without adequate protections, poses potential severe security risks. Overly stringent security precautions can make access very difficult.

Effective privacy protection is more than a numbers game. Even if 100% of Web sites provided easy access to information, without stringent security precautions, 100% access may in fact diminish rather than enhance consumer privacy. It is thus not surprising that while most Web sites address notice and choice, many are still struggling with how best to address access and security. The online community is nevertheless committed to addressing these areas in a timely and effective manner.

Though groups such as the Online Privacy Alliance (OPA), ANA and others in the business community have reached out to encourage all commercial Web sites to post privacy policies. There are now three major privacy seal programs in operation and numerous software programs available in the marketplace. Several tools are available that allow consumers to surf online completely anonymously. New technological solutions such as P3P are closer to implementation. A number of major marketers have refused to place advertising on Web sites that do not have strong privacy policies.

These and other self-regulatory efforts can respond more quickly to changes in the marketplace than an overly restrictive regulatory regime. We must be careful not to impose regulations that would impede the growth of the Internet, rather than enhance it.

While more must be done, we believe self-regulation is working and becoming stronger. ANA, several of our member companies and other industry groups are committed to taking major steps to accelerate these efforts. These steps will include improving privacy policies and making them more user-friendly, further development of technological tools to empower consumers to protect themselves, and a broad consumer education program.

As you know, the FTC already has broad power to regulate the online marketplace under section 5 of the FTC Act. We believe that this authority, coupled with consumer education programs and enhanced technological tools, is the most effective and flexible approach to the rapidly changing online environment. Since the Internet is a global medium, there are real, practical limitations to the reach of national legislation and regulation. Therefore, effective self-regulation and consumer empowerment become more important in this environment.

We remain committed to working with you to protect the privacy of online consumers. However, we believe that broad privacy legislation at this point would be premature and counterproductive.

Thank you for your consideration of these views. Please feel free to contact me if you have any questions.

Sincerely,

DANIEL L. JAFFE,
Executive Vice President.

PREPARED STATEMENT OF HON. ROBERT G. TORRICELLI, U.S. SENATOR FROM NEW JERSEY

Mr. Chairman and Members of the Committee, I am honored to have the opportunity to address online privacy, an issue that is of growing concern to the millions of Internet users all across the country and the world. It is estimated that over 100 million Americans have the ability to access the Internet. The rise in the use of the Internet has led to concerns regarding the privacy of personal information transmitted online, particularly, as more people use the Internet for transmitting sensitive financial and medical information and for shopping purposes. While some argue that given the Internet's global reach and constantly changing technology, industry self-regulation would best protect privacy, others advocate for strong legislative and regulatory protections. And, still others, such as the witnesses here before us today, recommend a multilayered protection consisting of self-regulatory efforts supplemented by legislation authorizing regulatory oversight. Today's hearing is an important way for Congress to gather the information necessary to thoughtfully consider the range of issues involved in the online privacy debate and to evaluate the proper way to address those issues.

An Internet users' life is "virtually transparent." [1] This is in part due to the number of companies that fail to provide consumers with full disclosure regarding how the company may use personal information transmitted online. As the Federal Trade Commission's (FTC) May 2000 report "Privacy Online: Fair Information Practices in the Electronic Marketplace" reveals, only forty-one percent of Web sites in the random sample and sixty percent of the most popular sites provide the most critical of fair information practice: notice and choice.[2] The notice that is provided is often densely worded and at times even misleading.

Even more troubling are the number of companies allowing online marketers to place third-party cookies on their Web sites. Without our consent or knowledge, programs known as "cookies" monitor and collect information regarding our Web browsing habits. Personal data is also extracted directly by Web sites whenever we transmit the information required to purchase a product or surf the Internet for a specific topic. The FTC survey found that fifty-seven percent of sites in the random sample and seventy-eight percent of the most heavily trafficked sites allow the placement of cookies by third parties and that the majority of these cookies are placed by advertising companies engaging in online profiling. The report further revealed that the majority of Web sites that allow third-party cookies do not disclose that fact to consumers.[3]

Our actions will be monitored and our information will be shared unless we specifically request that a company not do so, a process known as "opting out" Opting out requires a user to directly contact a site to decline disclosure. Online industries argue that by posting opt out features, they are, in fact, affording consumers a choice to protect their privacy. However, as a means of securing the right to online privacy, opting out is a burdensome solution that has proven itself largely ineffective. Opt out procedures are often confusing and obscured within a Web site. They are therefore rarely exercised. One leading marketing company that tracks eighty million online consumer profiles has revealed that it receives an average of only twelve opt out requests per day.

This situation, while unsettling, is not inherently menacing. Marketing, both online and off, is a common and often beneficial practice occurring daily in other forms such as mailings and telephone surveys. Businesses benefit from online marketing through improved efficiencies resulting from a more detailed analysis of their markets. Many consumers also desire the information marketing provides about products and services that reflect their preferences and budgets. A healthy balance can and must be established that allows consumers and commerce to reap the benefits of these practices but in a way that is mindful of the public right to privacy. This balance has yet to be achieved. Unlike individuals choosing to partake in surveys and questionnaires, those of us participating in online marketing do so unwittingly and involuntarily, unable to hang up a phone or throw away an envelope.

Disturbing examples such as these point to an immediate need to provide consumers with direct control over outside access to their online activities. Consumers must be given the right of consent prior to any disclosure of personal information. They must be afforded a clear choice to "opt in" to disclosure programs rather than the need to opt out of them. They must also be given clear and accessible knowledge of the extent of their privacy so that any choice they make will be fair and informed. Web sites must accept the burden of persuading consumers of the benefits and desirability of information sharing. If companies are successful in convincing consumers that these benefits are clear and substantial, consumers will readily agree to participate.

Early this year, with these provisions in mind, I introduced S. 2063, the Secure Online Communication Enforcement Act of 2000. This legislation was intended to establish a national dialogue to educate Americans about the challenges of cyberspace. In doing so, I hope it will intensify public participation in an emerging debate to determine the relationship of the Internet to our society and the role of our government in determining that relationship. This dialogue is also vital towards preserving and strengthening public confidence in the viability of the Internet as a secure medium for commerce and information exchange. Consumers are currently spending over fifty billion a year at over eleven million dot-coms.[4] As "The Industry Standard" recently argued, customer relationships are the new currency of the Internet. And, if e-commerce companies place a greater value on the customer data

---

[1] Jeffrey Rosen, *Why Internet Privacy Matters,* The New York Times Magazine, April 30, 2000, at 52.

[2] FTC, *Privacy Online: A Report to Congress,* May, 2000 at 13.

[3] *Id.* at 21.

[4] Saul Klein and Tara Lemmey, *Customer Relationships: The Net's New Currency,* The Industry Standard, Mar. 13, 2000, at 275.

they collect rather than on the customer relationships they are building, they risk squandering the enormous potential of the Internet, thereby relegating it to a secondary role in the American economy.[5]

The SECURE Act is mindful of the need to involve Congress in the issue of online privacy because of the industry's demonstrated inability to provide adequate and enforceable self-regulation. It is also mindful of the need to limit our involvement and shield the Internet from a system of rigid government regulations that would stifle its dynamic expansion and development. We must remember that during America's great economic revolutions, government has functioned best as a silent partner with industry, fostering growth, but also molding it in a socially responsible manner. Therefore, instead of regulating, the SECURE Act expands online freedom. It empowers consumers with the ability to protect themselves and make the informed choices that will render this legislation self-enforcing. It prevents a patchwork of state laws from miring the global growth of online commerce. And, it avoids the necessity to resort to extensive FTC oversight.

The SECURE Act is a beginning of a national dialogue on online privacy and does not represent an end product in addressing this issue. Senator's Burns, Wyden, Leahy, Hatch and now Hollings have also introduced important contributions to the debate. I look forward to working with them in reaching a consensus on the most appropriate legislative response to the privacy issues raised by the new technologies of the information age. Although I believe that entrepreneurial and innovative practices online are best served by minimizing the government's regulatory authority over the Internet, the FTC's report is pivotal to the development of appropriate public policy regarding online privacy. I am pleased that the FTC has officially acknowledged the need for online privacy standards with a statutory basis.

Again, I thank the Chairman for giving me the opportunity to participate in this hearing. I look forward to working with the Committee to reach conclusions that are balanced and fair and that give Americans a greater sense of confidence in the privacy of their personal information.

○

[5] *Id.*