S. HRG. 106–1147

S. 2928, S. 2606, AND S. 809—INTERNET PRIVACY CONCERNS

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

OCTOBER 3, 2000

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

U.S. GOVERNMENT PRINTING OFFICE

85–657 PDF WASHINGTON : 2004

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*
ANN CHOINIERE, *Republican General Counsel*
KEVIN D. KAYES, *Democratic Staff Director*
MOSES BOYD, *Democratic Chief Counsel*

CONTENTS

	Page
Hearing held on October 3, 2000	1
Statement of Senator Breaux	7
Statement of Senator Bryan	5
Statement of Senator Burns	3
Statement of Senator Cleland	53
Statement of Senator Gorton	5
Statement of Senator Hollings	2
Statement of Senator Kerry	63
Statement of Senator McCain	1
Statement of Senator Rockefeller	50
Statement of Senator Wyden	4
WITNESSES	
Cooper, Scott, Manager, Technology Policy, Hewlett-Packard Company	7
Prepared statement	10
Garfinkel, Simson, Cambridge, MA	20
Prepared statement	21
Rotenberg, Marc, President, Electronic Privacy Information Center	30
Prepared statement	33
Rubin, Paul H., Professor of Economics and Law, Emory University	56
Prepared statement	57
Vradenburg, George III, Senior Vice President for Global and Strategic Policy, America Online	14
Prepared statement	16
APPENDIX	
Cleland, Hon. Max, U.S. Senator from Georgia, prepared statement	71
Cooper, Scott, Hewlett-Packard Company, Manager, Technology Policy, prepared statement	71
Response to written questions submitted by Hon. Ernest F. Hollings to: George Vradenburg	75
Garfinkel, Simson L., letter dated October 3, 2000, to Hon. John McCain	77

S. 2928, S. 2606, AND S. 809—INTERNET PRIVACY CONCERNS

TUESDAY, OCTOBER 3, 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. I want to thank the witnesses for participating in today's hearing. As evidence of the importance of this issue, this is the third hearing the Committee has held since this summer on Internet privacy.

Today the Committee will hear testimony on the legislative proposals before the Committee dealing with Internet privacy. The purpose of this hearing is to begin the process of moving toward the enactment of legislation which would enable consumers to protect their privacy online.

The Federal Trade Commission in its recent report on online privacy recommended legislation to require the implementation of the four fair information practices of notice, choice, access, and security. The FTC found that, while voluntary efforts had advanced the issue of privacy, those efforts were failing to adequately protect privacy. Specifically, the Commission found that nearly 41 percent of random sites and 60 percent of the top 100 sites provided consumers with notice about their information practices and offered a choice about how that information is used. I agree we must work to enact legislation to enable consumers to protect their privacy. I am not convinced that we must mandate all of the four information practices to protect privacy.

Last July, Senators Kerry, Abraham, Boxer and I introduced the Consumer Internet Privacy Enforcement Act. The bill is focused around the two fundamental principles of notice and choice. It would ensure that consumers are informed of a website's information practices in a clear and conspicuous manner. It would also require websites to give consumers a simple method of exercising meaningful choices about how that information is used. By focusing on these two fundamental principles, I believe we strike the delicate balance between protecting privacy and imposing burdensome rules that do little to help consumers.

We may not all agree about the specific details of the legislative proposals, but we all agree that the time has come to enact legislation to protect consumers' privacy. Some of the proposals before the Committee go further than the bill my colleagues and I introduced. Some of the bills currently before Congress propose far less, such as a simple commission to merely study the issue. Regardless of the proposal, I think it's important we move forward through the difficult process of reaching compromise and forging legislation.

I look forward to engaging in this process as we move toward the next Congress, and I believe that next year we can report legislation from the Committee and work for its passage on the floor.

Again, I want to thank the witnesses for their testimony today.

Senator Hollings.

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

Senator HOLLINGS. Mr. Chairman, we have fiddle-faddled with this problem now for 5 years, and like you, I would have wished that they could have voluntarily regulated themselves. But as Newsweek, the business magazine—this is not Consumer Reports or the Consumer Federation—cites, and I read: "In short, self-regulation is a sham. The policies that companies have posted under pressure from the government are as vague and confusing as anything Lewis Carroll could have dreamed up. Again, if a business wants to collect information about a consumer's health, financials, or sexual orientation, it should ask them for permission first. This allows a Web surfer to opt-in."

That is why myself and the other cosponsors have introduced our bill after a complete study and 5 years of the FTC trying to get self-regulation. There is no doubt in a comprehensive field as the Internet that you are going to have to try to protect the privacy if you are going to protect the users of the Internet. This is not a government restriction against business. This is a government restriction to propagate the business in a proper fashion.

So, any bill that does not have the opt-in is just whistling Dixie. All these studies going back and looking and wondering and everything else of that kind. Mind you me, this is not asking those about your personal information that are not making it a business or not making a profit from it. On the contrary, this is those who really are making a business and a profit and money out of your own private information. I think we are going to have the opt-in, the opt-out, the security, and the availability of it if we are going to have a good bill.

We came back here last week and we were all in a heat over the proposition of advertising violence and not doing something about the violence itself after 30 years.

Now after 5 years, there are some that want to still study and everything else after the Federal Trade Commission has tried over the 5-year period. Their in-house studies, working with the industry, and everything else have found that you are going to have to have an opt-in provision.

Thank you.

The CHAIRMAN. Senator Burns.

Senator BURNS. I think Senator Wyden was before me.

Senator WYDEN. Go ahead.

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

Senator BURNS. Well, thank you, Mr. Chairman, I appreciate that, and I appreciate you holding this third hearing on privacy in a new digital economy.

While the Internet has offered us some amazing things, we have seen a lot of things happen, and it offers a lot of commercial opportunities to millions of Americans, the new information technologies have allowed the collection of personal information on an unprecedented scale. Many times this information is collected without the knowledge of consumers, but we also face that in our grocery stores and wherever we go to restaurants. And every time we do business with a credit card and even sometimes with cash, we are confronted with the same thing.

But what is particularly concerning to most of us is that information is collected without the knowledge of consumers. Online profiling poses particular concerns, especially those profiles that are merged with offline information to create massive, individualized data bases on consumers.

Given the continuing erosion of Americans' privacy, I am more convinced than ever that legislation is necessary to protect and empower consumers in the online world. Privacy is a bipartisan issue. The number of bills before this Committee is evidence of the high level of member interest in this important topic. Recently Senator Hollings and Senator McCain have introduced legislation in this area, and I look forward to working with them.

I would also like to thank my colleague, Senator Wyden of Oregon, for his hard work on the privacy issues. Well over a year ago, Senator Wyden and I introduced the Online Privacy Protection Act which was based on our shared view that while self-regulation should be encouraged, we need also to provide a strong enforcement mechanism to punish those people who would act in bad faith.

I have grown increasingly frustrated with the industry's continuing stance that no legislation is necessary, even in the face of overwhelming public concern. Many in the industry have claimed that our bill, the Burns-Wyden bill, goes way too far and that the time still is not right for privacy legislation. I want to reiterate my commitment to moving strong privacy legislation to protect consumers, whether industry agrees with it or not.

I commend the Federal Trade Commission for recognizing the industry has failed to produce progress and finally calling for legislation. The Commission's recent report to Congress reveals the extent of a stunning lack of consumer privacy on the Internet. Even among the 100 most popular websites, only 42 percent have implemented fair information practices to ensure consumer privacy, and among a broader random sample of all commercial websites, the number drops dramatically to 20 percent in compliance.

So, I remain open in working with you, Mr. Chairman, and Senator Hollings and Senator Wyden, and all of my colleagues on this Committee and the rest of the Senate and the Congress as we work

on this vital issue. I look forward to the testimony of the witnesses today, and I thank you very much.

The CHAIRMAN. Thank you.

Senator Wyden.

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

Senator WYDEN. Thank you, Mr. Chairman. I want to thank my friend from Montana for his kind words. He and I did, a year a half ago, introduce legislation. We note your bill, Mr. Chairman, Senator Hollings' bill. We have got a variety of good bills now before the Committee, and I would just make a couple of points at this time.

First, I just do not think it is right for the Congress to wait until there is an Exxon Valdez of privacy, and I am very concerned, given the fact that we have some who are certainly not rushing to embrace these voluntary programs that that is going to happen.

The reason that I feel so strongly about it is when you look at this Committee's work—and I am very proud of what we have done on a bipartisan basis, the Internet Tax Freedom bill, for example, the law that went into effect yesterday, the Digital Signatures law. What we have been able to do in the last couple of years is to begin to write the ground rules for the new economy, and we have done it in a way that has made sense for business and made sense for consumers and helped to inspire confidence in these new economic opportunities that revolve around the Internet. You have an Exxon Valdez of privacy and that will, to a great extent, drain much of the confidence out of the exciting things that are taking place in our country. So, it is critically important that we move forward, do it in a bipartisan way.

I would wrap up with just a couple of additional comments. First, Mr. Chairman, I do feel strongly that on a bipartisan basis we ought to figure out a way to embrace these four key principles that the Federal Trade Commission has called for in their proposal. They have said that it is important to include notice and choice and access and security. We do have differences of opinion in this Committee with respect to these four principles. I would hope that we would work with industry on a bipartisan basis and consumer groups and develop a plan that does incorporate those four key principles.

Finally, with respect to the nature of the information, it does seem to me that the American people, when you are talking about their health and their financial information, sensitive, personal information, want in some way to give explicit permission before it is used. You can walk into any coffee shop in this country and that is what people think ought to be done.

At the same time, there are scenarios that seem almost absurd if you carry this to absolutes. For example, if somebody subscribes to Newsweek for 20 years, it seems kind of preposterous to require that the Newsweek company send them a notice asking them permission to send them another notice to sign up for the 21st year. So, the nature of this information is very key, and I hope that with respect to the financial and health information that we can develop a plan that is in line with the expectations of the American people.

Mr. Chairman, again I thank you. I think this is an important week. That Digital Signatures bill that this Committee led the effort on is going to be a revolution in the private sector economy. Now it is time for us to join forces again in the privacy arena, and I look forward to working with you and our colleagues to do that.

The CHAIRMAN. Senator Gorton.

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

Senator GORTON. Mr. Chairman, as others have said, this is your third hearing on a vitally important subject. You have introduced a bill yourself that seems to me to have great merit, as have two other Senators or groups of Senators here, including the bipartisan approach that Senator Wyden and Senator Burns have.

I think each of those show how important this issue is. I think each shows the absolute necessity for us to do something here. The other approaches have not worked.

I want to echo Senator Wyden in saying that it seems to me that this is a field in which we do need to be working together. There are four basic elements that we must consider. The degree to which we have got to legislate on each of them is certainly a matter for negotiation. But as is the case with so many other issues in this Committee, it is not going to break down on partisan lines by any stretch of the imagination. Whether we are going to finish something in the next 2 weeks I think is questionable, highly questionable, but that we should be working, at the very least, toward doing something early in the next Congress in my view is very important.

You have helped give us the ground for that. You have helped us focus on the proposition that we should not have significant information about people being used without their knowledge and without their consent, which is exactly the situation we find ourselves in today. Solving that problem as promptly and as justly as possible, both taking advantage of the tremendous opportunities given us by the Internet, but protecting people against things that they do not want and do not know is very, very important. It seems to me that we are moving toward a consensus on this Committee and that you are helping us through this hearing in doing so.

The CHAIRMAN. Thank you, Senator Gorton.

Senator Bryan?

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

Senator BRYAN. Mr. Chairman, I would like to thank you for calling today's hearing on this important issue of Internet privacy.

The right to privacy is constitutionally recognized by the Supreme Court and is a reflection of our citizenry's long-held expectation that they should be able to engage in a wide range of day-to-day activities with a significant degree of autonomy and independence.

The Internet presents new challenges, as well as 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 enti-

ties to track the flow of this information with relative ease, poses serious privacy concerns for many consumers.

By way of example, the recent revelation involving the dynamic pricing strategy employed by Amazon.com is further evidence of how consumer privacy is threatened on the Internet.

A recent survey showed that 92 percent of consumers are concerned about the misuse of their personal information online. Only 15 percent of those polled by Business Week earlier this year believe that the government should defer to voluntary industry-developed privacy standards, and as recently as August, the Pew Research Foundation reported that 86 percent of those surveyed supported an opt-in requirement as a necessary component of any company's privacy policy.

I agree with the recommendations contained in the Federal Trade Commission's latest report on online privacy, but the time has come for Congress to establish a baseline standard for the protection of consumer privacy on the Internet.

Earlier this year, I joined with our distinguished ranking member, Senator Hollings, in introducing privacy legislation that largely tracks the recommendations contained in the FTC report. This legislation builds upon the framework established by the Children's Online Privacy Protection Act, which I was privileged to sponsor and which enjoyed the unanimous approval of all Members of this Committee. As you know, it went into effect earlier this year in April. It embodies the four widely accepted fair information practices of notice, choice, access, and security for the collection of personally identifiable information about consumers online.

It is important to note that the Children's Online Privacy Protection Act, which as I said, enjoyed the unanimous support of Members of this Committee in the last Congress, contains an opt-in requirement in the form of verifiable parental consent. This requirement means that a website operator must make reasonable efforts to ensure that before personal information is collected from a child, a parent of the child receives notice of the operator's information practices and consents to those practices. This legislation also had the near unanimous support of the Internet industry, including the industry representatives that are testifying before the Committee today.

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.

But technological advancement should not be viewed as a substitute for strong legal protections. I understand the industry's concern 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 that that occurred in the offline world with the credit card industry in the 1970's. And I am hopeful, Mr. Chairman, that this Committee will continue to endeavor to enact a responsible bipartisan piece of legislation that adequately protects consumer privacy online in a manner that does not unduly burden the growing e-commerce market in America.

The CHAIRMAN. Senator Breaux.

STATEMENT OF HON. JOHN B. BREAUX,
U.S. SENATOR FROM LOUISIANA

Senator BREAUX. Well, thank you, Mr. Chairman. I am sure everything has been said that needs to be said except from our panel of witnesses.

Let me just add my congratulations to you for focusing in on what many consumers feel is one of the most important concerns that they have in today's modern society; that is, what happens to their personal information when they sit down in front of the Internet and use it for legitimate purposes. I think that there has been a growing fear of even using the Internet because of the possibility that personal information will be disseminated to those who seek to use it for purposes that the owner of that information has not agreed to.

I think a solution to this problem is a win-win, both from the business community who seeks to take advantage of the services allowed by the Internet operations, as well as a win for those who are concerned about their own personal information being disseminated, in some cases sold to others, third parties in particular.

Time is running out but I think that we have laid the groundwork for what needs to be done in the next Congress, and I look forward to working with the Chairman in order to do that.

The CHAIRMAN. Thank you.

Mr. Scott Cooper, Mr. George Vradenburg, Mr. Simson Garfinkel, and Mr. Rotenberg. Mr. Cooper, Manager of Technology Policy of the Hewlett-Packard Company, welcome.

STATEMENT OF SCOTT COOPER, MANAGER, TECHNOLOGY POLICY, HEWLETT-PACKARD COMPANY

Mr. COOPER. Mr. Chairman and Members of the Committee, Hewlett-Packard appreciates this opportunity to testify today at this important hearing on privacy. My name is Scott Cooper and I am Manager of Technology Policy for HP.

We at HP believe that the Information Age will provide numerous tools that will empower consumers and allow them to participate with confidence in the global electronic marketplace. Consumers already have access to a tremendous amount of information to help them negotiate prices, terms and conditions. They are no longer limited in where they shop, when they shop, or with whom they do business.

But these benefits cannot be realized if consumers are concerned about how their personal information is treated online.

While industry self-regulation is not the complete solution, we believe the private sector has done a pretty good job of responding to privacy concerns during the seminal period of the growth of electronic commerce. It is sometimes easy to forget how recent a phenomenon Internet commerce is. Five years ago, almost nothing was bought or sold online. So, we are still finding our way in this new environment. From that perspective, the efforts to date by businesses to meet consumer privacy concerns have been impressive. HP believes that self-regulation and credible third party enforcement, such as the Better Business Privacy Seal program, are the

single most important steps that businesses can take to ensure that consumer privacy will be respected and protected online.

As an example of our concern on this issue, HP is making an offer we hope will encourage many other companies to join HP as members of the Better Business Bureau Privacy Seal program. For the past four months, HP has paid the application fees of start-up companies identified by the Better Business Bureau to join the BBB*OnLine* Privacy Seal program.

This offer reflects, we believe, a commitment to address consumer privacy concerns and, in fact, the BBB program has been singled out by the European Commission as the kind of privacy program that gives them confidence that an American safe harbor will meet European adequacy standards on privacy.

And just two weeks ago, HP's CEO, Carly Fiorina, joined with Michael Dell of Dell Computer to send a joint letter to their fellow Fortune 500 CEO's requesting that they also join the BBB Privacy Seal program.

But even with all these self-regulatory efforts by HP and other companies, it is unlikely that the majority of commercial websites will post consumer-friendly, easily readable privacy policies or join privacy programs such as the BBB, at least in the short run.

And unfortunately, there is a perverse legal incentive for commercial websites not to post a clear and conspicuous privacy notice. Currently if a website posts a privacy policy or posts a third party privacy seal and then fails to live up to that policy, it is then liable for enforcement by the FTC for having committed a deceptive act. If the website does not state a policy or couches that policy in so many disclaimers and other confusing legalese in order to limit liability, then consumers will not have the material information they need to decide whether they wish to do business with that site.

Hewlett-Packard has argued for some time now that consumers deserve to have the necessary material information about a website's privacy policy in order for them to make an informed choice whether they want to do business with that site. We have advocated that key consumer right is that of disclosure, that is requiring that all commercial websites clearly and conspicuously state what that website does with personal information. Consumers can then decide whether they want to continue a transaction with that website or go to another that has a privacy disclosure more to their liking.

HP believes that clear and conspicuous privacy disclosure is not only the right thing to do for consumers; it is also the right thing to do for businesses if they want to grow and serve their customers in the Internet environment. If consumers in the marketplace decided that privacy is important to them—and they have—then the competitive advantage will be with those sites that have a more consumer-friendly privacy policy.

Hewlett-Packard, therefore, strongly commends the original cosponsors of S. 2928, Senators McCain, Kerry, Abraham, and Boxer, for their leadership in protecting the privacy of consumers who use the Internet. We look forward to substantive legislative hearings in the next Congress to flesh out the details of this proposal, but for the most part, we think the authors have it just about right:

1. Clear, conspicuous and easily understood disclosure requirements are key. We also commend the authors for including a safe harbor section that recognizes the importance of self-regulatory third party seal programs that have been approved by the FTC.
2. Recognizing the importance of empowering state attorneys general to protect their citizens' privacy through national uniform regulations, while preserving the right of the FTC to intervene when it feels necessary.
3. A study and report back to Congress by the National Academy of Sciences on a series of complex but important issues that must be resolved in order to ensure that the benefits of the Information Age are not distorted or unrealized. These include:
   a. An analysis of the benefits and risks inherent in the use of personal information for both consumer empowerment and continued growth of electronic commerce;
   b. an important examination of existing differences between the collection of information online and offline, an examination we hope will lead to greater harmonization between the two;
   c. an analysis of the benefits and risks of providing various levels of consumer access to business databases and;
   d. an examination of the security of personal information collected online.

It is our view that the Information Age cannot move forward without these questions being answered. At the same time, the importance of getting the answers right precludes any overly precipitous rush to judgment. Hewlett-Packard does not believe that balancing consumer confidence and market growth is a zero sum game. We are confident that the National Academy of Sciences will present Congress with a reasoned set of recommendations of where further policymaking may be necessary and also where it may not. Congress should not be asked to legislate on this complex, vital area of our economy based on anecdotal evidence. Nor should a reasoned debate be limited by proscriptions that, given enough time, the marketplace will ultimately supply all answers.

We would welcome the public debate that will be spawned by the studied recommendations of the National Academy of Sciences and believe it is by far the best way to discover, as Senator Breaux said, win-win answers for consumers and the economy.

And finally,

4. we think it important that the Internet and electronic commerce be treated as an interstate issue. We agree with the authors of 2928 that we must develop national uniform privacy policies.

We also think that S. 809 has also defined the right goals for consumer privacy protections, and we would like to continue to work with Senator Burns' and Senator Wyden's offices to find industry consensus on how we can achieve workable solutions for such issues as opt-in and access.

We also think S. 2606 has raised many of the right issues for consumer confidence, including clear and conspicuous disclosure. Other sections of S. 2606 raise issues that deserve further study,

and others, such as section 303, the Private Right of Action, may be inappropriate as a solution for an issue that we believe we can find agreement and consensus solutions between consumers, businesses, and policymakers.

Current concerns about consumer confidence must not be allowed to turn into barriers for empowering consumers through global electronic commerce. Hewlett-Packard believes that this hearing is an important step in the right direction, and we welcome the opportunity to work with this Committee in the development of national policies governing the collection and use of personal information.

I would be pleased to answer any questions you all may have.

[The prepared statement of Mr. Cooper follows:]

PREPARED STATEMENT OF SCOTT COOPER, MANAGER, TECHNOLOGY POLICY, HEWLETT-PACKARD COMPANY, WASHINGTON, DC

Mr. Chairman and Members of the Committee. Hewlett-Packard appreciates this opportunity to testify today at this important hearing on privacy. My name is Scott Cooper, and I am Manager for Technology Policy for HP.

We at HP believe that the Information Age will provide numerous tools that will empower consumers and allow them to participate with confidence in the global electronic marketplace. Consumers already have access to a tremendous amount of information to help them negotiate prices, terms and conditions. They are no longer limited in where they shop, when they shop, and with whom they do business.

But these benefits cannot be fully realized if consumers are concerned about how their personal information is treated online.

While industry self-regulation is not the complete solution, we think the private sector has done a good job of responding to privacy concerns during the seminal growth of e-commerce. It is sometimes easy to forget how recent a phenomenon Internet commerce is. Five years ago, almost nothing was bought or sold online. So we are still finding our way in this new environment. From that perspective, the efforts to date by businesses to meet consumer privacy concerns have been pretty impressive. And HP believes that self-regulation and credible third party enforcement—such as the Better Business Bureau privacy seal program—is the singlemost important step that businesses can take to ensure that consumers' privacy will be respected and protected online.

As an example of our concern on this issue, HP is making an offer that we hope will encourage many more companies to join HP as a member of the Better Business Bureau Privacy Seal program. For the past four months HP has paid the application fees of start-up companies—identified by the BBB—to join the BBB*OnLine* Privacy Seal program. We have also offered limited, free consultation from HP's Privacy Managers to help each company get started.

This offer reflects, I believe, our commitment to addressing consumer privacy concerns, and in fact, the BBB program has been singled out by the European Commission as the kind of privacy program that gives them confidence that an American 'safe harbor' will meet European adequacy standards for privacy.

And just two weeks ago, HP's CEO, Carly Fiorina joined with Michael Dell of Dell Computer to send a joint letter to their fellow "Fortune 500" CEO's requesting that they also join the BBB privacy seal program.

Even with all these self-regulatory efforts by HP and other companies, it is unlikely that the majority of commercial websites will post consumer-friendly easily-readable privacy policies, or join privacy programs such as the BBB; at least in the short run. And unfortunately, there is a perverse legal incentive for commercial websites *not* to post a clear and conspicuous privacy notice. Currently, if a website posts a privacy policy or posts a 3rd-party privacy seal and fails to live up to that policy, then it is liable to enforcement from the FTC for having committed a deceptive act. If the website does not state a policy, or couches that policy in so many disclaimers and other confusing legalese in order to limit liability, then consumers will not have the material information they need to decide whether they wish to do business with that website.

And consumers have expressed their dissatisfaction with the ability of self-regulation *alone* to provide necessary consumer confidence on privacy. In a recent Business Week/Harris Poll, 92 percent of Net users expressed discomfort with sites shar-

ing personal information with other sites. And 57 percent of those respondents to the survey said that government should pass laws on how personal information is collected.

Hewlett-Packard has argued for some time now that consumers deserve to have necessary material information about a website's privacy policy in order for them to make an informed choice whether they wanted to do business with that site. We have advocated that a key consumer right is that of disclosure; that is, requiring that all commercial websites—clearly and conspicuously—state what that website does with personal information. Consumers can then decide whether they want to continue a transaction with that website, or go to another that has a privacy disclosure more to their liking.

Hewlett-Packard was therefore supportive of efforts by Congressman Boucher and Goodlatte—the co-chairs of the House Internet Caucus—to protect consumer privacy through greater disclosure. And in May of last year, they introduced H.R. 1685 which includes as Title III an "Online Privacy Protection" section that requires commercial websites to "clearly and conspicuously provide notice of its collection, use and disclosure policies" with enforcement authority to the Federal Trade Commission.

HP believes that clear and conspicuous privacy disclosure is not only the right thing to do for consumers; it is also the right thing for businesses if they want to grow and serve their customers in the Internet environment. If consumers in the marketplace decide that privacy is important to them—and they have—then the competitive advantage will be with those sites that have more consumer-friendly privacy policies.

Hewlett-Packard thus strongly commends the original co-sponsors of S. 2928, Senators McCain, Kerry, Abraham and Boxer, for their leadership in protecting the privacy of consumers who use the Internet. We look forward to substantive legislative hearings in the next Congress to flesh out the details of this proposal; but for the most part we think the authors have it just about right:

1. "[C]lear, conspicuous and easily understood" disclosure requirements are key. We also commend the authors for including a "Safe Harbor" section that recognizes the importance of self-regulatory 3rd party seal programs that have been approved by the FTC.
2. Recognizing the importance of empowering state attorneys general to protect their citizens privacy through national uniform regulations; while preserving the right of the FTC to intervene when it feels necessary.
3. A study and report back to Congress by the National Academy of Sciences on a series of complex but important issues that must be resolved in order to ensure that the benefits of the Information Age are not distorted or unrealized. These include:
    a. An analysis of the benefits and risks inherent in the use of personal information for both consumer empowerment and continued growth of the electronic marketplace;
    b. an important examination of existing differences between the collection of information online and offline; an examination we hope will lead to greater harmonization between the two;
    c. an analysis of the benefits and risks of providing various levels of consumer access to business databases;
    d. and an examination of the security of personal information collected online.

It is our view that the Information Age cannot move forward without these questions being answered. At the same time, the importance of getting the answers *right* precludes any overly-precipitous rush to judgement. Hewlett-Packard does not believe that balancing consumer confidence and market growth is a zero-sum game. We are confident that the National Academy of Sciences will present Congress with a reasoned set of recommendations of where further policymaking may be necessary; and also, where it may not. Congress should not be asked to legislate in this complex, vital area of our economy based on anecdotal evidence. Nor should a reasoned debate be limited by proscriptions that given enough time, 'the marketplace' will ultimately supply all answers.

We would welcome the public debate that would be spawned by studied recommendations of the National Academy of Sciences and believe that that is by far the best way to discover "win-win' answers for consumers and the economy.

And finally,

4. we think it important that the Internet and electronic commerce be treated as an interstate issue. We agree with the authors of S. 2928 that we must develop national, uniform privacy policies.

But in order to truly earn the trust on consumers, we cannot stop here, We also need to expand ongoing efforts to ensure that the *global* electronic marketplace is a clean, well-lighted venue for both consumers and businesses. For example, consumers need to have confidence that when they do business across national borders, that there will be a redress system in place should anything go wrong with the transaction.

HP is working with 70+ businesses from around the world through the Global Business Dialogue for electronic commerce to develop worldwide consensus standards on consumer redress systems; what are called alternative dispute resolution mechanisms, or ADR. In this effort we are working with consumer groups, government bodies such as the FTC and the European Commission to ensure that consumers and businesses will quickly, fairly and cheaply resolve complaints related to online transactions.

Current concerns about consumer confidence must not be allowed to turn into barriers to empowering consumers through global e-commerce. Hewlett-Packard believes that S. 2928 is a significant step in the right direction, and we welcome the opportunity to work with this Committee in the development of national policies governing the collection and use of personal information.

I would be pleased to answer any questions that you may have.

Hewlett-Packard Proposal on Privacy Disclosure

1) Industry self-regulation and credible third party enforcement is the best model for developing the necessary trust that private data will be respected and protected online. It is unlikely however that the majority of websites will post privacy policies in at least the short run. And unfortunately. there is a perverse legal incentive for commercial websites not to post a privacy statement. Currently, if a website posts a privacy policy and fails to live up to that policy, it is liable to enforcement from the FTC for having committed a deceptive act. If the website does not state any policy, it is not legally vulnerable because no deception can be inferred. Therefore while the largest websites will probably post privacy statements, the large majority of sites may not: and that makes industry vulnerable to intrusive regulatory initiatives.

2) One way to deal with that problem would be through disclosure: that is requiring that *all* commercial websites—clearly and conspicuously—state what that website does with personal information. A disclosure requirement would not require a website to do anything other than it is currently doing; it would only require that the website inform consumers what it is that they do with personal information. Consumers could then decide whether they want to continue a transaction with that website, or go to another that has a privacy disclosure more to their liking. If consumers in the marketplace decide that privacy is important to them, then the competitive advantage will be with those sites that have more stringent privacy policies.

3) This concept of "material information" is a basic concept of U.S. consumer protection law. (See the "FTC Policy Statement on Deception".) Simply stated, consumers have the right to information that is essential for them to make an informed choice about a product or service. To fail to make such information available to consumers is a deceptive act. Through rule or case law, this 'material information' concept is a basis for US advertising regulation, and in a number of other areas:

Telemarketing: It is deceptive to fail to verbally disclose (in a clear and conspicuous manner) costs, material restrictions, refund policies, prize odds, material costs, etc.

900-Number (Pay-per-Call): It is deceptive to fail to verbally disclose (in a free preamble) the service to be provided, cost per minute, and other fees created by the call. (The 'clear and conspicuous' disclosures also carry over into print and TV ads for 900#s)

Used Car Warranties: It is deceptive not to conspicuously post on every used car a sticker that states in writing what warranty (if any) a dealer offers on a used car.

Acknowledging that consumers have the right to know how their personal information may be used is a pro-consumer initiative that will give consumers and businesses greater certainty and confidence in undertaking negotiations on the Internet.

(All documents cited can be found on the FTC website at *www.ftc.gov*)

September 15, 2000

<<First__Name>> <<MI>> <<Last__Name>>
<<Company__Name>>
<<Address>>
<<City>>, <<ST>> <<Zip__Code>>

Dear <<First__Name>>:

We are writing to enlist your company's participation in meaningful and credible self-regulation to protect your customers privacy on the Internet. BBB*OnLine,* the Internet subsidiary of the Council of Better Business Bureaus, was developed to promote trust and confidence on the Internet. Eighteen major corporations sponsor, serve on the Board, and helped build the BBB*OnLine* Privacy Program (a list of these companies is attached.) The goal was to build the most comprehensive and least expensive privacy trustmark so that businesses could demonstrate their commitment to adhere to their online privacy notices.

The recent "Safe Harbor" agreement covering online transfers of personal data reached between the U.S., Department of Commerce and the European Union would have not been possible without BBB*OnLine*'s credibility and reputation. This agreement will allow personal data transfers from European Union citizens to BBB*OnLine* participants and others meeting the safe-harbor provisions. If you do not meet these "Safe Harbor" provisions your company may have difficulty transferring data from Europe (including from your European operations) to the U.S. If these transfers are not possible this could obviously take a staggering negative toll on US—EU commerce.

In addition, BBB*OnLine* has recently announced a joint trustmark with the government-sponsored privacy seal program in Japan operated by the Japan Information Development Processing Center (JIPDEC) This joint venture will allow BBB*OnLine* seal holders to qualify for Japan's privacy seal and JIPDEC seal holders in Japan to qualify for the BBB*OnLine* seal. This option is unavailable from any other trustmark program and is another example of the global reach of BBB*OnLine*'s reputation as the most comprehensive and credible form of online privacy self regulation available.

The U.S. Congress, state legislatures, and federal regulatory agencies are continuing their efforts to regulate online privacy. While they recognize the value of the BBB*OnLine* Trustmark program, they highlight that not enough businesses have made a commitment. There is still time to send a significant message to legislators and regulators that businesses are committed to protecting consumer privacy through self regulation by participating in the BBB*OnLine* Privacy Program.

This letter is to urge <<Company__Name>> to apply and qualify for the BBB*OnLine* Privacy seal to demonstrate your commitment to self-regulation. The cost is low and the benefits to your company and business in general are great. Together we can send a strong message that industry is willing to accept the online privacy challenge. For information on the BBB*OnLine* Privacy Program please have your staff contact Ms. Mercedes Lemp at 703.247–3661, email her at Mlemp@lcbbb.bbb.org or look at BBB*OnLine*'s website at *www.bbbonline.org.*

Sincerely,

CARLY FIORINA,
CEO,
Hewlett Packard Company.

MICHAEL DELL,
CEO,
Dell Computer Corporation.

BBB*OnLine* Founding Sponsors

America Online
Ameritech
AT&T Corp.
Bank of America
Dun & Bradstreet
Eastman Kodak Company
GTE
Hewlett-Packard Company
IBM Corporation

Intel Corporation
Microsoft Corporation
The Procter & Gamble Company
Reed Elsevier Inc.
Road Runner
Sony Electronics
US WEST
VISA
Xerox Corporation

The CHAIRMAN. Thank you, Mr. Cooper.
Mr. Vradenburg, welcome.

STATEMENT OF GEORGE VRADENBURG, III, SENIOR VICE PRESIDENT FOR GLOBAL AND STRATEGIC POLICY, AMERICA ONLINE

Mr. VRADENBURG. Thank you, Mr. Chairman and Members of the Committee, and I thank you very much for the opportunity to testify here this morning on this important issue.

As consumers demand the power and convenience of the PC on their TV sets and the mobility to take the Internet with them on their wireless and other personal devices, it is becoming clear that online interactivity will become an integral and seamless aspect of how we live in a modern society. This rapid consumer-driven environment we live in in the Internet requires industry to know more about our consumers than in the past in order to serve them better, at lower cost, and with the products and services they want. This is all to the good for consumers, for our economy, and for our society. But we must recognize that we in business, and you as government, have a greater responsibility than in the past for the proper treatment and handling of consumers' personal information.

With that in mind, we are happy to be participating in this important national debate. We believe that we have reached a critical point at which industry and government must take the next step together in order for us to get where we need to be on privacy.

AOL is proud to have been a leader in a wide range of industry-led and industry-based efforts to address privacy issues. We were founding members of the Online Privacy Alliance and NetCoalition and are strong supporters of TRUSTe, BBB*OnLine,* the DMA, and other efforts to set high corporate standards for privacy protection. And we have worked in our role as co-chair of the Global Business Dialogue on Electronic Commerce to promote strong privacy policies around the world because we believe this particular issue knows no boundaries, no borders, and must be addressed with its global impact in mind.

Within our own company, we have worked hard to develop privacy policies based on the input we have received from our members over the years. We have described our privacy policy in detail before this Committee in recent testimony, so I will not discuss all the specifics here again. I would just emphasize that the cornerstone of our policy is that we clearly explain to our members what information we collect, why we collect it, how they can exercise choice about the use and disclosure of that information.

We at AOL are proud of the steps we have taken to create a privacy friendly environment online for our members. We have adopted these policies because our business, more than ever, requires us

to respond to consumer demands. We take privacy seriously in order to build consumer and our own member trust in the medium. And we know that many other online businesses feel exactly the same way.

The progress that industry has made in recent months is real. One thing the FTC Online Privacy Report last May clearly shows is that the proportion of commercial websites posting privacy policies has skyrocketed in less than 3 years from fewer than 14 percent to over 90 percent. Unbelievable progress for an industry that barely existed just a few years ago. And the rapid adoption and use of the Internet in this country, it seems to me, is a symbol that in fact consumers are taking to this new medium with a greater rapidity than virtually any medium in history, suggesting that in fact consumer confidence not only is high but growing in this medium.

Despite this remarkable progress, it is clear from the level of public concern that still more needs to be done in order to broaden consumer confidence in the online medium. Although the industry has come a long way in creating and promoting best practices in protecting consumer privacy online, we think legislation may now be able to play an important role in setting baseline standards for privacy protection and ensuring that companies all play by the same rules.

How do we decide what those baseline standards should be? Examining this issue in light of the needs of our own members, we have come to realize that the success that industry has attained thus far in the area of privacy protection is largely attributable to market-led initiatives premised on notice and choice. The fundamental principle of privacy protection is to inform consumers of our personal information handling practices—to give them the ability to determine how that information may be collected, used and disclosed. Only in that way can we both reflect the diversity of suppliers in our industry and the wide diversity of consumer privacy preferences in society.

As Congress turns its full attention to this issue next year, we at AOL would, therefore, ask the Members of this Committee to base their legislative initiatives on these key principles of notice and choice, backed up by strong enforcement authority. This type of solution will allow companies to determine the most effective ways to implement notice and choice under their particular business models, while ensuring that companies do indeed comply with those requirements. In today's online world, consumer preferences can vary greatly from user to user, and we are in need of a legislative approach that will give consumers the flexibility to express those preferences on an ever-expanding variety of platforms and devices, from their PC's to their televisions, to their hand-held wireless devices.

We think that the legislation that you, Mr. Chairman, have cosponsored is a good example of a legislative approach that does set a baseline standard for notice and choice backed by strong enforcement, under which market-driven initiatives and technology innovation can continue to blossom, but providing additional confidence to consumers that they are, in fact, being honestly informed of what is being done with their personal information and that they have choices in how that information is used.

So, we commend you, Mr. Chairman, along with your cosponsors, Senators Abraham, Kerry, and Boxer, for their efforts in drafting this bill which would ensure that all companies live up to these important principles by giving the FTC clear authority to enforce the notice and choice requirements.

We are also pleased that other Members of this Committee have recognized the importance of addressing this issue, most notably Senators Hollings, Wyden, Burns, and Bryan, with whom we have worked very closely in adopting the Children's Online Privacy Protection Act. We look forward to working with all Members of this Committee in the next Congress to develop privacy legislation that will respect what we believe to be important principles of notice and choice.

We recognize 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 the many benefits that this medium has to offer. As the Committee continues its work on this issue next year, we urge you to consider the risks of an over-regulatory approach and the need for a solution to this issue that is flexible enough to sustain both diverse business models and to respond to diverse consumer preferences.

We must also encourage user-friendly consumer interfaces. That is, we must emphasize the importance of easy-to-use, easy-to-find, easy-to-read policies of choice and to develop in the marketplace a wide variety of choice techniques and technologies.

We commend the efforts of all the Members of this Committee. We look forward to working with you next year to build an effective privacy solution that will work for all of us. Thank you, Mr. Chairman.

[The prepared statement of Mr. Vradenburg follows:]

PREPARED STATEMENT OF GEORGE VRADENBURG, III, SENIOR VICE PRESIDENT FOR GLOBAL AND STRATEGIC POLICY, AMERICA ONLINE, DULLES, VA

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 proposed legislative responses to the issue of online privacy.

From the very beginning, we at AOL realized that this medium would not grow, and our company would not succeed, unless our members were confident in their privacy and security online. That's why protecting our members' privacy has always been one of our top priorities at AOL and why we have dedicated significant time, energy, and resources to establishing one of the industry's strongest privacy policies and educating our members about this issue.

Online privacy has gained increasing attention in recent months, as the Internet has become a central part of the lives of more and more Americans. As consumers demand the power of the PC on their TVs, the convenience of interactivity on their TVs, and the mobility to take the Internet with them on their wireless and other personal devices, it is becoming clear that Internet-oriented interactivity will become an integral and seamless aspect of how we live in a modern society. This rapid, consumer-driven environment requires industry to know more about their consumers than in the past in order to serve them better and at lower cost and with the products and services they want. Gone are the days when a manufactured good was delivered through a tiered distribution system into the hands of distant and anonymous customers. In the future, many services will be delivered completely online and the service provider and customer will have an almost intimate relationship. In that environment, businesses will be under increasing pressure to be responsive but will also be necessarily entrusted with more personal information about their customers. This is all to the good . . . for consumers, for our economy and for our society. But in that environment we, as a society, must recognize that businesses will have a greater responsibility than in the past for the proper treat-

ment and handling of customer's personal information, and for ensuring that consumers are fully informed about just what corporate policies and practices are. With that in mind, we are happy to be participating in this important national debate, and we believe that we have reached a critical point at which industry and government must take the next step together in order for us to get to where we need to be on privacy.

AOL is proud to have been a leader on a wide range of industry-based efforts to address privacy issues. We were founding members of the Online Privacy Alliance and NetCoalition and are strong supporters of TRUSTe, BBB*OnLine*, the DMA, and other efforts to set a high corporate standard for privacy protection. We also were an early supporter of P3P, a technology being developed by the World Wide Web Consortium that will empower consumers to set their own privacy preferences as they surf the Web. And we have worked in our role as Co-Chair of the Global Business Dialogue on Electronic Commerce (GBDe) to promote strong privacy practices by companies around the world, because we believe that the issue of privacy knows no borders and must be addressed with its global impact in mind.

Within our own company, AOL has worked hard to develop privacy policies based on the input we've received from our members over the years. Because consumers want to control their own privacy—rather than having their privacy options dictated by government or private industry—we've created a privacy policy that clearly explains to our members what information we collect, why we collect it, and how they can exercise choice about the use and disclosure of that information. We have described our privacy policy in detail in recent testimony before this Committee, so I will not discuss all of the specifics again here. I would just emphasize that the cornerstone of our policy is that we give our members clear choices about whether and how we use their personal information, we make those choices easy to find and easy to exercise, and we make sure that our members are well informed about what those choices are.

AOL's privacy commitment is company-wide. We have a designated official within the company who is devoted to ensuring privacy compliance among all of our brands, and we have integrated privacy criteria into the review process for new products. We also make sure that our policies are well understood and properly implemented by our employees. We require all employees to agree to abide by our privacy policy, and we limit employee access only to member information needed for their jobs.

AOL takes extra steps to protect the safety and privacy of children online. To protect our youngest members, 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. 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 closely with Senator Bryan, Chairman McCain, the FTC, and key industry and public interest groups to help pass and implement the Children's Online Privacy Protection Act (COPPA), and we believe the enactment of this bill was a major step in the ongoing effort to make the Internet safe for children.

Because the best privacy protection is an informed consumer, we have dedicated significant efforts to educating our members about the steps they can take to protect their own privacy online. Through Steve Case letters, in-house advertisements, and industry-wide public service campaigns, we have given tens of millions of users helpful tips about keeping their personal information secure. For instance, we encourage our members to check to see whether every site they visit on the Web has posted a privacy policy and to review those policies before giving any information or purchasing any products on those sites. We also help them learn how to protect their passwords and personal information and avoid falling for scams or downloading viruses.

Additionally, we have developed tools to help all Internet users protect their privacy when they surf the Web. Netscape, which is part of the AOL family, has one of the strongest commitments to privacy in the industry, and the newest version of the Netscape browser clearly demonstrates that commitment. Netscape 6.0, which is now in a beta testing phase, includes an exciting new tool called the "Cookie Manager," which allows users to control the amount of passive information that is collected about them by other companies when they surf the Net. Through that tool, consumers are able to view, edit, or delete any or all of the cookies that are placed on their computers by the websites that they visit; and they can choose for themselves which websites they will accept cookies from and which websites they won't.

Although AOL does not track the movements of our members when they surf the Web, we believe that it is important, given the recent concerns raised about the issue of "online profiling," to give consumers the ability to control what information they disclose online wherever they go on the Internet. The Netscape Cookie Manager is a timely and effective way to empower consumers to set their own privacy preferences.

We at AOL are proud of the steps we've taken to create a privacy-friendly environment online for our members. We are also 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 hundreds of business partners to guarantee our members the highest standards of privacy and customer satisfaction when they visit e-commerce sites through AOL. Under that program, AOL requires every merchant doing business on AOL to adhere to strict consumer protection standards and privacy policies as rigorous as our own.

We've adopted these policies because our business, more than ever, requires us to respond to consumer demands and take privacy seriously in order to build consumer trust in the medium. And we know that many other online businesses feel exactly the same way. That's why AOL helped form the Online Privacy Alliance 2 years ago. And that's why AOL and NetCoalition.com, a group representing some of the largest and most active online companies, sent a letter to 500 CEOs earlier this year encouraging them to post comprehensive privacy policies based on 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 online privacy report last May clearly shows is that the proportion of commercial websites posting privacy policies has skyrocketed in less than 3 years from less than 14 percent to over 90 percent—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.

Despite this remarkable progress, it is clear from the level of public concern over privacy that more still needs to be done to broaden consumer confidence in the online medium. Although many industry leaders—including AOL—have worked hard to build their brands on privacy protection, too many online users are still worried about how their information will be collected and used by other companies doing business online. We believe, therefore, that it is time for government and industry to move forward together to expand consumer confidence and protect consumer privacy. Although the industry has come a long way in creating and promoting best practices for protecting consumer privacy, we think that legislation can play an important role in setting baseline standards for privacy protection and ensuring that all companies play by the same rules.

But how do we decide what these baseline standards should be? Examining this issue in light of the needs of our own members, we have come to realize that the success that industry has attained thus far in the area of privacy protection is largely attributable to market-led initiatives premised on *notice* and *choice*. The fundamental principle of privacy protection is to inform consumers of personal information practices and give them the ability to determine how that information may be collected, used, and disclosed. These tenets of "notice and choice" are essential to the development of all of the privacy initiatives that AOL undertakes, and guide the efforts of all companies who have made strong commitments to user privacy.

As Congress turns its full attention to this issue next year, we at AOL would therefore ask the Members of this Committee to base their legislative initiatives on these key principles of notice and choice. Furthermore, we believe that the best way to implement these standards is by backing up these basic notice and choice requirements with strong enforcement efforts. This type of solution will allow companies to determine the most effective ways to implement notice and choice under their particular business models, while ensuring that companies do indeed comply with these requirements. In today's online world, consumer preferences can vary greatly from user to user, and we are in need of a legislative approach that will give consumers the flexibility to express these preferences on an ever-expanding variety of platforms and devices—from their PCs to their televisions to their handheld wireless devices.

We would suggest that the U.S. securities laws provide a helpful model for this type of enforcement-based approach. Securities disclosure requirements offer flexibility for a variety of business models, but the strong enforcement behind these requirements ensures that companies will provide consumers with honest disclosures about their securities practices. Just as the U.S. financial markets are thriving under this type of enforcement-based model for securities law, so too will e-com-

merce continue to thrive if Congress enacts an enforcement-based approach to consumer privacy.

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. Less than 3 years ago, many companies had to be convinced to join the OPA and adopt robust privacy policies. Today, these same companies are competing to build the best privacy solutions, have invested millions of dollars in developing privacy technology, and are spending large advertising dollars to distinguish themselves as privacy-friendly. The privacy technology fair sponsored by the Congressional Internet Caucus just 2 weeks ago gave companies an opportunity to demonstrate some of the exciting tools that are being developed today, as businesses compete to find the best ways to empower consumers to protect their own privacy online. Restrictive regulatory action could very likely curb such market innovation and competition, and discourage creative and flexible approaches to privacy protection.

We think that S. 2928 is a good example of a legislative approach that sets a baseline standard for notice and choice backed by strong enforcement, under which market-driven initiatives and technology innovation can continue to blossom. We commend Senators McCain and Kerry on this Committee—as well as Senators Abraham and Boxer—for cosponsoring this bill, which would ensure that all companies live up to these important principles by giving the FTC clear authority to enforce the notice and choice requirements. We believe this type of enforcement-based approach appropriately builds on existing market practices to set a baseline standard for privacy protection.

We are also pleased that many other Members of the Committee have recognized the importance of addressing this issue—most notably Senators Hollings, Wyden, and Burns. Senators Burns and Wyden have worked hard to craft S. 809, an approach that is based also on the key principles of notice and choice. The bill would ensure that companies provide clear notices to consumers about the personal information being collected and the possible use or disclosure of that information, as well as providing an easy-to-use mechanism for limiting the use and disclosure of that information. We are concerned that this bill would delegate broad rulemaking authority to the FTC, which could have an adverse impact on competition and technology innovation in the privacy space.

S 2606, drafted by Senator Hollings, is one of the most comprehensive privacy proposals introduced to date. However, we respectfully disagree with the approach taken by this particular bill, and hope to have the opportunity to work further with Senator Hollings next year on possible modifications to the proposal. S. 2606 recognizes the importance of ensuring that companies provide consumers with meaningful notice and choice with respect to the collection and use of their personal information. However, this bill mandates that the choice mechanism provided to consumers be based on an "opt-in" model.

While we agree with Senator Hollings that consumers should be provided with meaningful choice, we believe that it is not appropriate for all types of consumer information to be forced into the opt-in model in all circumstances. In the diverse online marketplace, we believe it is impossible to mandate a "one-size-fits-all" solution to consumer choice, and we should ensure that the legal framework for online privacy is flexible enough to accommodate the diversity in the online world.

We commend the efforts of all of the Members of this Committee, and are particularly pleased that each of the approaches includes a provision that would preempt inconsistent state law so that companies would not be subject to a potential patchwork of contradictory privacy requirements. We look forward to working with you next year, Mr. Chairman, along with the other members of this Committee and other Members of Congress, as you consider the appropriate legislative approach to protecting online privacy, because we believe that baseline privacy protections are important both to consumers and to the continued growth of the Internet.

At AOL we recognize 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 the many benefits that this medium has to offer. If consumers do not feel secure online, they will not engage in online commerce or communication—and without this confidence, our business cannot continue grow. For this reason, the borderless environment that is the Internet needs privacy solutions that are workable and can scale across state and national boundaries, while encouraging technology solutions that hold the greatest promise for user empowerment. Most of all, we must balance privacy initiatives with consumers' desire for personalization, customization and the other exciting benefits of the interactive medium, so that consumers can choose for themselves what kind of online experiences they want to enjoy.

As you continue your work on this issue next year, we urge you to consider the risks of any over-regulatory approach and the need for a solution that is flexible enough to sustain diverse business models, encourage user-friendly consumer interfaces, accommodate widely varying consumer preferences, and allow for rapid changes in technology, platforms, and services. The time has come for us to work together to find an effective legislative approach to online privacy protection. We at AOL are ready for that challenge, and look forward to working with all of you next year to build a solution that works for all of us. Thank you.

The CHAIRMAN. Thank you.

Mr. Garfinkel, welcome.

STATEMENT OF SIMSON GARFINKEL, CAMBRIDGE, MA

Mr. GARFINKEL. Thank you. Mr. Chairman, Members of the Committee, my name is Simson Garfinkel. In January, I published a book called *Database Nation: The Death of Privacy in the 21st Century*. It was my ninth book. Besides that, I have experience as an entrepreneur in the field of computers and as a reporter who has covered this field for many years. What I am not very good at is reading prepared statements, and so I am going to diverge from my prepared comments, which have been given to you as part of the record.

The CHAIRMAN. Your entire statement will be made part of the record, Mr. Garfinkel.

Mr. GARFINKEL. Thank you.

In January and February, I went around the country speaking with Americans because of my book being published, and since then I have received literally thousands of e-mail messages. The conclusion that I have is that most Americans want much more privacy protection both in the law and in technology.

I have also discovered that Americans are largely ignorant about the extent of abuses and uses of their personal information at this point in time and that they do not understand how to use the mechanisms that have already been made available to them under the current self-regulatory regime. A good example is many of AOL users are very unhappy that they get these advertisements popping up, but few of them that I have spoken with know how to turn that off.

Many Americans feel that privacy is over. One of the things that I was trying to show people is that it is not over. There are many opportunities for us to change the future right now.

The other thing is that many Americans feel that they own their personal information. I have them repeat this to me again and again. In fact, in the law they do not own their own personal information. What Americans are looking for is a way of controlling their personal information, some sort of moral right for that information, and that is what the legislation proposed here can do for them.

The fundamental right that they are seeking is access to their own personal information that is stored on other computers and at other businesses and organizations. This is the basis of the Fair Credit Reporting Act. It is the basis of the Privacy Act. And it is something that advanced technology makes very easy to do. All of these Web-based systems for collecting personal information can be easily turned around and give the user access to the information

that has been collected both from the user and from other sources. All these systems need that personal information to serve up customized advertisements or to make decisions. I have built these e-commerce systems and I know that it is merely a decision on the part of the company running the system whether or not to give the consumer access to their own information. It is not a technical hurdle.

I am also very concerned about the connection of software running on a person's PC with software on the Internet. You can imagine your PC programs, your Microsoft Word, other programs could scan through personal information on your computer and then send that over an encrypted link to a third party or to the vendor. Right now American consumers have no way of knowing if that is happening and, in fact, no right to know if that is happening or not.

I am also very concerned that any legislation this Committee passes have opt-in provisions rather than the opt-out provisions that is currently embodied in two pieces of legislation. The problem with the opt-out is that the opt-out provisions can be very difficult for consumers to follow. Opt-in provisions require that companies properly disclose what they are doing and propose a value proposition to the consumer. I think that without that, many of the deals happening between companies and consumers are inherently one-sided.

Finally, I would like to say that we really do need a comprehensive solution for all privacy issues facing Americans. I would like to see legislation on that matter considered, but we should not let the need for comprehensive legislation get in the way of adopting legislation right now that covers the online regimes. It is very important that we put in place protections for consumers in the online world now before more companies spring into being that make violating privacy or make using personal information in ways that are counter to the interests of most Americans the basis of their business plans. We are seeing more and more of these companies spring up.

Last, I think that we should be creating a single privacy office as a focal point for the enforcement of all of this legislation. There are many, many pieces of privacy legislation in the code right now. Such a privacy office could be a resource center for both government and for business and for consumers. One of the concerns that I have with many of the pieces of legislation is that they break up enforcement into many different divisions of the federal government. I understand that there are reasons for doing that, but ultimately I think that the interest of consumers and business will be served by a single focal point.

That is what I wanted to say.

[The prepared statement of Mr. Garfinkel follows:]

PREPARED STATEMENT OF SIMSON GARFINKEL, CAMBRIDGE, MA

Mr. Chairman and members of the Committee, I am honored to speak before you today.

My name is Simson Garfinkel. I am perhaps best known in the field of consumer privacy because of my book *Database Nation: The Death of Privacy in the 21st Century,* which was published this January. As a journalist, I have written about intersection of privacy and information technology for more than twelve years. Besides *Database Nation,* I am the co-author of five books on computer security. Finally, I

am an experienced technologist and an entrepreneur. I have had an Internet e-mail address since 1983. In 1995, I started Vineyard.NET, an Internet Service Provider on Martha's Vineyard. In 1998, I started a company called Sandstorm Enterprises, which develops advanced computer security tools. I am currently the Chief Scientist at Broadband2Wireless, a company that is building a nation-wide high-speed wireless Internet service. I also serve as an advisor to two firms that sell privacy-related products and services. I must say, however, that I am here speaking for myself, for none of the companies with which I am currently affiliated.

Mr. Chairman, as you know, many surveys have found that Americans are very concerned about the growing number of threats to their privacy. Other surveys have found that many Americans are refusing to participate in e-commerce on the Internet, because they are fearful that they will be compromising their privacy in the process. Indeed, I have many friends who do not use the Internet to make purchases, to view their bank statements, or to pay their bills. Some of these friends are extremely sophisticated individuals: they feel that by making use of e-commerce, they will be putting their personal information at risk, and that they might become victims of fraud as a result. It's hard to argue with this point of view given the dramatic rise in identity theft that we have seen in recent years.

In any event, this January, after my book was published, I went on a book tour around the country. I spoke with many Americans about privacy, both on and off the Internet. Most of the people that I spoke with realized that there were few if any protections for their personal information in Cyberspace. What you might find more revealing, however, is that few Americans realized how poorly their privacy is protected off the Internet. Although Congress has passed a whole slew of privacy laws over the past twenty years, it really is a legislative patchwork. There are many basic protections that Americans feel they do have, but which in fact they do not. For example, many Americans do not realize that stores routinely engage in covert video surveillance, and that there is no legal requirement to notify shoppers that such surveillance is taking place.

One of the points that I make when I speak about privacy is that Americans tend to approach electronic privacy issues as a big *tabula rasa,* an uncharted ocean, if you will, in which there are many questions and few answers. Yet for more than 25 years we've had a consistent set of principles that do a wonderful job confronting and solving these electronic privacy issues. I am speaking, of course, of the Code of Fair Information Practices, as well as the refinements on the code that have been made over the years.

The reason that the principles in the CFIP have been around so long is that they resonate with our basic democratic beliefs. The CFIP was developed for the information age, and I think that these practices can and should be extended to the Internet.

All of the bills that you are considering embody aspects of the CFIP. I believe that S.2606 goes further and does a better job protecting the interests of Americans. In the rest of my time, I'd like to explain why.

Each and every bill you are considering require businesses to state their policies regarding the collection of personal information. But what then? After **notice,** I believe that **access** is a value that is central to our principles of fair play and justice.

Access

Imagine that you learned of a company that was in the business of collecting and selling large amounts of personal information. You contact the company and ask them if they have a file on you. They say that they won't tell you. You ask if you can see the contents of your file. The company says "no." You ask if you can have a list of the other firms to which your personal information has been transferred. The company responds that it is impossible to create such a list, and even if it were, that information is trade secret.

You can imagine how frustrated and how powerless you would feel.

This is the situation that confronted most Americans in the 1960s. The companies were credit reporting agencies like Retail Credit (now Equifax) and TRW (now Experian.) When Congress considered legislation that ultimately became the Fair Credit Reporting Act, those companies insisted that giving consumers access to their credit reports would be unworkable, a tremendous economic burden, and would be subject to abuse. Today, nearly 30 years later, we view access to credit reports as a fundamental right.

As a technologist, I can tell you that it is granting an individual access to their personal information is much easier to do today than it was 30 years ago. Consider the case of cookies and Doubleclick. I have met many people who do not want an internet advertising firm such as Doubleclick watching over their shoulder and keeping track of every website they visit, every article that they read. They see that

Doubleclick has put a cookie on their computer and they want to know what Doubleclick's computer's have in the databanks.

Now Doubleclick's computer's consult this database every single time they show a banner advertisement over the Internet. Doubleclick prides itself on this capability—it is Doubleclick's value added. The company even has a patent on the technology, US5,948,061: a "Method of delivery, targeting, and measuring advertising over networks." It would be a simple matter to turn this technology around so that when a user visits the Doubleclick site, the Doubleclick computers would report the personal information that they have on file about the individual.

Consent

Beyond the issue of access, the issue of Consent is paramount to any discussion of online privacy.

An overwhelming number of Americans that I have spoken with believe that they own their personal information. It's true that this information runs contrary to US law. Nevertheless, it is a deeply held belief among the vast majority of Americans.

The bills that you have for consideration before you take two very difficult views of personal information ownership. By creating a so-called "opt-out" regime, S.809 and S.2928 essentially give ownership of personal information to corporations and businesses. These bills tell Corporate America: "you can do anything you want with a consumer's personal information, unless that consumer has the knowledge and the foresight to tell you otherwise."

I submit to you that this approach is inherently unfair.

Many Americans complain about telemarketing calls that they receive during dinnertime. When I was writing the book *Database Nation,* I was surprised to learn that Americans have been complaining about these nightly interruptions for more than **thirty-five years.** Now for many years the Direct Marketing Association has operated its so-called Telephone Preference Service that lets Americans put their phone numbers on a "do-not call list." But few Americans know that these services even exist.

Now many people think that privacy policies and the use of personal information are solely issues having to do with junk mail, telemarketing calls, and spam e-mail. This is not the case. As we move into the 21st Century, there is a vast array of actions that Internet-savvy firms will be able to perform with our personal information. It will be difficult for us to keep track of all the ways that our personal information can and will be exploited. It will be nearly impossible for us to meaningfully opt-out.

Consider this hypothetical example. What if a company were to electronically rifle my online address book, get the list of every person that I correspond with, and then send each one an e-mail message? What if these e-mail messages claimed to be from me, and contained endorsements of the company's new product? What if the company had an opt-out privacy policy, but it was so complicated to opt-out that few people understood what was being done with their personal information until it was too late? This Committee might very well hold hearings to investigate the company, alleging that the practices were illegally appropriating the personal information and identities of consumers. As it turns out, technologies that appropriate e-mail address books are already being deployed. I have attached to the end of my written testimony an article written by Boston Globe columnist Hiawatha Bray which alleges that Microsoft is using a technique such as this to market its new MSN server. Indeed, the only reason that Mr. Bray did not inadvertently send out thousands of e-mail to every person in his address book when he tried out Microsoft's new MSN server is that the service first asked Mr. Bray's permission—that is, the service abides by an opt-in policy.

An opt-in regime is inherently more democratic than an opt-out one. With opt-in, companies explain to consumers what will be done with their personal information, and then it's up to the consumer to decide whether or not they wish to participate. This is the same sort of "informed consent" system that has become the standard in medicine, banking, and other areas.

One of the growing critiques of the opt-out approach favored by S.809 and S.2928 is that these policies require consumers to read, understand, and act upon the so-called "privacy policies" posted by websites. Unfortunately, these policies are frequently difficult-to-understand and do little to protect privacy. To demonstrate how opaque these privacy policies are, I've attached the "DoubleClick Privacy Statement" at the end of my written testimony. I have a master's degree in journalism, I've written a book on privacy, and I've taken courses at law school, and I really don't understand what DoubleClick is with personal information. The advantage of an opt-in regime is that, in an opt-in regime, if a company does clearly explain its prac-

tices and their advantages to consumers, the resultantly confused consumers will have reason to opt-in.

As I said before, most Americans believe that they own their personal information. But ownership really isn't the right word. As I make clear in my book *Database Nation,* what is owned can be transferred or sold. American's view of their own privacy is much closer to the French notion of moral rights. Americans feel that they have a right to privacy protection. They feel that they have a right to have companies protect their privacy unless they give explicit permission otherwise. Americans feel they have a right to be let alone. Americans want to live in an opt-in system. Opt-out is contrary to our democratic principles and heritage.

Enforcement

One concern that I have with all of the bills that you are currently considering is the issue of enforcement. I think that it makes sense to have a single agency within the US government that is responsible for enforcing privacy laws. Right now, that agency seems to be the Federal Trade Commission. I'm not sure that the FTC is the right choice—I would like to see an independent Privacy Office that's responsible for both the commercial sector and for the laws that apply to the federal government and to the laws that are enforced through the FCC. I think that it makes sense to build a center of expertise within the federal government. I think that a Privacy Office could be a resource to the rest of the federal government, and to private industry as well.

But I understand that this Congress is unlikely to create a Privacy Office and that the Federal Trade Commission seems to be the current privacy torchbearer. Indeed, the Commission did an excellent job on its recent privacy study. I'm pleased that S.2606 would create a FTC Office of Online Privacy.

I am however concerned that both S.2928 and S.2606 split enforcement between the Federal Trade Commission and an assortment of other federal agencies. I understand that there are technical reasons for doing this, but I think that they should be reconsidered.

I am very pleased that S.2928 establishes a statutory civil penalty of $22,000 for each privacy violation. Traditionally, one of the hardest problems for those faced with privacy violations has been to demonstrate damages. Likewise, creation of a private right of action in S.2606, with awards up to $50,000 for willful and knowing violations, will make it far easier for wronged individuals to pursue compensation in our courts. This may be an effective deterrent.

I think that S.2606's protection of Whistleblowers (section 305) is an important protection that is missing from the other bills under consideration. Often times the privacy abuses that occur within an organization are unknown to outsiders. In these cases, it is important to encourage insiders to step forward, and the protection for whistleblowers will create protections for these individuals.

In this age of mega-corporations, a vast amount of personal information could be collected and used in a manner that could be considered "solely for internal company processes." For this reason, I think that the exemption for "internal company processes" in S.809 is a dangerous precedent. Company policies should not be exempt from privacy legislation simply because they do not involve third-parties.

Bankruptcy is a real threat faced by many organizations that collect personally identifiable information. It is very important that information collected by an organization when it is financially healthy not be auctioned off to the highest bidder during a bankruptcy proceeding. S.2606 takes personally identifiable information off the table of the bankruptcy courts. This is a very important provision that should be echoed by the other legislation under consideration.

I am also concerned that the legislation under consideration does not adequately address non-commercial threats to privacy. For example, exempting non-profit organizations, such as S.2928 does, would allow public radio stations to engage in privacy abuses in the interest of fund raising. As we know, this has happened in the past; I would like to see legislation prohibit such abuses from happening on the Internet in the future.

In Conclusion

Mr. Chairman, I believe that the United States will eventually have some form of legislation that protects consumers' personal information, both on and off the Internet. I believe that such legislation is vital to the long term health of democracy in this country.

What I do not know, Mr. Chairman, is whether comprehensive privacy-protecting legislation will be passed this year, next year, or in twenty years. I do know that the longer the US Congress waits to pass such legislation, the more economic dislocation there will be when it is final passed. That is because the longer you wait,

the more businesses will spring up whose business model depends upon misrepresentation and privacy invasion. There are a few such companies now; with no action, there will be more next year.

Nevertheless, I think that it would be foolish to delay the passage of legislation that protects online privacy while the Congress tries to create that comprehensive privacy legislation.

The American people believe that they have a right to privacy, and they wish to see this body pass legislation that affirms that right. Paramount to protecting the right to privacy in the digital age is the rights of individuals to have access to their own information, and the right to have their information protected and held in trust unless they explicitly give permission for it to be used otherwise. I therefore cannot support S.809 and S.2928, because both of these bills would create an opt-out regime. Instead, I would urge this body to make S.2606 the basis of any privacy legislation that is approved by this Committee.

UPGRADE

Microsoft serves up its own spam

By Hiawatha Bray, Globe Columnist, Globe Staff

9/28/2000

Sometimes I feel like that ape in the beginning of the movie "2001." There he is, starving amidst a pile of animal bones. He's so stupid that it takes a singing black slab from outer space to make him grab a tibia and go kill something. Couldn't he just figure it out on his own?

I felt that way yesterday as I read of the latest outrage involving unwanted e-mail, better known as spam. I am, of course, opposed to it. And so, ostensibly, is Microsoft Corp, which has built antispam features into its e-mail software and its Web-based Hotmail service.

This makes me wonder why Microsoft is presently engaged in a massive spam campaign of its own, one that features the unwitting participation of many Internet users. But I'm even more puzzled by the fact that evidence of the outrage landed in my lap, and I ignored it.

A few weeks back, I installed the preview version of the new Explorer software for Microsoft's MSN online service. Basically, Microsoft has customized its Internet Explorer browser with specialized links that mimic the features found on America Online. It's a pretty good job. MSN Explorer's extra clutter isn't to my taste, but newbies may find it congenial.

Anyway, after installing the MSN software, I was invited to click a check box that would have sent e-mails to my friends to announce the joyous event. This should have got me thinking.

Instead, I did what I almost always do when installing Internet software. I clicked "no thanks" and forgot all about it.

Alas, not every user of the new software was so cautious. That's why I received an e-mail last week from a reader who was hopping mad about getting an unsolicited advertisement from Microsoft, sent to him by some guy he'd never heard of.

The reader fired off a complaint to Microsoft, and got this reply: "When a user installs MSN Explorer, they have the option of sending an e-mail from MSN Explorer to invite you to use the program. This is not an advertisement or commercial e-mail sent to solicit information from you by MSN—it is only an invitation sent by an individual member to try the new product."

This didn't satisfy the reader, but incredibly, it satisfied me. Here's my response: "Well, that's not quite spam, is it? Maybe it's a questionable tactic, but it was sent by someone you presumably know."

Proof positive that too much e-mail makes you stupid. Had I not been so swamped with the stuff, I might have put two and two together.

After all, I'd written quite a bit on the Melissa computer virus—the one that automatically sent copies of itself to every e-mail address on a victim's computer. Melissa, you'll recall, only affected users of Microsoft's e-mail software.

So I had all of the pieces of the puzzle, and only needed to snap them together. I didn't. But others did, and by yesterday morning it was the talk of the Web.

Sure enough, the MSN software, unless you tell it otherwise, will check to see if your computer has a copy of Microsoft's Outlook Express e-mail program. If it's there, the software then checks the program's address book, scoops up all of the e-

mail addresses contained therein, and sends them an "invitation" to join MSN. This invitation is, of course, signed by you.

If I hadn't clicked the "don't you dare" box while installing MSN Explorer, I'd have sent this warm, personal invitation to 2,290 of my nearest and dearest friends. That's how many names are in my Outlook Express address book. These are mostly tech-industry types who'd have held me in even lower regard than they already do once this personalized spam arrived. For spam is exactly what this is, and of a particularly insidious kind.

Granted, MSN Explorer asks for permission before cranking out the mail. But how many users realize that they'll be sending advertisements for Microsoft? How many understand that they're sending these ads to their bosses, their bookies, their best customers—everybody?

I understand that Microsoft is frustrated; MSN has 3 million users to AOL's 24 million. But I never thought they'd stoop to the favorite market tool of Internet pornographers. Somebody at MSN had a brainstorm, but then failed to think it through. I guess we need a couple more of those black slabs. Put one in the MSN marketing department, and the other next to my desk.

Hiawatha Bray is a member of the Globe Staff. He can be reached by e-mail at *bray@globe.com.*

September 28, 2000

DoubleClick Privacy Statement

Internet user privacy is of paramount importance to DoubleClick, our advertisers and our Web publishers. The success of our business depends upon our ability to maintain the trust of our users. Below is information regarding DoubleClick's commitment to protect the privacy of users and to ensure the integrity of the Internet.

Information Collected in Ad Delivery

In the course of delivering an ad to you, DoubleClick does not collect any personally-identifiable information about you, such as your name, address, phone number or email address. DoubleClick does, however, collect non-personally identifiable information about you, such as the server your computer is logged onto, your browser type (for example, Netscape or Internet Explorer), and whether you responded to the ad delivered.

The non-personally identifiable information collected by DoubleClick is used for the purpose of targeting ads and measuring ad effectiveness on behalf of DoubleClick's advertisers and Web publishers who specifically request it. For additional information on the information that is collected by DoubleClick in the process of delivering an ad to you, please.

However, as described in "Abacus Alliance" and "Information Collected by DoubleClick's Web Sites" below, non-personally identifiable information collected by DoubleClick in the course of ad delivery *can be associated with a user's personally identifiable information* if that user has agreed to receive personally-tailored ads.

In addition, in connection solely with the delivery of ads via DoubleClick's DART technology to one particular Web publisher's Web site, DoubleClick combines the non-personally-identifiable data collected by DoubleClick from a user's computer with the log-in name and demographic data about users collected by the Web publisher and furnished to DoubleClick for the purpose of ad targeting on the Web publisher's Web site. DoubleClick has requested that this information be disclosed on the Web site's privacy statement.

In addition, in connection solely with the delivery of ads via DoubleClick's DART technology to one particular Web publisher's Web site, DoubleClick combines the non-personally-identifiable data collected by DoubleClick from a user's computer with the log-in name and demographic data about users collected by the Web publisher and furnished to DoubleClick for the purpose of ad targeting on the Web publisher's Web site. DoubleClick has requested that this information be disclosed on the Web site's privacy statement.

There are also other cases when a user voluntarily provides personal information in response to an ad (a survey or purchase form, for example). In these situations, DoubleClick (or a third party engaged by DoubleClick) collects the information on behalf of the advertiser and/or Web site. This information is used by the advertiser and/or Web site so that you can receive the goods, services or information that you requested. Where indicated, DoubleClick may use this information in aggregate form to get a better general understanding of the type of individuals viewing ads

or visiting the Web sites. Unless specifically disclosed, the personally-identifiable information collected by DoubleClick in these cases is not used to deliver personally-tailored ads to a user and is not linked by DoubleClick to any other information.

Abacus Alliance

On November 23, 1999, DoubleClick Inc. completed its merger with Abacus Direct Corporation. Abacus, now a division of DoubleClick, will continue to operate Abacus Direct, the direct mail element of the Abacus Alliance. In addition, Abacus has begun building Abacus Online, the Internet element of the Abacus Alliance.

The Abacus Online portion of the Abacus Alliance will enable U.S. consumers on the Internet to receive advertising messages tailored to their individual interests. As with all DoubleClick products and services, Abacus Online is fully committed to offering online consumers **notice** about the collection and use of personal information about them, and the **choice** not to participate. Abacus Online will maintain a database consisting of personally-identifiable information about those Internet users who have received notice that their personal information will be used for online marketing purposes and associated with information about them available from other sources, and who have been offered the choice not to receive these tailored messages. The notice and opportunity to choose will appear on those Web sites that contribute user information to the Abacus Alliance, usually when the user is given the opportunity to provide personally identifiable information (e.g., on a user registration page, or on an order form).

Abacus, on behalf of Internet retailers and advertisers, will use statistical modeling techniques to identify those online consumers in the Abacus Online database who would most likely be interested in a particular product or service. All advertising messages delivered to online consumers identified by Abacus Online will be delivered by DoubleClick's patented DART technology.

Strict efforts will be made to ensure that all information in the Abacus Online database is collected in a manner that gives users clear notice and choice. *Personally-identifiable information in the Abacus Online database will not be sold or disclosed to any merchant, advertiser or Web publisher.*

Name and address information volunteered by a user on an Abacus Alliance Web site is associated by Abacus through the use of a match code and the DoubleClick cookie with other information about that individual. Information in the Abacus Online database includes the user's name, address, retail, catalog and online purchase history, and demographic data. The database also includes the user's non-personally-identifiable information collected by Web sites and other businesses with which DoubleClick does business. Unless specifically disclosed to the contrary in a Web site's privacy policy, most non-personally-identifiable information collected by DoubleClick from Web sites on the DoubleClick Network is included in the Abacus Online database. However, the Abacus Online database will not associate any personally-identifiable medical, financial, or sexual preference information with an individual. Neither will it associate information from children.

Sweepstakes

DoubleClick's Flashbase, Inc. subsidiary provides automation tools that allow our clients to provide online contests and sweepstakes ("DoubleClick sweepstakes").

All DoubleClick sweepstakes entry forms must provide a way for you to opt-out of any communication from the sweepstakes manager that is not related to awarding prizes for the sweepstakes. Entry forms must further provide consumers with a choice whether to receive email marketing materials from third parties. When you enter a DoubleClick sweepstakes, the information you provide is not be shared with DoubleClick or any third party, unless you agree by checking the opt-in box on the sweepstakes entry form. If you enter a sweepstakes, you agree that the sweepstakes sponsor may use your name in relation to announcing and promoting the winners of the sweepstakes. See the official rules of the sweepstakes you are entering for additional information.

DoubleClick does collect aggregate, anonymous information about the sweepstakes. That information is primarily used to help sweepstakes managers choose prizes and make other decisions regarding the organization of the sweepstakes. DoubleClick does not associate information provided through the sweepstakes with your other web browsing activities or clickstream data.

Email

DoubleClick uses DARTmail, a version of DART technology, to bring you emails that may include ads. Email is sent only to people who have consented to receive a particular email publication or mailing from a company. If at any time you would like to end your subscription to an email publication or mailing, follow either the

directions posted at the end of the email publication or mailing, or the directions at the email newsletter company's Web site.

In order to bring you more relevant advertising, your email address may be joined with the information you provided at our client's website and may be augmented with other data sources. However, DoubleClick does not link your email address to your other Web browsing activities or clickstream data.

Information Collected by DoubleClick's Web Sites

The Web sites owned or controlled by DoubleClick, such as *www.NetDeals.com* and *www.IAF.net* may ask for and collect personally-identifiable information. DoubleClick is committed to providing meaningful notice and choice to users before any personally-identifiable information is submitted to us. Specifically, users will be informed about how DoubleClick may use such information, including whether it will be shared with marketing partners or combined with other information available to us. In most cases, the information provided by a user will be contributed to the Abacus Online database to enable personally-tailored ad delivery online. Users will always be offered the choice not to provide personally-identifiable information or to have it shared with others.

Access

DoubleClick offers users who have voluntarily provided personally-identifiable information to DoubleClick the opportunity to review the information provided and to correct any errors.

Cookies and Opt-Out

DoubleClick, along with thousands of other Web sites, uses cookies to enhance your Web viewing experience. DoubleClick's cookies do not damage your system or files in any way.

Here's how it works. When you are first served an ad by DoubleClick, DoubleClick assigns you a unique number and records that number in the cookie file of your computer. Then, when you visit a Web site on which DoubleClick serves ads, DoubleClick reads this number to help target ads to you. The cookie can help ensure that you do not see the same ad over and over again. Cookies can also help advertisers measure how you utilize an advertiser's site. This information helps our advertisers cater their ads to your needs.

If you have chosen on any of the Web sites with which Abacus does business to receive ads tailored to you personally as part of Abacus Online's services, the cookie will allow DoubleClick and Abacus Online to recognize you online in order to deliver you a relevant message.

However, if you have not chosen to receive personally-targeted ads, then the DoubleClick cookie will not be associated with any personal information about you, and DoubleClick (including Abacus) will not be able to identify you personally online.

While we believe that cookies enhance your Web experience by limiting the repetitiveness of advertising and increasing the level of relevant content on the Web, they are not essential for us to continue our leadership position in Web advertising.

While some third parties offer programs to manually delete your cookies, DoubleClick goes one step further by offering you a "blank" or "opt-out cookie" to prevent any data from being associated with your browser or you individually. If you do not want the benefits of cookies, there is a simple procedure that allows you to deny or accept this feature. By denying DoubleClick's cookies, ads delivered to you by DoubleClick can only be targeted based on the non-personally-identifiable information that is available from the Internet environment, including information about your browser type and Internet service provider. By denying the DoubleClick cookie, we are unable to recognize your browser from one visit to the next, and you may therefore notice that you receive the same ad multiple times.

If you have previously chosen to receive personally-tailored ads by being included in the Abacus Online database, you can later elect to stop receiving personally-tailored ads by denying DoubleClick cookies.

Your opt-out will be effective for the entire life of your browser or until you delete the cookie file on your hard drive. In each of these instances, you will appear as a new user to DoubleClick. Unless you deny the DoubleClick cookie again, DoubleClick's ad server will deliver a new cookie to your browser.

Disclosure

DoubleClick makes available all of our information practices at *www.doubleclick.net,* including in-depth descriptions of our targeting capabilities, our privacy policy, and full disclosure on the use of cookies. In addition, we provide all users with the option to contact us at with any further questions or concerns.

Security

DoubleClick will maintain the confidentiality of the information that it collects during the process of delivering an ad. DoubleClick maintains internal practices that help to protect the security and confidentiality of this information by limiting employee access to and use of this information.

Industry Efforts to Protect Consumer Privacy

DoubleClick is committed to protecting consumer privacy online. We are active members of the Network Advertising Initiative, NetCoalition.com, Online Privacy Alliance, Internet Advertising Bureau, New York New Media Association, and the American Advertising Federation.

For more information about protecting your privacy online, we recommend that you visit *www.nai.org, www.netcoalition.com,* and *www.privacyalliance.org*.

We also recommend that you review this Privacy Statement periodically, as DoubleClick may update it from time to time.

1973: The Code of Fair Information Practices

The Code of Fair Information Practices was the central contribution of the HEW (Health, Education, Welfare) Advisory Committee on Automated Data Systems. The Advisory Committee was established in 1972, and the report released in July. The citation for the report is as follows:

U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens (1973).

The Code of Fair Information Practices is based on 5 principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
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 misuses of the data.

1980: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Today privacy advocates have moved beyond the 1973 Code of Fair Information Practices and have adopted the OECD's 1980 Guideliens on the Protection of Privacy and Transborder Flows of Personal Data. You can find the *entire document on the OECD website.* The most important principles are:

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.

Data Quality Principle

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.

Purpose Specification Principle

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 fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a. with the consent of the data subject; or

b. by the authority of law.

Security Safeguards Principle

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

Openness Principle

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.

Individual Participation Principle

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.

Accountability Principle

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

The CHAIRMAN. Thank you, Mr. Garfinkel.

Mr. Rotenberg, we will go with you and then we will run over and vote.

STATEMENT OF MARC ROTENBERG, PRESIDENT, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ROTENBERG. Mr. Chairman, Members of the Committee, thank you very much for the opportunity to be here. My name is Marc Rotenberg. I am Director of the Electronic Privacy Information Center. I have also taught the law of information privacy at Georgetown for the last 10 years, and my textbook, which is a collection of privacy laws from the U.S. and around the world, is now in its third edition.

I am going to focus on the substance of the three proposals before the Committee today. I would like at the outset to commend you for your focus on this issue. Privacy is obviously a very important concern for Americans. Many believe it is the No. 1 issue facing the future of the Internet, and there has clearly been progress in addressing the issue, among the privacy groups and the Congress and also the industry groups.

But the critical decision now is what is the legislative approach that is going to provide meaningful protection for Americans going forward.

Now, there is a very attractive proposal on the table. It is a proposal based on notice and choice. It says, in effect, let us inform people about the collection and use of their personal information

and give them some choices. This is the approach that Mr. Vradenburg and others have endorsed. It is, by and large, the approach, sir, in your bill, and it is the approach generally followed by the industry groups that talk a great deal about privacy.

But the critical point to understand is that notice and choice operating alone, without the other rights that are typically found in a privacy bill, do not provide privacy protection. What they will provide, in fact, is a type of warning label or disclaimer. They will allow companies to do whatever they wish with the personal information that they collect, and they will not establish any substantive rights for individuals who provide their information.

The CHAIRMAN. That is an interesting interpretation of this legislation. It is a fascinating one, but please proceed. It could not be further from the truth, but please go ahead.

Mr. ROTENBERG. It may not be the intent of the legislation. I will be clear on this point. It may not be the intent, but I have to tell you that in practice this is how it operates.

Privacy warning notices are found in the work place. They tell employees that they do not have an expectation of privacy in the use of a computer or a telephone. Privacy warning notices are found on commercial websites. They tell people who buy products that the information that they offer will be disclosed to third parties. This is how privacy notices have typically operated.

Now, I think it is important to contrast this approach with the way that privacy laws have traditionally been constructed in the United States. Privacy laws in the past, whether it is the cable act or the video act or the credit reporting act, are based on a group of rights called fair information practices. They include rights of access, rights to limit the disclosure of information, sometimes even obligations to destroy the information about individuals that is collected. This is what you see, for example, in the Video Privacy Protection Act. Companies are actually told that after a period of time, to protect the privacy interests of their customers, they are expected to destroy the information. Now, that approach, the approach that is based upon fair information practices, is the way that we have traditionally constructed privacy protection in this country.

Now, the argument can be made, well, things are changing very quickly with the Internet. Maybe we need a more modern approach.

The CHAIRMAN. Do you disagree with that, that times are changing very quickly?

Mr. ROTENBERG. No. Actually I think things are changing quickly.

But the second point I wanted to make, Mr. Chairman, is that these privacy laws that we have adopted in the past, that have included all of these rights—quite a bit more, I am trying to point out, than notice and consent—were in fact a response to changing technologies. The Privacy Act was a response to the computerization of records in the federal government.

The CHAIRMAN. No. The Privacy Act was an attempt to protect someone's privacy whether it be computerized or on paper. At my age, Mr. Rotenberg, I remember it very well. I do not think you were around then.

Mr. ROTENBERG. Well, Mr. Chairman, I was around. I was maybe a few years younger.

I think there is certainly a lot to show in the history that it was the automation of records, and the Cable Act was the response to cable television.

The CHAIRMAN. If you do not mind my interrupting you again. It was because of egregious violations of people's privacy that took place that required Congress and the American people to demand action. There were a number of scandals. It had nothing to do with computerization or non-computerization. It had to do with direct and egregious violations of Americans' privacy. I think I can show you a clear legislative record of that and the scandals associated with it.

Please proceed.

Mr. ROTENBERG. Mr. Chairman, the Privacy Act was passed by the post-Watergate Congress in 1974, and there was no question that the misuse of personal information by the President at that time supported the congressional effort.

But the beginning of congressional hearings, the reason that Congress got interested in this issue in the 1960's, was because of a proposal called the National Data Center. In 1965, the federal government said let us take all of the information on American citizens, automate it, made possible now with computers, and use it for statistical purposes and government programs. And beginning in 1966, both the House and the Senate held a series of hearings to look at the automation——

The CHAIRMAN. And never acted until egregious violations of American citizens' privacy were committed.

Look, I have got to stop because there is only one minute left. We will take a very brief break. There are two votes, and I will look forward to continuing this dialog. We will return in approximately five to ten minutes. We will take a break.

[Recess.]

The CHAIRMAN. We will recommence the hearing, and Mr. Rotenberg, I will try to restrain myself from interrupting you for the rest of your testimony. I do not guarantee it. I will try.

[Laughter.]

The CHAIRMAN. Thank you and thank you for your indulgence.

Mr. ROTENBERG. Thank you, Mr. Chairman. I will also agree to move on past the Privacy Act because I guess we have our differing views.

This really was my point, that over the last 25 years, there have been a lot of new technologies that Congress has confronted. Congress has confronted cable and electronic mail and videotapes, fax machines, and so forth. In each instance, rather than saying technology is changing quickly or we do not understand it, maybe we should not regulate, Congress has come up with good privacy legislation. You did it with children's information on the Internet last year.

The point of my testimony here is to really say that I think we need to put in place the kind of meaningful safeguards that we have in the past with new technologies to safeguard the interests of consumers. I think 2606 does that very well. This is a bill that is forward looking. It anticipates a bunch of problems. It updates

and amends current privacy laws that are already doing a good job, and most critically, it provides an effective form of protection. It gives people some baseline rights. And I think that is what they need. I think that is what the public is asking for. I think that is what the industry increasingly understands is likely to come about.

Now, I understand this is toward the end of the session and maybe all these things cannot be worked out now, but I do have to underscore, we have never done a privacy bill in this country based simply on notice and choice. We have always tried to give people something more. We can talk about how far we can go, whether access works in all circumstances or in some circumstances or for certain types of information. I think that is an important debate to have, but we have to give people something more than notice and choice.

We also have to give them an opportunity to pursue privacy complaints on their own if they wish. We think a private right of action is absolutely vital to protect privacy interests. One of the problems that we have seen over the past year following the developments with the FTC, which is certainly working very hard to try to protect privacy, is that they are just not able to respond to all the privacy complaints that they are receiving. And because of the way section 5 is structured, they really do operate almost like a choke point on the types of claims that can be brought under this unfair and deceptive trade practices.

Privacy bills have traditionally given people a private right of action so that if they wish, they can pursue the matter in court. Not many of these cases are brought, but when they are brought, I think they are quite important to protect and safeguard privacy interests.

So, I want to thank you again, Mr. Chairman. I understand the Committee has done a lot of important work in this area. And I just urge you, please, to consider what type of rights people are going to have online going forward to protect their privacy.

[The prepared statement of Mr. Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, PRESIDENT, ELECTRONIC PRIVACY INFORMATION CENTER, WASHINGTON, DC

My name is Marc Rotenberg.[1] I am the Executive Director of the Electronic Privacy Information Center (EPIC) in Washington DC and an adjunct professor at Georgetown University Law School where I teach information privacy law.[2] I am grateful for the opportunity to appear before the Committee today. I also appreciate the Committee's ongoing efforts to explore the important issue of Internet privacy.

I will focus my comments on the need to ensure strong privacy safeguards for the Internet based on Fair Information Practices. These guidelines are the basis for almost all privacy laws, and provide the framework to evaluate the proposals currently before the Committee.

I will address specific provisions of the Online Privacy Protection Act, the Consumer Privacy Protection Act, and the Consumer Internet Privacy Protection Act. I will recommend that the Committee adopt strong, sensible provisions that safeguard the interests of consumers and provide clarity and a level playing field for

[1] Executive director, Electronic Privacy Information Center; adjunct professor, Georgetown University Law Center; editor, *The Privacy Law Sourcebook 2000: United States Law, International Law, and Recent Development;* editor (with Philip Agre) *Technology and Privacy: The New Landscape* (MIT Press 1998).

[2] The Electronic Privacy Information Center is a project of the Fund for Constitutional Government, a non-profit charitable organization established in 1974 to protect civil liberties and constitutional rights. More information about EPIC is available at the EPIC web site *http://www.epic.org*

businesses. I will also address some of the issues that are not addressed directly in the legislative proposals, such as the need to protect online anonymity.

Status of Internet Privacy

Mr. Chairman, at the outset, I wish to make 3 brief points concerning Internet privacy. First, we believe that there is widespread public support for legislation in this area and also that industry recognizes that such legislation is appropriate and necessary. Polling data routinely shows that the public believes that privacy laws for the Internet are needed.[3] And although industry groups have objected as a general matter to government regulation of the Internet, in the area of online privacy I believe most will concede that legislation is likely.[4]

Second, while we recognize that commercial web sites have made progress in developing and posting privacy notices, we do not believe that these policies alone protect online privacy. In fact, privacy notices without other substantive rights operate more like warning labels or disclaimers than actual privacy safeguards. Although it would be tempting to pass legislation based simply on the notice requirement, we believe such a bill over the long term would reduce the expectation of privacy and the level of online protection. A substantive privacy measure must provide more than notice.

Third, we believe that enforcement mechanisms must remain flexible. Any legislation that leaves a central agency in the position to limit enforcement at the local level or prevents an individual from pursuing a privacy complaint in court could significantly undermine the protection of privacy interests. And to the extent that the FTC plays a central role in overseeing the enforcement of privacy, it is vitally important that formal reporting requirements be established so that this Committee, the Congress, and the public will be able to evaluate the effectiveness of privacy protection in the United States.

Privacy Laws and the Role of Fair Information Practices

The basic goal of privacy legislation is to outline the responsibilities of organizations that collect personal information and to provide rights to those individuals that provide the personal information. These rights and responsibilities are commonly referred to as "Fair Information Practices." Fair Information Practices ensure that consumers have control over their personal data and that companies abide by ethical business practices.

Fair Information Practices have provided the basis for privacy legislation across both the public and private sectors. The Fair Credit Reporting Act of 1970 placed requirements on credit reporting agencies, restricting their ability to disclose information about individual consumers and providing a right of access so that individuals could inspect their credit reports and determine whether decisions affecting their ability to obtain a loan or receive credit were based on accurate and complete information.[5] Since 1970, privacy laws based on Fair Information Practices have covered educational records[6], cable subscriber records[7], email[8], video rental records[9], and telephone toll records[10]. The recently passed Children's Online Privacy Protection Act[11] requires parental consent before information is collected from minors and access to any information already collected.

For more than 25 years, the United States has established privacy laws based on Fair Information Practices directly in response to the development of new technologies, such as computer databases, cable television, electronic mail, movies on video tape, and fax machines. Far from discouraging innovation, these baseline privacy standards have promoted consumer trust and confidence as new services have

---

[3] Business Week/Harris Poll: A Growing Threat, March 20, 2000, [*http://www.businessweek.com/2000/00__12/b3673010.htm*]. The poll found that 57 percent of people surveyed supported laws governing the collection and use of personal information online while only 15 percent supported letting industry groups develop voluntary standards. Georgia Tech Graphic, Visualization, & Usability Center's Tenth WWW User Survey (October 1998) [*http://www.gvu.gatech.edu/user__surveys/survey-1998-10/graphs/privacy/q59.htm*] This poll found that 41 percent agreed strongly and 31 percent agreed somewhat with the statement: "There should be new laws to protect privacy on the Internet."

[4] "Mixed Views on Privacy Self-Regulation," DM News, October 2, 2000 [*http://www.dmnews.com/articles/2000-10-02/10780.html*]

[5] Fair Credit Reporting Act (1970) 15 U.S.C. § 1681.

[6] Family Educational Rights and Privacy Act (1974) 20 U.S.C. § 1232g.

[7] Cable Communications Policy Act (1984) 47 U.S.C. § 551.

[8] Electronic Communications Privacy Act (1986) 18 U.S.C. § 2510.

[9] Video Privacy Protection Act (1988) 18 U.S.C. § 2710.

[10] See Telecommunications Act (1996) 47 U.S.C. § 222.

[11] Children's Online Privacy Protection Act (1999) 15 U.S.C. § 6501.

emerged. Privacy laws have also provided businesses with clear rules and a level playing field.

Fair Information Practices have also contributed to the development of privacy laws around the world. Important international agreements such as the Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the recently concluded Safe Harbor arrangement have been built on Fair Information Practices [12]. These international guidelines have become more important as we move toward a global economy where US firms seek to sell products online in other countries and US consumers have increasingly made their personal information available over the Internet to companies operating all around the world.

Because of the central role that Fair Information Practices have played in the development of privacy law in the United States and the increasing importance of these principles for online commerce going forward, I believe they provide the appropriate framework to evaluate the bills now pending before the Committee.

Fair Information Practices Principles and Consumers

Strong legal protections built on Fair Information Practices satisfy the basic, common sense privacy expectations of consumers. The bills under consideration today follow the rubric of notice, "choice," access, security, and enforcement when discussing Fair Information Practices. While this is not a complete list of the obligations that can be found in US privacy law, it is a useful framework for evaluating privacy measures. All three bills present various approaches towards upholding Fair Information Practices and establishing baseline standards for Internet privacy.

Notice

The first principle of privacy protection is that a consumer should be provided notice of the collection, use and dissemination of his or her personal information. A privacy notice or a privacy policy should tell a consumer when his or her personal information will be collected, the purpose it will be used for and whether it will be disclosed to a third party. Simply put, a privacy notice should be a basic description of what information a company collects and for what purposes.

The problems with current privacy policies have been brought up by the Committee in earlier hearings. They tend to be long, confusing, and full of obscure legal language. It is ironic that a principle intended to make consumers aware of privacy practices has been subverted to one that misleads and frustrates consumers on a regular basis. There is the additional problem that companies have found it too easy to change privacy policies when they wish. This was the problem with Doubleclick that gave rise to the FTC investigation.

Furthermore, although notice is an important part of a privacy policy it does not by itself constitute privacy protection. Notice must be accompanied by the other principles of Fair Information Practices. This point was made clear in EPIC's recent report "Surfer Beware 3: Privacy Policies Without Privacy Protection". This study found that while the vast majority of high-traffic e-commerce sites had privacy policies none of those sites displayed a privacy policy that provided the full range of Fair Information Practices [13].

S. 2928, the "Consumer Internet Privacy Enhancement Act", has the most extensive discussion of notice in comparison to S. 809 and S. 2606. However, it is possible that the amount of information that this bill requires to be disclosed will likely overwhelm the average Internet user. The speed and convenience of shopping online will quickly hit speed bumps if all consumers are expected to read such notices before transacting business. Consumers should be assured that baseline principles to safeguard their privacy apply to every site they visit. They should not be burdened with having to examine and comprehend each line of a privacy policy before they decide whether or not to transact business with that specific company.

The notice provisions of S. 809, the "Online Privacy Protection Act of 1999", and S. 2606, the "Consumer Internet Privacy Enhancement Act", are less burdensome but neither are perfect. While S. 2606 specifies that notice should be "clear and conspicuous", S. 809 prudently requires that contact information is provided. While the legislative construction would be difficult, notice should be able easily understood by most consumers. Of course, contact information should be included as well.

In addition to this basic analysis of notice, S. 2606 properly addresses a growing trend of Internet companies that unilaterally change privacy policies on their customers. The requirement of notice of a policy change and consent before information can be used in accordance with the new policy would ensure that companies could

---

[12] *http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM*

[13] *http://www.epic.org/reports/surfer-beware3.html*

not change terms on their customers. Furthermore, it would force companies to think more carefully the first time they write their privacy policy.

Consent

The principle of consent is based on the view that if a consumer provides information for a particular transaction it should not be used for another purpose without first obtaining the consent of the consumer. The purpose of this requirement is to ensure fairness and transparency and to prevent the type of "bait and switch" that can easily result if a consumer is led to believe that a disclosure of personal data is necessary for a transaction when it will in fact be used for another purpose. If I provide my name and mailing address so a book I ordered online will arrive at my house, the information should not be used for another purpose without my permission.

Opt-in means asking the consumer's permission before information is collected or used. Opt-out means that a consumer will have to go through a long, burdensome process to tell a company that she doesn't want information used in a particular way. Which one will help a consumer control her information? Which will encourage companies to make it as difficult as possible to let her exercise that control?

We support opt-in as a common-sense standard that will give consumers a fair chance at controlling their personal information. The affirmative consent requirement that would be established by S. 2606 is a "consumer friendly privacy standard" that allows for individuals to rightly decide how their information held by others should be used.

The exceptions in S. 809 for consent present an issue that the Committee should consider. S. 809 excludes "transactional information where identifiable information is not removed" from its consent requirement. While S. 2606 establishes that personally identifying information may only be collected and used with consent, a great deal of information is collected and tied to unique identifiers.

While it does not establish an opt-in, only S. 809 recognizes that "transactional information" or clickstream data should be considered personal information. Within the bill, personal information includes "information that is maintained with, or can be searched or retrieved by means of" other identifiers. Transactional information is data generated by online movements—pages visited, searches conducted, links clicked—and has been at the center of recent privacy controversies over online profiling. Not including this information as part of an online privacy bill and protecting it would overlook a major concern of Internet consumers.

Access

One of the critical requirements of genuine privacy protection is to ensure that consumers are able to see the information about them that is collected. The right of access, which can be found in laws ranging from the Fair Credit Reporting Act to the Privacy Act to medical privacy laws across the country, is oftentimes the most effective way that individuals have to monitor the collection of their date and to object to inappropriate uses of personal information.

Businesses sometimes object to providing access because they claim that it is too costly. But it is also possible that many organizations simply don't want to actually show their customers how their personal information is actually used. This is a risky strategy that we believe online companies should avoid.

In the online world it is much easier to provide access to profile information. Many websites today, from airline reservations to online banking, are making information that they have about their customers more readily available over the Internet. Many of these companies realize the importance of ensuring the information they have is accurate and developing a transparent and accountable business-customer relationship.

But we need a much broader right of access in the online world because some bad actors are taking advantage of technological tools that are beyond the knowledge of most Internet users. The online world enables far-reaching profiling of private behavior in a way that is simply not possible in the physical world. This became clear during the past year over the debate with Doubleclick and it is today a critical issue with Amazon.

Any company that creates a persistent profile on a known user, or that could be linked to a known user, should be required to make known to that user all of the information that is acquired and how it is used in decisions affecting that person's life. The profile should always be only "one-click" away—there is no reason on the Internet that companies should force users to go through elaborate procedures or pay fees to obtain this information about them.

It would also be appropriate in many cases to give individuals the right to compel a company to destroy a file that has been created improperly or used in a way that

has caused some harm to the individual. Data could still be preserved in an aggregate form, but individuals should be able to tell a company that they no longer have permission to make use of the personal information that they have obtained.

S. 2606 provides the most robust right of access. Providing "reasonable" access to personally identifying information and the ability to correct or delete information allows the consumer to control what happens to her data.

S. 809 is better than S. 2928 on access, though the numerous exemptions create several problems. Transactional information, especially where identifiable information is not removed, has received some of the greatest recent attention as mentioned above via online profiling. Personal information that is used internally or confidentially is the type of information that should be most subject to access since it is used outside the realm of normal customer interaction. If one of the goals of access is transparency, the information which is most hidden should be brought to light. The other exceptions for discarded data and data that has no impact seem redundant or unnecessary. The presumption of access is that if personal information is held by a company, it should be provided to the consumer. Discarded data is not held by a company and whether data has impact should be a question the consumer should answer.[14]

Enforcement

Perhaps the most important element of Fair Information Practices is enforcement. Absent an effective means to ensure compliance, privacy principles will have little impact on business practices.

The key to enforcement is the independence of the enforcer. Self-regulation has been an incomplete solution to privacy protection due to this lack of independence. A company overseeing its financial supporters will not be effective or independent. In our view, the Safe Harbors created by both S. 809 and S. 2928 lack sufficient oversight to ensure privacy protection. Privacy advocacy groups like EPIC have documented reasons to be concerned through its "Surfer Beware" reports.[15] If self-regulation had been effective, the FTC would not have reluctantly made its recommendation for legislation earlier this session and we would not be discussing 3 potential Internet privacy laws today.

All three bills allow State Attorneys General to police unethical companies that harm the consumers in their jurisdiction. However, all three allow the FTC to intervene in proceedings and permit its actions to take precedence over the actions of State Attorneys General. While we recognize the important role of the FTC in the protection of consumers, it still remains unclear whether it is the appropriate agency to safeguard privacy interests. Rather than putting roadblocks in the way of State Attorneys General, we should allow consumers to be protected by local authorities and other independent agencies that are available.

It is also important to ensure that individual consumers are able to pursue privacy complaints. For that reason, a right to private action with a provision of liquidated damages should be provided. This preserves the right of consumers to pursue privacy complains when necessary. While S. 2928 does establish a fixed level of civil penalties, S. 2606 establishes a private right of action, liquidated damages attorney's fees, and punitive damages.

None of the bills provide for the establishment of a privacy agency. S. 2606 goes furthest in establishing a FTC Office of Online Privacy but like the other bills rely on the existing section 5 authority of the Federal Trade Commission. The reliance of privacy guidelines on the FTC Act prohibiting unfair and deceptive business practices has not provided an adequate basis for the protection of privacy interests and has failed to develop simple dispute resolution procedures that could assist both consumers and companies resolve privacy problems.

Most consumers are not lawyers, computer experts, or privacy advocates. For that reason, many countries have created independent data protection agencies that answer questions and follow up on consumer complaints. In addition to providing invaluable assistance for consumers, a privacy agency can bring the consumer perspective to other government agencies and business groups. These agencies are also generally responsible for public education and international coordination with pri-

---

[14] For further comments on S. 809, see Testimony and Statement for the Record of Marc Rotenberg, Director Electronic Privacy Information Center, Hearing on S. 809, The Online Privacy Protection Act of 1999, Before the Subcommittee on Communications Committee on Commerce, Science and Transportation, U.S. Senate, July 27, 1999, [*http://www.epic.org/privacy/internet/EPIC_testimony_799.pdf*]

[15] EPIC, "Surfer Beware I: Personal Privacy and the Internet" (1997) [*http://www.epic.org/reports/surfer-beware.html*]; EPIC, "Surfer Beware II: Notice is Not Enough" (1998) [*http://www.epic.org/reports/surfer-beware2.html*]; EPIC, "Surfer Beware III: Privacy Policies without Privacy Protection" (1999) [*http://www.epic.org/reports/surfer-beware3.html*].

vacy agencies in other countries. In order to help consumers resolve complaints and to penalize unethical companies, they should have the power to take action when irresponsible companies breach privacy principles established in law.

Additional Issues

State Preemption

All three bills propose state preemption, though S. 2606 will allow for common law tort and certain other claims to go forward. Limiting the ability of states to develop additional safeguards to protect the privacy interests of their citizens is a dangerous precedent and has only occurred in a few statutes. By and large federal privacy laws operate as a floor and allow states, "the laboratories of democracy," to develop new and innovate safeguards as required.[16] We believe this approach should be followed with Internet privacy.

Additional Safeguards

In addition to the other substantive provisions to protect privacy on the Internet. S. 2606 also proposes important amendments that would update current privacy laws. The Video Privacy Protection Act would be extended to include all video recordings, recorded music, and book purchases. The Cable Communications Policy Act would be extended to satellite TV subscriptions. These are sensible recommendations that build on current laws.

Anonymity

Finally, although the bills do not directly address the issue of online anonymity, I would like to underscore that this issue remains one of the central challenges of Internet privacy. While anonymity does create some risk, the loss of anonymity in the online world could significantly undermine any legislative effort to safeguard privacy. We have noticed a disturbing trend in the last year with more and more web sites requiring registration and making use of new tracking techniques to profile Internet users. Legislative safeguards will help limit the worst of the abuses, but formal recognition of a right to be anonymous in the online world may be the most robust form of privacy protection in the years ahead.

Conclusion

We commend the Committee for the important efforts to address online privacy. We believe that S. 2606 provides the most robust framework to protect privacy on the Internet, that it is consistent with other privacy laws, and that it is in the interests of consumers and business to ensure a high standard for privacy protection in the world of e-commerce. We urge the Committee not to place too much value on privacy notices without other substantive safeguards. Privacy law is based on Fair Information Practices, a collection of rights and responsibilities that help safeguard the interests on consumers in the world of rapidly changing technology.

References

Articles, Reports and Web Sites

EPIC letter to FTC, Dec. 14, 1995 [*http://www.epic.org/privacy/internet/ftc/ftc_letter.html*]

EPIC, "Surfer Beware I: Personal Privacy and the Internet" (1997) [*http://www.epic.org/reports/surfer-beware.html*]

EPIC, "Surfer Beware II: Notice is Not Enough" (1998)
[*http://www.epic.org/reports/surfer-beware2.html*]

FTC, "Online Privacy: A Report to Congress" (1999) [*http://www.ftc.gov/reports/privacy3/index.htm*].

Doubleclick page [*http://www.privacy.org/doubletrouble/*]

Junkbusters [*http://www.junkbusters.com/ht/en/new.html#Ginsu*]

Jerry Kang, "Information Privacy in Cyberspace Transactions," 50 *Stanford Law Review* 1193 (1998).

Letter to Senator John McCain, August 1, 1997 (from Center for Media Education, Privacy Rights Clearinghouse, Privacy Times, Electronic Frontier Foundation, Consumer Federation of America, EFF-Austin, Consumer Project on Technology, Electronic Privacy Information Center, Privacy Journal) [*http://www.epic.org/privacy/databases/ftc_letter_0797.html*]

Joel R. Reidenberg, "Restoring Americans' Privacy in Electronic Commerce," 14 *Berkeley Technology Law Journal* 771 (1999).

[16] See, e.g., Video Privacy Protection Act (1988) 18 U.S.C. §2710(f), Cable Communications Policy Act (1984) 47 U.S.C. §551(g).

Testimony of Marc Rotenberg before the Subcommittee on Communications, Senate Commerce Committee on the Online Privacy Protection Act of 1999, July 27, 1999.

Paul Schwartz, "Privacy and Democracy in Cyberspace," 52 *Vanderbilt Law Review* 1609–1702 (November 1999).

Gregory Shaffer, "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards," 25 *Yale Journal of International Law* 1–88 (Winter 2000)

Books

Phil Agre and Marc Rotenberg, eds., *Technology and Privacy: The New Landscape* (MIT Press 1997)

Colin Bennet, *Regulating Privacy* (Cornell Press 1992)

David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (Chapel Hill 1989).

Priscilla M. Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (University of North Carolina Press 1995)

Marc Rotenberg, *The Privacy Law Sourcebook 2000: United States Law, International Law, and Recent Developments* (EPIC 2000).

Paul Schwartz and Joel Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (Michie 1996)

The CHAIRMAN. I thank you and I thank the witnesses for being here.

A great deal of the debate on this issue revolves around the issue of opt-in versus opt-out. I would like to hear all the witnesses' views of the advantages and disadvantages to both consumers and businesses associated with each of these approaches. We will begin with you, Mr. Cooper, and go down the line.

Mr. COOPER. Thank you, Mr. Chairman.

Hewlett-Packard has done a lot of work lately, in fact very aggressive work, in moving from an opt-out to an opt-in situation for our own websites. We have learned a lot as we are doing it. It is not as easy as we first thought. Very few things dealing with the Internet are. But we think that that is the way to go. It is certainly right for consumers. It is also, we think, a good business practice.

As we are doing this, we are finding that there are certain areas where opt-in may be difficult either because of logistics or because it then sets off other problems that kind of escalate down the road.

I think we have come to the conclusion that we think there should be sort of a reverse of what is now kind of the rebuttable presumption on opt-in/opt-out. I think now it is that everything is opt-out unless there is the decision either by the company or Congress or others that it should be an opt-in. We have certainly seen with financial services, with children, with medical records, those have turned into opt-in.

I think ultimately we could see where there should be the rebuttable presumption where everything would be an opt-in unless there were reasons that could be given that it should be an opt-out. So, we do not think that opt-in works in all cases, but we think that is probably where companies should go in their own personal uses.

The CHAIRMAN. Mr. Vradenburg.

Mr. VRADENBURG. I think we are only at the beginning of understanding exactly how to effectively give consumers choice. Your bill, Senator McCain, focuses on the ease of use and clarity with the choices offered and exercised. It neither uses the word opt-in or opt-out. I think that focus is right. How easy do we make the

choice and how clear do we make the information needed by the consumer to make that choice? A one-size-fits-all kind of approach here is not going to work.

In a number of areas, we too have moved toward an opt-in approach, whether it be in the financial area, where obviously people do not put their financial records online unless they clearly choose to do so, whether it be the medical and health area, where in fact the High Ethics Coalition has recommended opt-in policies for a wide variety of companies dealing with health care information, and clearly we did that in the children's arena. But in fact, I think to say that one-size-fits-all with respect to all of the information exchanges that are currently going on or may go on in the future is an unwise approach and that we ought to focus, as your bill does, on the ease with which consumers can both find, understand, and then exercise the choices they are offered.

The CHAIRMAN. Mr. Garfinkel.

Mr. GARFINKEL. Thank you, Mr. Chairman.

A few years ago, Bill Gates said that opt-in/opt-out was an irrelevant distinction. He said you could just put up a question and force people to answer it one way or another.

The CHAIRMAN. Do you agree with Mr. Gates' assessment?

Mr. GARFINKEL. No, I do not and I am about to explain why.

Since then we have learned that opt-in/opt-out is extraordinarily important. With opt-out, it requires that consumers be tremendously informed. I have been a computer security practitioner for about 10 years now, and for the first five, I thought that all the security problems would be dealt with when we properly educated people. But we have learned that you really cannot educate people. People just do not have the time. Many people do not have the ability.

With an opt-in system, it requires that the business explain to the consumer the value proposition to get the consumer to make an affirmative statement to share their information. If the business does not adequately explain what is going on, the consumer has no incentive to opt-in. With opt-out, it is just the reverse. The business has an incentive not to explain things clearly.

Now, let me explain this in terms of positional information, something I am extraordinarily concerned about. Every cellular telephone that is used in the world right now has to track the movements of its user because that is the way the cellular telephone systems deliver the calls. Now, it might be that the company is recording your positions over time and selling that information. If you have an opt-out regime, it is up to me to find my cellular company's privacy statement to read it to find out if they are selling my positional information rather than simply being told that they would like to do that and being given the choice.

We have recently seen that with the Sprint PCS. They have Web forms that you can do on your phone, and it was revealing personal information when people filled out their forms. It was revealing their phone number. People were never told it was doing that. It might have been on some privacy statement somewhere.

So, my feeling is that with the way Americans approach technology, an opt-in regime is the only one that really makes sense. It is the only one that is fair.

The CHAIRMAN. Mr. Rotenberg.

Mr. ROTENBERG. Mr. Chairman, I think opt-in is just common sense. I think if a company wants to take personal information that is acquired through a commercial transaction and use it for a purpose unrelated to the transaction, most people would think maybe I will agree to do that, but should you not ask me first?

What happens under the opt-out regime is companies realize that this information has a great deal of value and that if they actually have to go back and ask the customer, the person might object. So, they make it difficult and they discourage people from exercising any control.

I think it is not surprising, and in some ways commendable, that industry has moved toward opt-in, but I think if you legislate opt-in, you will, in effect, protect the good actors. If you do not, there will be a lot of bad actors running around taking advantage of weak opt-out policies.

The CHAIRMAN. I have one more question for the panel. Mr. Cooper, you want to respond to that.

The FTC would favor an approach that would provide them with rulemaking authority to regulate privacy on the Internet. Do you agree with that approach?

Mr. COOPER. First of all, one last thought on opt-in/opt-out. I think that your legislation has advantages that really have not been discussed to the degree that they need to be, which is clear and conspicuous. I think this is the important key to opt-out, and I think it is something that we need to do as quickly as possible. If the FTC has authority to insist that any privacy policy is described in a clear and conspicuous manner, then I think a lot of the problems that have been discussed at the witness table should go away because businesses cannot hide what their policy is. I think if you are going to do one thing, having clear and conspicuous privacy policies is the thing. The FTC does that for a living. They do clear and conspicuous on advertising, on used cars, on telemarketing, you name it. That is the front line of defense for the FTC on consumer protection.

As far as giving a rulemaking to the FTC, we are not too sure that they do not already have the power within their section 5 authority to do pretty much I think everything that you have described in your bill. If it requires a further working through of that, I would hope that it would be an open process where we would have either hearings before this Committee or some sort of hearing process before the FTC to ensure that there is that balance between their needs for protecting consumers and the ability of the marketplace to continue growing as it has.

The CHAIRMAN. Mr. Vradenburg.

Mr. VRADENBURG. Mr. Chairman, I have gotten somewhat distrustful of the FTC's rulemaking authority recently, and I would say this: It does seem to me that Congress is going to set the policy here, and if the policy is notice and choice, as I think it should be, that is a market-driven choice where basically companies will be out there clearly and conspicuously giving notice of precisely what information is being collected, how they are using it, what choice is being made.

My concern with additional rulemaking authority beyond the traditional enforcement power of the FTC is that we will get into a debate about what size the font ought to be, exactly how many scrolls you ought to be able to go through, how you put it on the cell phone. What we will end up doing is constraining the innovation that is going on in the marketplace by depriving the consumer of a variety of choices simply because the FTC has described with excruciating detail precisely all of these elements in a way that will make innovation and continued technological progress in this industry and, indeed, new choice techniques and methodologies and technologies continue to evolve on the marketplace.

So, I am in favor of your approach in your bill, which is a notice and choice approach, with clear and conspicuous disclosure, with enforcement authority, believing that that gives the marketplace its maximum capacity to continue to innovate in this area and at the same time give confidence to the American people through this body that, in fact, there are some baseline standards being set in this arena.

The CHAIRMAN. Mr. Garfinkel.

Mr. GARFINKEL. Thank you, Mr. Chairman.

I have long said that Congress should not be making legislation on cookies, that it is far better for a regulatory body to make those decisions. I think that the technology is moving very fast and that a regulatory body is able to respond to the changes in technology more quickly than Congress can respond to it. So, I would think that would be a very good place for the rulemaking authority, to be with the FTC.

At the same time, I do have some concerns about the FTC largely because they are relating to trade, and I think that there are issues on the Internet involving privacy that the FTC is not concerning itself with, like the way nonprofits collect information on the Internet. That is why I would ideally like to see the creation of an independent organization to do that within the government. But given the choice of not giving the power to the FTC or giving the power to the FTC, I think that giving it to the FTC and funding a privacy office within the FTC so we can have a set of experts there who are resources for the rest of the federal government would be the best solution.

The CHAIRMAN. Mr. Rotenberg.

Mr. ROTENBERG. Mr. Chairman, I actually do not favor FTC rulemaking authority in this area. I think the better approach is to establish the statutory obligations to give people the private right of action and to allow the FTC to do enforcement. But my assessment is that when we do these very detailed regulations with elaborate participation, as it should be, from all the stakeholders, we end up with a set of rules, as Mr. Vradenburg has suggested, that become very time-bound. They work today but they may not look as good a couple of years out.

One of the remarkable things about U.S. privacy law, whether it passed 5 years ago, 10 years ago, or 25 years ago, is that it has been aging pretty well. As long as we stay away from specific technologies, as long as we do not build privacy laws tied to the technology of the day, I think that is the more durable approach over time.

The CHAIRMAN. Thank you.

I think one thing that is clear from this hearing and from the statements of the Senators and Members of the Committee, as well as the witnesses, is that there is a wide division of opinion as to how we address this issue. There is agreement that it is an incredibly important and challenging issue that continues to grow daily. There is not a consensus yet. We may have to, in January, have another set of hearings in order to try to build consensus on this issue.

But I also think that there is a compelling argument that we not remain dormant here without acting on the issue. As every day Internet users increase, the fact is that this issue becomes more and more important.

We have never passed a bill that I can remember out of this Committee directly on partisan lines. In fact, both sides have different views on this issue, but we have usually tried to reach consensus because it never moves if we do not get it out of Committee with an overwhelming majority. So, I think the hearing today, the statements by the Senators, as well as the witnesses indicate that we have a ways to go before we have consensus on this issue.

Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. I agree with the statement you just made as well.

A question for you, Mr. Cooper and Mr. Vradenburg. This is an effort to find this consensus the chairman talks about. Are the two of you against including access and security in a bill at this point? Just yes or no I think would be helpful because then I am going to ask you to explain it in a minute.

Mr. COOPER. Well, in a sense it is in the chairman's bill. It just goes to a study for a report back to Congress.

Senator WYDEN. But other than a report, you would not favor any action at this time.

Mr. COOPER. We think those issues are too complicated to decide within legislation.

Mr. VRADENBURG. I agree with that.

Senator WYDEN. As you know, in the Burns-Wyden bill, we include access and security in an effort to try to give a lot of flexibility for business and the like. Especially the access issue is so key because if a consumer's profile contains mistaken or fraudulently obtained information about a sensitive topic, credit or medical information, there is a question about how they would ever correct it if they did not have access to it. I understand your concerns, and you all have been very thoughtful in terms of dealing with us.

What I would like to do is ask Mr. Rotenberg and Mr. Garfinkel to tell us why they think it is workable to do access and security, and then have the two of you respond to that in the name of, again, trying to find the kind of common ground the chairman is talking about. Mr. Garfinkel and Mr. Rotenberg, why do the two of you think it is possible to address access and security now?

Mr. ROTENBERG. I think the main point, Senator, is that in this highly dynamic environment where companies are still exploring a lot of different ways to take advantage of the new technology, people are finding it not so difficult to provide extensive information to their customers that in the past would have been impractical or

too expensive to provide. You can go online today and see a profile of information that the airline company that you deal with or the hotel that you make reservations with or the bookstore that you buy from collected. All the information that they have about you or, I should say more precisely, most of the information they have about you is now available to you. That is possible because the technology is changing today and makes it possible for companies that say we value access to do this.

Now, there are certain types of information that are not being made available and then there are certain companies like the online advertisers who have made it particularly difficult to find these profiles. But I think the key point here is that the technology makes it much easier today than it had been in the past to make access real.

Mr. GARFINKEL. I want to amplify what Marc says with two examples.

The first example is from online advertising. The online advertisers build a comprehensive profile of a person viewing an Internet site, and they use that profile to decide what advertisement to show the individual.

Now, a way to deal with the access and the security issues are the information on the user's computer, the cookie that pulls into that profile, could also be used as a kind of password to access that profile. The computers that are serving up the advertisement have the possession of all that information, and they could very easily display the information at the same time or at another time with another form rather than simply using that information internally and then not displaying it.

Technically, access is very easy to convey. The security techniques that we have come up with on the Internet that we have said are sufficient for downloading credit card information, sufficient for viewing other kinds of highly confidential information online should provide the same sorts of security provisions for personal information when you are showing that to the user.

Now, if you look at Amazon, Amazon has a tremendous amount of personal information that they record. One of the things that they record is every book that you have ever purchased, and they use this for making recommendations when they show you other books. You can ask for recommendations. One thing you can do is you can go to a Web page on the Amazon system and see the list of all the books that you have ever purchased, and if you want Amazon to strike one of those books so that there will not be a record, they allow you to delete it. Now, what I do not know is if it is actually deleting it inside Amazon's computers or not or if it is simply deleting it from what it shows me because Amazon is not really known as a strong privacy player.

On the other hand, the fact that they are doing this and making this capability available to consumers—and I have used it and it seems to work—leads me to believe that these are not insurmountable hurdles. They are in use now by some of the corporations that are doing business on the Web.

Senator WYDEN. Mr. Cooper, Mr. Vradenburg.

Mr. VRADENBURG. Senator, I think the difficulty here is more pragmatic than anything else. It is a matter of whether or not one

can develop adequate access standards and decide when they apply in what circumstances and where we may not create a greater danger to privacy than we create a user opportunity to see their own records.

Regarding security, I think it is just a difficulty of setting those standards. We have tried that inside the industry and we have tried that inside government and have been unable to do so.

Let me come back a second to access. We do not use navigation information on our service. We do not use it for marketing purposes. We do not sell it. So, the only purposes that we would ever use that information for internally are aggregated information and, indeed, really to improve the service by finding out exactly in aggregate where people tend to go and why they tend to go there. As a consequence, none of our files are organized by a member, by a user. To require access would perhaps cause us to have to create files that do not now exist to make things more accessible not just to the average user, but to the average hacker.

So, our problem and concern here is less sort of the principle than the pragmatic effort to get at what it is that people are to have access to, under what circumstances. The easier you make it for the average user of the Internet to get access to their information that may be disaggregated inside our files is to make it more accessible to hackers.

I would also say, not in any adversarial way, one ought to try and apply the standard to government. That is to say, I say that not with an effort to say government is lousy and we are great. I am just say to really apply the access standards that you would adopt, go to your federal government agencies and say, apply this access standard, and figure out whether or not you are creating more danger to government users and government records than you are creating an opportunity to use.

We saw this with Social Security records about a year ago when there was an effort to provide more information to users and more information about the file, and the great concern was that those were hackable and that the information has become more widely dispersed. Thus, there was a greater danger to privacy in making access available, easier to users because it was easier to get at by hackers.

So, this is a pragmatic problem that we address. We do not think that the state of affairs is ready yet to address this in federal legislation, and that is why we do not think it ought to be embraced. That is why we have supported Senator McCain's approach.

Mr. COOPER. We are always nervous when somebody says that there is a simple solution to a technical Internet problem because it may work in the first case or the first 10,000 cases, but when you try to scale these things with companies that have very different kinds of approaches and they have artifact systems and they have very different data bases or completely non-interoperable data bases, trying to find a simple solution that will fit all these I think is going to be a problem.

I think what the FTC Advisory Commission on Access and Security was able to describe was I think a direction where we can work through those problems. They did not reach conclusions, but I think they raised all the right questions. But I think if we turn this

over to a study, a reputable study and one that reports back to Congress on a date certain with a recommendation to Congress, I think that will certainly get our attention. I think it will get every other companies' attention. I think we can work through probably to some kind of finality.

Senator WYDEN. Mr. Chairman, I know my time is expired. The reason I ask about these two points is I do not think you can go to the American people in a credible way without a provision involving access. I think you know, as a result of the efforts that we have worked on together, that I want to do this in a bipartisan way. I think what Mr. Vradenburg has said with respect to ensuring that this is pragmatic is absolutely right.

But particularly with respect to this access question, I do not see how you can go to the public without some way to get the ability to get the chance to see that personal information. I look forward to working with you on a bipartisan basis.

The CHAIRMAN. Senator Burns.

Thank you, Senator Wyden.

Senator BURNS. Along the same line as Senator Wyden's questioning—by the way, thank you you for coming today. Just listening to the exchange, I happen to agree with the approach that Senator Wyden and I have taken on access. It also points to what you have remarked that it gives some concern to hackers and this type of thing. We have talked about encryption ever since I have been here, and the security measures that we have to take in order to make ourselves secure. Yet, we keep getting some feedback on strong encryption legislation. I think they go hand in hand. I think as we go along with collecting this information that we have to figure out some way to make it secure.

Let us talk a little bit about the statement that you put up with regard to your privacy. How many people actually download that thing and read it and understand it? No matter if you are an opt-out or an opt-in, it makes no difference on your approach.

Mr. VRADENBURG. I do not know the answer to that, although we probably can provide that information to you, Senator. But there are a rather substantial number of hits to that and to the keyword privacy preferences on AOL and it is read quite widely. Whether we can actually provide you numbers is a good question, and I will look into that.

Senator BURNS. I know you cannot provide the numbers of people who want to read all the legalese and interpret it.

Mr. VRADENBURG. We have tried to set forth eight principles, which are relatively straightforward, on one or two pages and then have links back to deeper information if people would like to understand more about it precisely for that reason because, indeed, one of the problems here is to be clear with your customers. And to be honest with them, you have to be as comprehensive as you can be, and that requires some length, and you would like to lift out of that some basic principles that you can get, and if you have need for deeper information, you can get that too. So, how to present this in a way that is easy to read is a challenge. We think we have done that, but I recognize that it is a challenge.

Senator BURNS. Mr. Rotenberg, you would like to comment.

Mr. ROTENBERG. Senator, I was going to make two points. First of all, I think there is a particular problem with notice for Internet privacy from the consumer viewpoint, which is if you think about buying a car or some other big transaction, yes, you are going to read all the details——

Senator BURNS. I do not do that. I buy my cars in garage sales. [Laughter.]

Mr. ROTENBERG. Well, that is even better.

But, of course, if you are on the Internet, and you are going from one website to another—this is more changing than channel surfing on a television, if you find something interesting, you want to go on to the next website. The question is should you have to check the privacy policy before you start reading information from a website.

Now, some people suggest that maybe the solution to that problem is to automate it, but my concern about that approach and the reason that we have not been supporters of P3P is I think people are going to find pretty quickly that once they have a few websites that they want to get to with low privacy policies, they are going to have to turn down their privacy dial to continue surfing. So, that is one kind of problem. You move very quickly from one website to another.

Another kind of problem is that companies change their privacy policies. They may begin with a good notice. Amazon, for example, when they started, they said, we will not disclose your personal information to third parties. We said that is a good privacy policy. We are a privacy organization. We were actually one of their first affiliates. They have got hundreds of thousands now. We were one of the first groups online selling books with Amazon. A couple weeks ago, they said, well, we have changed our privacy policy and we can no longer give you that assurance. What do we do with that?

Senator BURNS. Mr. Cooper, and then I have a followup question.

Mr. COOPER. Very quickly. Again, I think that clear and conspicuous is the key here, and that is a term of art to the FTC and we think it is very important that they have that authority to go in and make sure that whatever somebody says is clear and conspicuous.

We think the other thing that should be done is joining a seal program. We have the Better Business Bureau seal on all our websites. It was a hard program to come under. We think it is sort of the gold standard for seal programs. It took a lot of work to get all our websites underneath that, but we feel very confident now that when people see that seal, that they will recognize that they are dealing with a reputable company.

Senator BURNS. I want to ask you, do you think Senator Wyden's and my approach—we do not make it clear enough on the opt-out situation? It is not clear?

Mr. COOPER. I think you and Senator Wyden have targeted exactly those issues that need work on next year and that we, as businesses, should be engaging with you and this Committee to find those answers, or at least find the approach that will lead us to those answers.

Senator BURNS. Thank you very much.

Now, with saying that, give me your assessment on safe harbor. Do you support safe harbor, and why has the majority, I would say, of the industry been reluctant to accept safe harbor legislation in this area.

Mr. COOPER. Speaking again for HP, we think that safe harbor can be very useful because the FTC—and even with the State attorneys general being able to enforce any FTC rules—you do not have the eyes and ears you need to make sure that this marketplace is going to be clean and well-lighted. I think you need to have things like third-party enforcers to be able to help police this market as well. So, I think the idea of having the FTC being able to vet third-party seal programs is a very good one. We would hope it would be a very high standard. Again, we think BBB would certainly meet that.

What you get from that also is that—and BBB does this with the FTC already—that if there are patterns of abuse, if they find that a company has got a constant series of complaints against them, each one perhaps not a very high level, but that pattern creates what they think is an abusive technique, they will pass that on to the FTC or the AG's as well. That might not show up coming down from the enforcers themselves. We think that third party can be very useful.

The CHAIRMAN. I want to apologize to my colleagues. I have been informed there has been an objection voiced on the floor to the hearing. We are going to have to be done in a half an hour, and we still have another panel of two witnesses to hear from. So, I would appreciate it if we could stick to a five-minute rule so that we at least can get the second panel's questions.

Senator BURNS. Thank you, Mr. Chairman. I have no more questions.

The CHAIRMAN. Thank you, sir.

Senator Bryan.

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

Mr. Rotenberg, let me ask you. You have had some reservations about FTC rulemaking, you indicated previously. You talk about the need for clear notice in terms of what the website is offering. How do we get that clear, understandable notice so customers or consumers can intelligently inform themselves, and what problems, for example, have occurred with respect to the rulemaking of the Children's Online Privacy Protection Act?

Mr. ROTENBERG. I think in terms of notice, a baseline requirement for clear and conspicuous notice of use and collection and so forth takes you pretty far.

Senator BRYAN. How do you define that? How do you enforce it if you do not have an FTC rulemaking?

Mr. ROTENBERG. Well, we have done it in other areas. The Cable Act, for example, has a notice requirement that has been litigated, and courts can take a look at that language, as they do in other areas, and try to give a reasonable interpretation. I think it is actually a good approach because it builds in some flexibility.

Now, in fairness, I think the FTC did a good job with the Children's Online Privacy Protection Act. It was a tough bill to write regulations for because of the technology and because of the range

of issues that the bill sought to address. I thought they did a good job.

But I think going forward, given the choice between FTC rulemaking and a good set of statutory principles that courts and others could come back to, the second will give you more flexibility.

Senator BRYAN. You believe that if we define what is required by notice by congressional act as opposed to delegating that authority to the FTC is likely to give us more flexibility?

Mr. ROTENBERG. In fact, Senator, that is what we have typically done with privacy laws, not generally with consumer protection because there are a lot of regulations and rulemaking procedures. Interestingly, we are big privacy advocates, but we are not necessarily in favor of a lot of regulation. If there is a way to establish legal rights, make those principles clear, create incentives, I think it is the better approach.

Senator BRYAN. Mr. Vradenburg, let me ask you about—there are two different spellings. One on the notice indicates that there is an N in his name and the other indicates there is not. What is the correct pronunciation?

Mr. VRADENBURG. Vradenburg, no N in there.

Senator BRYAN. So, the information here is incorrect and the information on our notice is correct.

The CHAIRMAN. We will fire one of the staffers.

[Laughter.]

Mr. VRADENBURG. No less a punishment.

Senator BRYAN. I would ask that this part of the colloquy not be subtracted from my five minutes.

[Laughter.]

Senator BRYAN. Mr. Vradenburg, the legislation that a number of us have supported, the S. 2606 option, defines data in two different categories. One is personally identifiable. With that, we say there is an opt-in requirement.

Now, let me ask you this. Among those personally identifiable information definitions would be included the individual's first or last name, his home or other address, telephone number, Social Security number, a credit card number. Why shouldn't the consumer have the right to require that his or her affirmative consent be given before that information be collected? We are not talking about all data. I want to make sure the record is clear.

Mr. VRADENBURG. Well, Senator, actually I speak only from AOL's experience. Quite clearly that information is obtained only with the consumer's consent because they have to give us that in order to sign up with the service, and they clearly have made a choice to do that, with the exception of Social Security information. But certainly name and address information and telephone number information is given to us right up front. We obviously do disclose at the time exactly what use we will make of that information and the fact that we do not disclose it to third parties except subject to that opt-out requirement.

But I am not sure then what the issue is because clearly the consumer is choosing to give us that information.

Senator BRYAN. But I do not understand your response. If that is the policy that you are following currently—that is, you are, in effect, giving the consumer the ability to say, look, I do not want

this information collected with respect to this type of information—why not provide a statutory protection for the consumer? What is the objection to that? We are not talking about all information. We are just talking about this personally identifiable information. What would be the objection?

Mr. VRADENBURG. I guess, Senator, I am misunderstanding the character of the issue here because clearly, in order to sign up for our service or any paid-for service, you are typically going to get that kind of information. The consumer clearly is going to make a choice whether or not to give up that information or to subscribe to the service.

If the question then is should they not be given an opt-in or an opt-out or some choice before that information is then redisclosed to somebody else outside the company, I agree with you that the consumer ought to be given a choice. At AOL, we make that choice available to the consumer, disclose to them up front that if they do not wish us to make it available to others by means of renting lists of our subscribers to others, that they can opt-out and quite a few of them do.

Senator BRYAN. Well, but that is opt-out, not opt-in. I think we are playing games here with the words. In other words, what opt-in requires is that you must get affirmative consent, not notify them, look, if you do not want us to do this, give us a call in some fashion. I am asking what is wrong with that, particularly with this kind of information, Social Security card number, telephone, credit card? Why should the policy not be that you have to get their prior consent before you disseminate——

Mr. VRADENBURG. Well, Senator, this is a matter of terminology. I do not want to get into a vocabulary debate. The question is whether you get the consumer's consent, and I think we do and we do in our processes get the consent. We do it through an easy-to-use, easy-to-find, easy-to-make-a-choice system online on our system. So, the vocabulary of opt-in and opt-out gets us boxed into whether or not this is going to be an easy-to-use choice on the part of the consumer.

Senator BRYAN. Let me say that this is a complicated area. I am the first to acknowledge it. Consumers are not confused. An opt-in requires you have got to get the affirmative permission before rather than saying, in effect, silence is acquiescence, and that is the effect of opt-out, is silence is acquiescence. If the consumer does nothing, you are interpreting his or her silence as giving you the right to do that. I do not think most Americans would view that as much protection.

Thank you very much, Mr. Chairman.

The CHAIRMAN. Thank you.

Senator Rockefeller.

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

Senator ROCKEFELLER. Thank you, Mr. Chairman.

Mr. Cooper, you indicated that you favor protection for the consumers. I want to do a little bit about opt-in. You support opt-in for anything that has to do with medical records. Correct?

Mr. COOPER. Yes. It is already I think a given.

Senator ROCKEFELLER. And you support it for financial records. Correct?

Mr. COOPER. Yes.

Senator ROCKEFELLER. Do you support it for religious affiliation?

Mr. COOPER. I am not too sure what the context would be. What we have done within HP——

Senator ROCKEFELLER. It is not a very complicated question.

Mr. COOPER. That would not be a question that would be asked of somebody, by our company——

Senator ROCKEFELLER. What about political party or beliefs?

Mr. COOPER. This is what I was afraid of. It is sort of the slippery slope and where is that line drawn? What I can say is that somewhere along that line, that line should be drawn, and I am not sure exactly where that should be. But we would certainly say that that is where I think the debate should be.

Again, back to the point I made earlier, I think we have to flip that rebuttable presumption. In other words, I think you should have to show the reasons why things should be left as opt-out as opposed to the rebuttable presumption that it will be considered opt-in unless there are other reasons. Some of it may be logistic, just you have different data bases out there.

I understand where you are taking that question, and I think we would agree that it would be the obligation of companies to say where that line should be and why it was important to have it as an opt-out rather than an opt-in.

Senator ROCKEFELLER. What about ethnicity? Should that be opt-in?

Mr. COOPER. I think it comes back to use of that information because obviously the Census or a lot of other groups will take that information and aggregate it. So, a lot of this is how this is going to be used.

Senator ROCKEFELLER. I find those answers troubling, as I find your earlier statement that this is going to be very hard to do in terms of technology. Of all the people in this world to say this is going to be difficult to do from the technological point of view—and I think you, Mr. Garfinkel, said that access just is not that difficult and the rest of it. I just find that not very compelling.

I do not have anything against commissions. I have served on a Medicare commission, a children's commission, a coal commission, all kinds of commissions. The problem is that commissions tend to be an amalgam and they do not come out with sharp things because there is always dissent because they are so carefully picked that they are almost doomed to fail at the very beginning.

So, when you say these are very hard to do from a technological point of view, things are not as simple as they would seem, of all the industries, yours would be the last one that I would expect to hear that from.

Mr. COOPER. Well, not that they are impossible to do because we can do them, but I think we have a better sense of where the difficulties are, and we would certainly want to share that with any group that is coming up with recommendations.

What we like about the National Academy of Sciences is that it avoids just exactly the kinds of problems you mentioned as being difficulties, which is that you have an amalgam of different groups

that kind of cancel each other out. We would want to have, an expert body, because we consider ourselves an expert company on the Internet, that we could work with and consumer groups could work with, to come up with those recommendations to Congress, again at a date certain.

We are not saying that you cannot do it. I think this is one of the problems that business has gotten itself into, is that we have come up as a group to the Congress and said, "you cannot get there from here." At HP, we think you can.

Senator ROCKEFELLER. I have got to hurry and I apologize to you.

Suppose I have had cancer and it is in a data base, but it has been in remission for 10 years, move a little bit out into the future. I want to go in and take that out. Or let us say that I have diabetes, and then for some miraculous reason, somebody discovered the cure for diabetes and it went out. Do you not believe that I should have the right to go in and correct that information, eliminate that information?

Mr. COOPER. I think you should have the right to correct any information that could identify you or certainly that is wrong. But we have found some State actions, where they have gone into medical privacy issues. You want to be careful how you approach this because you could end up taking out data that is used in the aggregate to identify problems with certain areas, such as how the structures of diseases are evolving. So, you want to make sure that you do not take this information in the aggregate and not be able to use it in ways that will serve people in general terms.

Senator ROCKEFELLER. So, that would be one of the advantages then of the Hollings bill that I support, and others could have this in their bill too. We would preempt States. It would be one standard for the whole country, so you would not have to worry about that, would you?

Mr. COOPER. Well, all three bills include that, but we definitely think that aggregated information can be very useful to individuals, the economy as a whole, and the Nation as a whole.

Senator ROCKEFELLER. I happen to believe in access and security very strongly. What is the point of having all of this if it is not really secure? You say the seal, the gold standard, all the rest of it. What is the point of having any of this if it is not secure? Why would any bill leave out security?

Mr. COOPER. Well, again we think that has to be addressed and we think that we are getting close to what the answer should be. We do not think that through the Committee process we will have all the right answers certainly this Congress.

Senator ROCKEFELLER. We are not going to pass this in this Congress. This will not get passed until the 107th Congress. It will be passed.

Mr. COOPER. We think there will be legislation at the federal level as well.

What we would like to see, is that extra step, of a year study within the McCain-Kerry bill to create the vetting process that we think will reach the right answers.

Senator ROCKEFELLER. But you do agree that the security aspect is absolutely necessary.

Mr. COOPER. Yes, we do, as well as access. Those answers have to be discovered to make the Internet work for consumers. How we get there I think has to be at least an open process so that the best answers can be discovered rather than the easiest answer.

Senator ROCKEFELLER. Mr. Rotenberg, just very quickly. In that I am detecting a certain ambivalence in the answers and, to be frank, wanting to have it both ways, could you comment on what Mr. Cooper has said?

Mr. ROTENBERG. I am sorry, Senator, which point? Regarding the need for access——

Senator ROCKEFELLER. Yes. In other words, yes, we want to have security, but yes, we want to have the commission. Yes, we want to take our time. There will be legislation but we need to look at these things carefully. This could be difficult to implement. Who knows what the consequences will be?

And we are not talking about telephone books. I did an interview yesterday and somebody said the U.S. Chamber of Commerce—wait a second. You have telephone books. Look, that was then. That was like 30 centuries ago. We are talking about worldwide millions, hundreds of millions of people.

Mr. ROTENBERG. As I suggested earlier, I do not think there is any question in anyone's mind at this point that privacy protection is the No. 1 issue facing the future of the Internet. This is everywhere that we read and in the polling and you ask consumers, what is your view about the Internet. It is exciting. It is great technology. It is a business opportunity. But am I going to lose my privacy? I do not think there is any question about the importance.

Now, on the access issue, I have to say it is a little amusing and maybe, sir, this was your reaction as well. You can go online tonight, if you do financial trading or bank records, you have a tremendous amount of information online. A lot of businesses have figured out how to make it possible for you to get to your bank account information, to write checks, conduct trades, give you access and provide you security. The thought that at this point we need to create a study group to figure out how to get that done—it is like turn on a computer and go to one of these online brokerage firms. It is being done. The question is, why is it not more widely done? Why can it not be routinely done?

Senator ROCKEFELLER. Thank you. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Cleland.

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

Senator CLELAND. Thank you very much, Mr. Chairman. Thank you for the hearing.

I guess my instincts about telecommunications go back some 30–32 years ago when I was a young signal officer in Vietnam and realizing that if you could not communicate securely, bad things were going to happen. It does seem to me that in the world of the Internet, where we have connectivity, where we do not have just one-way communication—say, looking at a television that is one way. If I voluntarily want to be part of the Nielsen ratings, I can have a little box sitting on my TV and I voluntarily opted in for somebody somewhere to follow the patterns of my television viewing. I

opted in. But if I did not want to be part of the Nielsen ratings or some other ratings system, I would have just sat there and enjoyed, in the privacy of my home, watching television.

It seems to me with the Internet and what has been described as the breaking down of walls, breaking down of barriers, and this open playing field here, that it is a two-way communication, and that when I access the Internet, I think most of us still feel that it is a one-way, that we are getting some good stuff. We access a lot of interesting things. It is fascinating. We can play with it. We can surf it. We can do a lot of good things. Basically I do not think Americans are aware that somebody else is watching them while they are doing that. I think therein is the rub.

The FTC found that some 92 percent of consumers on the Internet are concerned and some 67 percent—that is two-thirds—are very concerned about the potential misuse of their personal information online. The personal information is if you buy something online, you put your credit card on there, Visa, American Express, whatever. That is personal information.

Fifty-seven percent of Internet users have decided not to purchase online due to privacy concerns.

I think we are at one of those watersheds here where we either work to enhance confidence about the use of the Internet and being online or else we will see online usage attrit or not used to its fullest potential, as you pointed out.

It is called privacy but I guess another way to look at it is secure communication. Basically I think American consumers assume security until they find out differently. So, in many ways I think that is the baseline. They do not assume that someone is watching them do their thing. So, that is where I get a little bit confused here because my assumption is that when I pay for a service and I access it, that my transactions are going to be private unless told otherwise. It is when I pick up a telephone. Some government agency cannot listen in on my telephone or track my telephone conversation without my knowledge or a court order. We have this pretty much ingrained in our thought process.

So, quite frankly, I do not know whether to opt-in or opt-out. If it is a jump ball every time I click on, I do not know whether I am being watched or not being watched. I do not know whether they are going to sell it to somebody else I do not want to sell it to or not. Then if I access the privacy code, then that could be changed tomorrow based on their view not mine.

So, I think we are touching a raw nerve here with American consumers who would love all the benefits of the Internet and American business that would love all the benefits of the Internet. And I am all for that. We just have a wonderful tool here, but we just have to make sure that we keep American confidence or consumer confidence in the Internet alive.

Therefore, we need you all to help us walk through this mine field. None of us want to throw the baby out with the bath water here. We want to move forward and not backward.

In this whole opt-in/opt-out thing, do you have any sense, Mr. Rotenberg, that the American people just kind of assume that their transactions are private unless told otherwise? Do you have that sense?

Mr. ROTENBERG. I think that is the common sense view, Senator. I think it is as you described it. If a business asks you for your credit card because you are going to buy something by a credit card, you understand and you expect them to take the credit card number for the purchase. If you want to have a gift shipped to someone in your family around the holiday season and they say, what is the address, and you give them the address, you understand that that is to make sure that the package is delivered.

Senator CLELAND. May I just inject here? I call a florist and I give them my American Express card number, but I am dealing with that florist. It is a confidence thing. I do not expect the florist to go down the mall and give my American Express card number to everybody in the mall and then be deluged with a bunch of offers on other things. I just do not expect that. I expect the florist to hold that in confidence, and it is a relationship kind of thing.

Mr. ROTENBERG. I think the problem here and the reason that there is a great deal of consumer concern is that we are basically operating in an environment without rules. Businesses understand that this personal data has value. It can be sold. It can be reused, oftentimes for the benefit of consumers, I should point out. There are certainly some benefits. But consumers are losing control and businesses are not expected today to follow any rules.

And I think that this tension is going to accelerate. I think that this problem is going to increase going forward. Businesses are going to be under increasing pressure to generate revenues online, to make these e-commerce businesses profitable. Consumers are going to be asked for more and more detailed information.

We are about to enter a very interesting period where the collection and use of genetic information will be technologically possible within the next 5 to 10 years. And I think it is important to put the rules in place.

The CHAIRMAN. Senator Cleland, thank you.

Senator Kerry, I know you have been waiting to ask a question. Would you do me a favor? We have two more witnesses in the next panel. As you know, we have been objected to and are not supposed to go past 11:30. Mr. Berman is here in Washington. Mr. Rubin, who is in the next panel, is from Atlanta, and we all know how hard it is to get a flight out of Atlanta to Washington.

[Laughter.]

The CHAIRMAN. So, I would ask for your indulgence. We will assure Mr. Berman that we will invite him back to the next hearing, and we will ask Mr. Rubin, who came all the way from Atlanta, if he could give a brief statement, and then we could ask questions. Would that be agreeable to you, John?

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

Senator KERRY. Sure. I am not going to ask a question. I just wanted to make a couple of points.

The CHAIRMAN. Maybe you could wrap up the hearing.

Senator KERRY. I will be happy to accommodate.

The CHAIRMAN. Thank you.

Mr. Rubin, would you come forward? The witnesses remain. Bring a chair for Mr. Rubin. When the witnesses come from out of town, we like to at least allow them to be heard.

Mr. Berman, I want to apologize to you and promise you that you will be a witness at the next hearing in the first panel.

[Laughter.]

The CHAIRMAN. Mr. Rubin, would you give a brief statement? Then, Senator Kerry, because of the objection to the Committee meeting more than two hours, will wrap up by making some comments. Maybe we could allow a response to your comments by the panel, if that would be all right.

Senator KERRY. If they want to.

The CHAIRMAN. Mr. Rubin.

STATEMENT OF PAUL H. RUBIN, PROFESSOR OF ECONOMICS AND LAW, EMORY UNIVERSITY

Mr. RUBIN. Thank you for the opportunity to testify and thank you for you considering my schedule trying to get back and forth from Atlanta.

I am from Emory University, but I am here as a representative of the Progress and Freedom Foundation which is engaged in a big study, a major study, of how these Internet markets work.

I think the conclusion we are reaching is that at this point, in spite of all we have heard, there really is not very good evidence that there is a market failure. We have markets here. It is a new market, as we have all said.

In the FTC study, the most remarkable thing that I found was the number of Internet sites and websites that have increased their privacy notification. The various programs, BBB*OnLine,* TRUSTe, are all relatively new. I think things are progressing quite quickly and it is our belief and my belief that we should really be very careful in looking at the problem and seeing the extent to which markets can go some way toward solving the problem.

We have heard lots of testimony this morning that people are changing, the policies are changing. The websites are posting privacy policies, and of course, if you go to a website that does not have a privacy policy, consumers are starting to learn what that means. We have heard people say that consumers do not understand. We have also heard people say that consumers are very concerned about privacy, and to the extent they are concerned about privacy, it pays for private sellers and websites to begin posting privacy policies.

We have heard discussions of new technologies that may be coming online. We have heard mention of P3P, a protocol that will perhaps greatly simplify consumer privacy preferences as it goes forward.

So, I think the fear that we have is that it may be premature that we really have not had time to observe how the market will work.

There is discussion of a National Academy of Sciences study. Progress and Freedom Foundation is also engaged in a study. I think it is premature to legislate before we have this information, before we have really had these objective studies of the problem, as opposed to the evidence so far, which seems to us to be mainly

anecdotal. It is our belief that we really should get more information.

Now, there have been discussions of the FTC. I used to work at the FTC. I never found it to be a terribly flexible agency. Once a rulemaking was in place, for example, it became very difficult to change that rule. I was impressed, as I was reading the P3P protocol that it was labeled P3P, Release 1.0, which carries the connotation that there will be 2.0 and so forth and so on. I have yet to see a law or a rulemaking that comes with a release number, and the fear is that if we pass something, it will perhaps freeze technology or change technology, and that given the rapidity of change in this industry, there is a real danger of passing something too soon.

So, you discussed going forward with the analysis and I think that would be the recommendation, that we really do try to get more information before we go ahead and do it, and particular information about the way in which markets can and are beginning to solve these problems as consumers express their concerns.

[The prepared statement of Mr. Rubin follows:]

PREPARED STATEMENT OF PAUL H. RUBIN, PROFESSOR OF ECONOMICS AND LAW, EMORY UNIVERSITY, ATLANTA, GA

Mr. Chairman and Members of the Committee:

I want to thank you for inviting me to testify on this important matter this morning. I am appearing before you today in my capacity as a Senior Fellow at The Progress & Freedom Foundation. While the views expressed are my own and do not necessarily represent those of the Foundation, its board, officers or staff, you should know that I am the lead investigator in a major study of the costs and benefits of regulating privacy now underway at the Foundation.[1] The study is not complete, but we have found enough to raise some questions relevant for this morning's hearing. The issue as we see it is whether market forces will be able do handle issues of privacy, or whether government regulation will improve the functioning of the market.

I first discuss the market for privacy. I then address the issue of whether we can expect government regulation to improve the situation. I stress that these are preliminary results. To summarize, those results suggest that legislation at this time would be premature. While consumers clearly are concerned about on-line privacy, the risk of unforeseen consequences from proposals for government intervention is very high, and those consequences could be to impede the development of the new medium to the detriment of consumers and the economy alike.

The Market

A transaction between a consumer and the owner or operator of a website is a 2-party transaction. Therefore, in principle the parties are free to negotiate the terms of that transaction. One of the terms that can be negotiated in this way is the use of whatever information the consumer gives to the website. There is no obvious reason why the consumer cannot make the transaction conditional on the use of the information, or why the marketplace will not offer the kinds of choices consumers desire

For example, consider two competing websites both selling a product—say, CDs. Assume that site CDP has a strong privacy policy, and makes a strong and binding commitment to maintain privacy, and that site CDNP has no privacy policy, and makes use of the information provided by consumers for other purposes. Presumably, CDNP will sell CDs cheaper than will CDP, because it earns revenue from the sale of information received from consumers and so can charge a lower price for CDs and still make a profit. But consumers might still prefer to deal with CDP because the information is worth more to them than to the website. This means that consumers would be willing to pay a higher price for CDs and retain their rights in the information, rather than paying a lower price and losing their rights. If this is the preference of consumers, then at equilibrium CDP will get more business than

[1] I am also a professor of economics and law at Emory University.

CDNP, and ultimately CDP's business model will prevail in the marketplace. Alternatively, if the information were worth more to the website than to the consumer, then consumers will prefer to deal with CDNP because of the lower price, and CDNP's business model will prevail.

A more likely result is that some consumers will prefer more privacy and deal with CDP, and others will prefer lower prices and deal with CDNP. Merchants often offer different terms of sale and prices (Wal-Mart and Macy's) and there is no reason to expect more uniformity of terms in the market for information than in the markets for other sorts of contractual provisions.

There are of course various assumptions in the above story. One of the most important is that consumers know and understand the privacy policies of the two websites. If they do not, then the market will not function as described. For example, consumers who value the information more than does the website might shop at CDNP because of its lower price. Such consumers would be harmed, because they would be transferring information at a price below its value to them.

Government mandated notice requirements, such as those proposed in the Federal Trade Commission's recent *Report to Congress,*[2] and in the bills under consideration today, assume that consumers do not understand the privacy policies of alternative websites and that government action is needed to make such information available. As a general matter, however, there are strong incentives for the marketplace to provide such information to consumers. In the example above, CDP will have an incentive to tell consumers that they will guarantee privacy. They may do so by explicitly comparing themselves with CDNP, but even if they do not, consumers will be able to learn that CDP provides privacy. When they visit site CDNP they will not see any mention of privacy, and will rationally assume that the site does not provide this benefit.[3] This competition between websites over privacy policies is potentially important, although many analysts have ignored such competition.

It is sometimes argued that it may be too expensive for a given site to provide useful information. This argument suggests that, if consumers do not understand privacy issues, it would be costly for a particular site to explain these issues, and other sites could free ride on the efforts of one site to explain. Moreover, it would take a substantial amount of time for a consumer to read and absorb the privacy information provided by a site, and it may well be that the cost of obtaining this information is greater than the value. This could lead consumers either to avoid the Web altogether, or to "mistakenly" purchase from sites like CDNP and suffer a net loss.

The economics of transactions costs and various approaches to minimizing such costs are one of the areas we are examining in our study. As a general matter, however, issues like those above would be of greatest concern if consumers were broadly ignorant of privacy issues. While this may have been the case in the early days of the Internet, it no longer is. Indeed, as summarized in Table 1, privacy has become a major concern of users of the Internet, with most polls showing that majorities of users are concerned with privacy. Some take this level of concern as a justification for government regulation. But, in fact, it is the opposite: If enough consumers are concerned with privacy, the marketplace will be more likely to respond to their concerns.

The FTC's report seems to suggest the market is responding as one might expect. In its 1998 report, the FTC indicated that only 14 percent of websites disclosed their information practices. In the 2000 report, 88 percent of a random sample of sites and 100 percent of the Most Popular sites had some privacy disclosure.[4] Thus, in a very short time, the percentage of sites voluntarily providing information about privacy policies has increased from a small fraction of websites to all of the most popular, and most of the others.

There is substantial additional evidence that consumers and firms are already making well informed decisions about privacy matters. For example:

- In one survey, the most common reasons for not registering at a website are that the terms and conditions of the use of information are not clearly specified, or that revealing the requested information is not worth registering and being able to access the site.[5]

---

[2] "Privacy Online: Fair Information Practices in the Electronic Marketplace: a Report to Congress," Federal Trade Commission, May, 2000.

[3] Sanford Grossman (1981), "The Informational Role of Warranties and Private Disclosure About Product Quality," *Journal of Law and Economics* v. 24, December: pp. 461–483.

[4] Data from "Privacy Online," pp. i, ii.

[5] GVU's 7th WWW User Survey, *http://www.gvu.gatech.edu/gvu/user*__surveys/survey-1997-04/

- Many companies, including IBM and Walt Disney, do not advertise on websites that do not have privacy policies.[6]
- Companies are increasingly hiring "privacy officers" and giving them substantial power and discretion in setting company policies. In fact, Alan Westin, a well known privacy advocate and expert, offers a training course for this position.[7]

There are other mechanisms available to minimize the costs of dealing with privacy issues. One such mechanism is the use of voluntary standards, as defined and explained by a consortium of web operators. Large firms—Microsoft, AOL, Intel—make enough money and are large enough forces so that it pays for them to internalize production of various standards.[8]

As a general matter, there are voluntary standards organizations that deal with a wide variety of issues. ANSI (the American National Standards Institute), for example, is an umbrella organization for over 1000 members.[9] The American Society for Testing and Materials (ASTM) is another voluntary standards organization.[10] Defining a standard of Internet privacy is in principle no different than defining other standards. A standard can establish a set of defaults and can serve to inform consumers of the options and issues involved in privacy. In other words, a standard can serve to define the property rights so that transactions can occur and the right can be properly assigned through market processes.

For example, the World Wide Web Consortium (W3C) is a consortium of 434 members, including the largest players in the Internet, such as Microsoft, America Online and Cisco.[11] This consortium is in the process of drafting a major private privacy protocol, the Privacy Preferences Project, P3P.[12] While P3P is not yet operational, there are numerous private seal programs already in place, including TRUSTe and BBB*Online.*[13] The Direct Marketing Association also has various voluntary standards in place, including a method consumers can use to have their names removed from email lists, and members of the Association must meet certain requirements regarding privacy on the web.[14] Thus, organizations such as the BBB, TRUSTe or W3C can define property rights and provide information about them and about alternatives.

Government

While the market appears to be responding well to consumer demands for more control over their personal information, some still argue that there is a role for government regulation. Government, perhaps, might move more quickly than the marketplace, or provide a greater degree of uniformity, or better reflect the "value" of personal privacy in ways the market would not. These are all issues we are examining in our work.

One cautionary note about government regulation, however: It is extremely inflexible. Once a major law is passed, it tends to establish a regulatory framework that lasts for a long time. For example, the Federal Communications Commission began allocating licenses using inefficient methods such as administrative hearings when it was founded, and it took many years until the agency began using an auction, although economists and others advocated sale of licenses at least as early as 1951.[15] This danger has been referred to as "freezing technology"—that is, destroying incentives for innovation, since innovations will not satisfy the government requirements.

There are several reasons for the relative inflexibility of government regulation. First, simply getting Congress to pass a major piece of legislation is difficult. Congress has limited ability to pass such legislation, and does not tend to re-examine an issue frequently. Second, there is the regulatory time interval required to imple-

---

[6] "It's Time for Rules in Wonderland," *Business Week,* March 20, 2000.

[7] D. Ian Hopper, "Companies Adding Privacy Officers," AP, July 11, 2000.

[8] Peter Swire (1997), "Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information," in Privacy and Self-Regulation in the Information Age, U. S. Department of Commerce, Washington, DC. *http://www.ntia.doc.gov/reports/privacy/selfreg1.htm.*

[9] See *http://www.ansi.org/*

[10] *http://www.astm.org/index.html*

[11] For the W3C homepage, see *http://www.w3.org.* For the list of members, see *http://www.w3.org/Consortium/Member/List.*

[12] *http://www.w3.org/P3P/.*

[13] *http://www.bbbonline.org/*

[14] *http://www.the-dma.org.*

[15] Thomas W. Hazlett (1998), "Assigning Property Rights to Radio Spectrum Users: Why Did FCC License Auctions Take 67 Years?" 41 *Journal of Law and Economics,* Number 2, Part 2, October.

ment the law. Third, and perhaps most important, the passage of a law and subsequent promulgation of regulations create interest groups with an interest in maintaining that law. For example, attorneys specialize in dealing with the law as it exists, and become a vocal group in opposing changes. Firms come into being specializing in institutions that comply with the law, and these firms also lobby to retain the current law. Regulatory authorities in charge of enforcing particular laws lobby for the retention of these laws, an important component of the FCC delay mentioned above. The institutions created by the law themselves become barriers to entry, as potential entrants must adapt to these institutions. On the other hand, those who could benefit from changes in the law have difficulty in making their voices heard.

It is a cliché to say that the Internet is dynamic. But it is true. Any regulation at this time would freeze some aspects of the Internet in their current state. Even if the regulators were able to regulate perfectly for today's environment, any regulations would quickly become obsolete as the Internet changes. The P3P release is P3P 1.0, indicating that, like software in general, the drafters expect that the privacy policies embedded in the document will change over time. Indeed, at several places in the document itself there are indications of directions for change in future versions. While such expectations drive software and the development of the web, laws passed by government do not come with release numbers—because there is no expectation that they will be changed quickly (or ever). While change is the normal state of affairs for the Internet and for software and other elements that interact with the Internet, it is not the way in which government operates.

It is important to remember that technological and marketplace developments in the privacy and security arena are happening almost daily. One new program has increased the ability of websites to identify consumers logging on to the website.[16] The technology allows the Checkfree website, in conjunction with Equifax, the credit reporting agency, to identify customers quickly and accurately, thus increasing security. Another relatively new service, PayPal from X.com, enables consumers to pay bills on the Internet anonymously.[17] A virtually infinite array of such technologies is in development.[18] Any regulation passed by Congress could interfere in unknown and unpredictable ways with such technological progress.

It is also important to keep in mind that government regulation is of necessity of the "one size fits all" variety. But with respect to Internet privacy, different consumers have different preferences. These are documented carefully in a survey on Internet privacy by AT&T.[19] For example, those most concerned about Internet privacy—those the AT&T report calls "privacy fundamentalists"—often already protect themselves using a variety of techniques, such as anonymous remailers.[20] On the other hand, at least one company, AllAdvantage.com, pays consumers for the right to monitor their browsing, and some consumers are apparently willing to join this program.[21] Thus, consumers clearly have different preferences regarding Internet privacy.

Furthermore, it seems likely that consumers have different privacy preferences regarding different types of information. In one survey, for example, consumers were less willing to provide social security and credit card numbers than other types of information. Similarly, 78 percent would accept cookies to provide a customized service; 60 percent would accept a cookie for customized advertising; and 44 percent would accept cookies that conveyed information to many web sites.[22]

Incorporating such nuances in a government regulation would be difficult, and any privacy notice that resulted would have to be exceedingly complex, perhaps to the point that most people would be unwilling to read such a detailed notice. The very value of information to advertisers is evidence that at least some consumers benefit from the information being available to sellers. Advertisers would not value information if they could not use it to sell products. But if consumers buy products based on being contacted by merchants, then consumers must benefit, else they would not buy the products. The modern theory of advertising indicates that most or all advertising provides valuable information, and if advertising leads to sales than at least some subset of consumers is benefiting from the advertising.

---

[16] D. Ian Hopper, "New Way Found to ID Web Customers," AP, July 17, 2000.

[17] Michelle Slatalla, "Easy Payments Put Hole in the Pocketbook," *New York Times,* June 29, 2000.

[18] Peter Wayner, "New Tools to Protect Online Privacy," *New York Times,* November 11, 1999.

[19] Lorrie Faith Cranor, Joesph Reagle, and Mark S. Ackerman, (1999), "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy," AT&T Labs-Research Technical Report TR 99.4.3, *http://www.research.att.com/library/trs/TRs/99/99.4/*

[20] Lorrie Faith Cranor, "Agents of Choice: Tools That Facilitate Notice and Choice about Web Site Data Practices", available online.

[21] *http://www.alladvantage.com/home.asp?refid=*

[22] Cranor et al., 1999.

Summary

In summary, there are reasons for expecting the market to manage privacy issues efficiently. There are also substantial dangers from inappropriate government intervention. If we rely on the market and the decision turns out to be incorrect, we can always pass legislation later. But if we regulate, it is much more difficult to change our position. At The Progress & Freedom Foundation, we are working to produce a report to help Congress and other policymakers evaluate the relative merits of market-based approaches, on the one hand, and government regulation on the other. The results of that research, at this stage, suggest that premature legislation and/or regulation is likely to do more harm than good.

Mr. Chairman and Members of the Committee, that completes my prepared statement. I would of course be pleased to respond to any questions you may have.

Table 1: Is Privacy Important to Internet Users?

AARP National Survey, 2000	Percentage of respondents having made internet purchases who say they are concerned about privacy	74% (40% very concerned, 34% somewhat concerned, Page 35)
AT&T Labs-Research: Beyond Concern: Understanding Net Users' Attitudes about Online Privacy, 1999	Percentage of respondents who say they are very or somewhat concerned about threats to personal privacy while online	87% (Page 6)
Louis Harris and Associates, Inc.: E-Commerce and Privacy: What Net Users Want, press release, 2000	Percentage of net users who are concerned about threats to their personal privacy while online	81% (Page 3)
IBM Multi-National Consumer Privacy Survey, 1999	Percentage of U.S. respondents who somewhat or strongly agree with the statement ''Consumers have lost all control over how personal information is collected and used by companies.''	80% (Page 76)
IBM Multi-National Consumer Privacy Survey, 1999	Percentage of U.S. respondents who somewhat or strongly agree with the statement ''It's impossible to protect consumer privacy in the computer age.''	71% (Page 76)
IBM Multi-National Consumer Privacy Survey, 1999	Percentage of U.S. respondents who somewhat or strongly agree with the statement ''Most businesses handle the personal information they collect about customers in a proper and confidential way.''	64% (Page 76)
IBM Multi-National Consumer Privacy Survey, 1999	Percentage of U.S. respondents who somewhat or strongly agree with the statement ''Existing laws and organizational practices in the United States provide a reasonable level of consumer privacy protection today.''	59% (Page 76)
Cyberdialogue: Capturing Visitor Feedback, 1997	Percentage of respondents who feel that online services which ask for personal information are directly invading their privacy	52% (Page 12)
Cyberdialogue: Privacy vs. Personalization, 1999	Percentage of respondents who feel that online services which ask for personal information are directly invading their privacy	37% (Page 1)
AARP National Survey, 2000	Percentage of respondents who cited concerns about privacy as a reason for not having made any internet purchases (multiple answers were permitted; ''not interested'' was top answer)	24% (Page 34)
AARP National Survey, 2000	Percentage of respondents who cited security/privacy concerns as a reason for not having internet access (multiple answers were permitted; ''no interest or need'' was top answer)	6% (Page 24)

References for Table 1:

American Association of Retired Persons, "AARP National Survey on Consumer Preparedness and E-Commerce: A Survey of Computer Users Age 45 and Older." March, 2000.

AT&T Labs, "Beyond Concern: Understanding Net Users' Attitudes about Online Privacy". Available online at *http://www.research.att.com/library/trs/TRs/99/99.4/* 99.4.3/report.htm. April, 1999.

Cyber Dialogue, "Capturing Visitor Feedback." Available at *http://www.cyberdialogue.com.* March, 1997.

Cyber Dialogue, "Privacy vs. Personalization: A Delicate Balance." Available at *http://www.cyberdialogue.com.* 1999.

Cyber Dialogue, "Privacy vs. Personalization Part III." Available at *http://www.cyberdialogue.com.* 2000.

Harris Black International, "The Use and Abuse of Personal Consumer Information." Available online at *http://www.harrisblackintl.com/harris__*poll/index.asp?PID=8. January, 2000.

Georgetown University, "Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission". Available online at *http://www.msb.edu/faculty/*culnanm/gippshome.html. June, 1999.

IBM, "Multi-National Consumer Privacy Survey." October, 1999.

Louis Harris and Associates, Inc. and Dr. Alan F Westin, "E-Commerce and Privacy: What Net Users Want", press release. Available online at *http://www.pandab.org/E-Commerce%20Exec.%20Summary.html.* July, 2000.

National Consumers League, "Consumers and the 21st Century". Available online at *http://www.natlconsumersleague.org/FNLSUM1.PDF,* 1999.

NFO Interactive, "Online Retail Monitor: Branding, Segmentation, & Web Sites". 1999.

Privacy and American Business, "Personalized Marketing and Privacy on the Net: What Consumers Want." November, 1999.

Privacy and American Business, "'Freebies' and Privacy: What Net Users Think." Available at *www.privacyexchange.org/iss/surveys/sr990714.html.* July, 2000.

The CHAIRMAN. At what timeframe do you think we would have this?

Mr. RUBIN. Well, we are hoping to have at least a preliminary study by January. I do not know what the time table, for example, for the National Academy of Sciences is. But I think at this point we do not have the information to pass legislation.

The CHAIRMAN. Senator Kerry.

Senator KERRY. Thank you, Mr. Chairman.

The CHAIRMAN. And I thank you, Senator Kerry.

Senator KERRY. I am delighted. I just wanted to make a few comments, and I think obviously we have got to try to respect the time here.

I agree with Mr. Rubin, and I think you know, Mr. Chairman, you and I have been working together. I think I was one of the early advocates in this Committee, if not the first, to suggest that there is a lot of unknown here as Congress began to sort of respond to the hue and cry about privacy. There was some early legislation submitted on this Committee, and I have great respect for the authors of that legislation. It represents sort of one pole in the debate. Senator McCain and I have written a piece of legislation that represents a different one, and I am confident there will be even other views as we move forward here. But I would like to make a couple of points about it.

First, there is no question among any of us at all that consumers expect a certain degree of privacy on the Internet. We have seen that in survey upon survey, and we see it also I think in behavior. And those concerns, I am confident, will be addressed.

But I think the expectation of privacy when they surf the Internet is different from what they demand particularly for medical records and for financial information. I think those are two items that particularly are distinguished, and we have separate pieces of legislation addressing those.

A survey done in Massachusetts supports this conclusion. Mass Insight Corporation found in a survey performed in May of this year that where they can clearly perceive specific benefits from data collection and information sharing on the Internet, most people see the rewards outweighing any concerns about privacy.

Now, Massachusetts does have more Internet users than the national average, and that may make them more comfortable with privacy practices on the Internet. But I think it also indicates, as more and more people use the Internet, that they too become more comfortable sharing certain kinds of information in exchange for the benefits that they receive. A very interesting statistic from that survey is that 70 percent of Massachusetts adults have access to the Internet, and of those, 69 percent say the benefits of electronic information sharing outweigh the risks.

We also have a responsibility to establish a baseline for privacy standards, but I think what Senator McCain and I have done actually empowers consumers to make that kind of discerning decision that best suits their needs.

I have mentioned that we obviously will deal with the medical records and financial issues separately.

But I want to point out that another important finding in the Massachusetts survey is that when asked to choose between privacy risks and specific benefits and real-life tradeoffs, more people say that we should encourage rather than discourage technology-based information sharing.

In the category of shopping over the Internet, which is the area that we are really targeting, 49 percent of the people surveyed said we should encourage information sharing compared to the 38 percent who said we should discourage it.

Finally, Mr. Chairman, I would just point out that given our interest in campaign finance reform, 69 percent of the people surveyed believe we should encourage more technology-based information sharing in the laws regarding disclosure of political contributions.

Now, I would like to point out also part of the early debate, and Senator Cleland was just going through this a little bit in his questions about offline/online distinctions. Again, early on I have tried to point out that if privacy is the concern in Americans' minds, we have to recognize that while there are different sectors of the marketplace, the marketplace is essentially the marketplace and privacy no matter where it occurs. If the right to privacy accrues in one place, certainly it accrues in another, and we have to look very carefully at how we do anything—and a number of you have mentioned this in your testimony this morning—really affects the marketplace as a whole and the capacity to pick winners and losers inadvertently sort of as an unintended consequence of trying to protect rights in one place without being certain we fully understand the implication of those rights in other places.

Specifically, the list of areas which we are learning more and more about where Americans are affected in the context of privacy within the marketplace is really quite extraordinary. One can easily solicit campaign contributions from donors who have given to almost any list, and that is bought and sold in the marketplace every day.

Age of any individual. Date of birth is included in almost all data bases, and it can be used to determine whether the magazine you subscribe to includes ads targeted to seniors or to teenagers or so forth. All of that marketable and available.

The cost of your own house. Real estate transactions available to the public at the county courthouse. Companies copy this information, sell it to third parties. All kinds of targeting can take place through that.

Travel habits. Airline frequent flyer programs keep track of numerous habits, including frequency of travel, destinations, hotels, car rentals, all of it available within the marketplace.

Purchasing habits. Supermarket shopping carts could be used, anywhere you purchase whatsoever, to create a data base on individuals as to whether they purchase personal items that might be embarrassing, home pregnancy tests, baby food, anything, all of which can result in targeting.

Health information. When patients answer questionnaires and disclose that they have cancer, diabetes, or arthritis, that information can be sold to pharmaceutical companies and is and winds up in various kinds of marketing and targeting.

Phone habits. A telephone company can tell how often and where you travel by keeping track of how often and from where you use your telephone calling card. They can sell that information to hotel companies, to rental car companies, and airlines.

Creditworthiness likewise opens people up to all kinds of questions about bank marketing, higher interest rates, and so forth.

Sexual preferences, subscriptions to magazines, or contributions to an AIDS related charity would give marketers an indication of sexual preference and marketing capacity.

Birth of a newborn, women who subscribe to parenting magazines, shop at maternity stores, sign up for childbirth classes, any number of things.

Browsing habits. Department stores in malls use surveillance to study the best layouts of stores and displays. Other information can clearly be gleaned from that.

So, we probably all have great differences of opinions about which of these practices we believe is egregious and violates our propriety, but it does not stop us from going to the malls, making purchases or continuing to use credit cards and engage in the marketplace. Clearly there are tiers and distinctions of the violation, in a sense, of one's expected zone of privacy, and Americans understand that.

I think, Mr. Chairman, we need to understand that very, very clearly as we approach any kind of legislative effort here with the understanding that the consequences of that clearly can have major impacts on the marketplace itself, as well as the growth of the Internet which depends on advertising to be free. One of the most important things we need to take note of is that Americans have an expectation that it will be free. And if we are concerned about divide and other issues, that free access is going to be increasingly important to us in terms of equal access in America and equal opportunity to use the power of the Internet.

So, I welcome these hearings. I think they have already shed a lot of light. They have been helpful in educating the Committee.

We are not going to be able to legislate this year obviously, but as we come into next year, I hope our study and I hope other information will be available to us.

I do not know if any of the panelists want to comment quickly on anything I have said, but I will not ask a specific question.

The CHAIRMAN. I want to thank Senator Kerry for one of the more in-depth analyses of this issue. I hope that every member of the Committee gets a chance to read that statement because I think it puts a perspective on this issue that is vitally important. Sometimes we have a tendency to more narrowly focus.

I would like to ask the witnesses, beginning with you, Mr. Rubin, if you any response to Senator Kerry's statement. We will make it brief because we are about the incur the wrath of the Senate rules. Mr. Rubin.

Mr. RUBIN. I think it was a nice statement, particularly pointing out that there may be further implications and things that you do may affect the marketplace in ways that have not been thought about. I think that is a very important point to keep in mind going forward.

The CHAIRMAN. Mr. Rotenberg. By the way, you are free to make any additional comments.

Mr. ROTENBERG. I would just say, Mr. Chairman, I certainly agree, Senator, it is a big and complex issue and it touches many different aspects of our private lives. But we have struggled with this issue in the United States for more than a century now, and the wonderful thing about our legal system is that it has adapted, and we have over time enlarged the legal right of privacy as new technologies have evolved. This is a complex one, but I do not think the enormity of the task should be a reason not to proceed.

People value this right. They really do. We each value it in a different way, but we do value it as a country. I think we look to the Congress to ensure that it will be protected in law.

The CHAIRMAN. Mr. Garfinkel.

Mr. GARFINKEL. Senator Kerry, I am honored to be one of your constituents.

But I would like to say something that industry has been saying a lot, which is that unless there is this personally targeted information, the Internet will not remain free. There is no basis for that statement. There is no basis for saying that you can get higher ad rates if you know who is at the end of the Internet connection than you could by selling car ads on a car site and electronics ads on an electronic site. Personally targeted ads is something that the technology makes available, but it is not something that necessarily is good. We know that there are lots of things that the technology makes available but that do not make economic sense, like video telephones.

So, I would encourage you to say that there are a lot of very important privacy issues here, and you touched upon them all. But I am not sure we need to sell our privacy to get free Internet service.

The CHAIRMAN. Do you think it is a violation of privacy, one of the examples that Senator Kerry just mentioned, that because one of us donates to one individual in a political party, that that information should be sold throughout the Nation to virtually every

cause that there is? Do you believe that is a violation of our privacy?

Mr. GARFINKEL. We have made a decision as a people——

The CHAIRMAN. Well, I would like to know your opinion as to whether it is a violation of privacy or not.

Mr. GARFINKEL. I believe that the violation of privacy that comes from the disclosure of political contributions is an acceptable price because——

The CHAIRMAN. I am talking about selling that information, not having it disclosed. We all know about disclosure laws, Mr. Garfinkel.

Mr. GARFINKEL. I believe that any information that comes from the government that is sold now should be distributed for free to the people of this country.

The CHAIRMAN. I am sorry that you will not answer my question.

Mr. Vradenburg.

I think it is a legitimate question Mr. Kerry asked, and I am sorry you will not answer it.

Go ahead, Mr. Vradenburg.

Mr. VRADENBURG. Senator Kerry, I thought you brought a good perspective to this, and I think the only closing comment I would make is that we probably in industry share virtually every value you articulated. And the great challenge that we have to work through together during the course of the next congressional session is achieving the balance between a marketplace that provides free flow of information, which is innovative and which provides a continuing refreshment of the products and services and how we respond to consumers and, at the same time, honor and respect the privacy values that Senator Cleland has mentioned because I do think that there is a balance here.

I think that we try and respond to it in industry in terms of the conservatism with which, for example, AOL might take with the handling of the personal information of its members, but in fact, this is a conversation that we ought to have to make sure that we have struck the right balance, whether it be industry on the one side or government on the other.

Again, I do not think you were here, Senator Kerry, but I would challenge the Committee, as it thinks through its bills, to apply the bills to the government's handling of personal information, not because I say that as a challenge, but to say it as a technique by which we ought to discover the hardness of some of these questions and the balances that you seek to achieve.

Senator KERRY. I agree completely with that.

Mr. VRADENBURG. As you look at the Freedom of Information Act and the wider dissemination of government records, we will begin to question that when it becomes available to your neighbor as opposed to the private investigator or the lawyer that you can hire. In fact, the wider dissemination of information through electronic records is going to be a challenge to our Freedom of Information Act and the way we look at government records and the way we look at disclosure. I do not think that the government has got it right yet. I am not sure that business has got it uniformly right yet. But it is a conversation that I think is vitally important and I think we both have to go through that conversation honestly to

try to arrive at the right balance for both government and for industry.

The CHAIRMAN. Mr. Cooper.

Mr. COOPER. I think this Committee deserves a lot of credit for getting beyond the zero sum game that I think this issue has been held hostage to up till now. I think what we are finding is that a significant, hopefully a critical mass of companies are willing to say we need to work with you, we need to find ways of making this work, though not where we then say that all the answers have been revealed, because I do not think that they have.

We think that a lot of very useful information will be in the aggregate whether it is in medical or whatever. We do not want to lose that. We do not want to lose the advantages that technology is giving us for taking the aggregate use of this information to benefit the country as a whole.

At the same time, in working through these issues we will have to engage business, consumers, and policymakers to find the right answers. Hewlett-Packard thinks that McCain-Kerry has it about right. We think the National Academy of Sciences is the place to resolve a lot of these issues or at least give Congress the opportunity to have a debate based upon a clear set of facts that I do not think is going to come out of just a polarized debate by the loudest voices.

Senator KERRY. Well, Mr. Chairman, thank you.

I would just point out that what the chairman and I have introduced is a pretty strong requirement of notice and choice. In point of fact, one of the reasons I ran through that list of examples is, if you measure all of those, we are in fact providing greater privacy opportunity through what we have offered than anybody has in any of those other sectors I just talked about. I ask people to take note of that. You will have actually greater privacy, just through the notice requirements and the choice requirements, than you have in any of those other sectors of the economy.

You have to also measure the harm done. I go home and I have got 50 magazines waiting for me from whatever it is, targeted from whatever I have purchased previously. You could stop them all, and most of them wind up very quickly going straight—it is a shame what happens to the trees in the process, but that is what happens. But what is the harm done measured against the other choices we have? That is what we have to ask very carefully here, is what is the harm done that somebody got an advertisement. As long as personal information, medical, financial, genetic is obviously an enormous concern, these kinds of things. I think we ought to be able to define that line fairly readily. So, I welcome the debate.

Thank you, Mr. Chairman.

The CHAIRMAN. I would like to apologize again to Mr. Berman. Mr. Berman, we will see you next time. We will be having several more hearings in the month of January because this issue has obviously not been resolved.

I want to thank the witnesses for a spirited dialog. We like to have the point/counterpoint in this Committee, and I think it is very helpful to the members. I want to thank all of you for coming, and we will welcome you back in January.

As much as I would like to assure people that we will pass legislation between now and the next week or two, it simply is not something that is going to happen. But at the same time, I think by the time January or February rolls around, this issue will have increasing importance that the Congress of the United States act in some way on it.

I thank you all. This hearing is adjourned.

[Whereupon, at 11:49 a.m., the Committee was adjourned.]

APPENDIX

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

Reality television has hit an all-time high in the ratings system. This form of entertainment allows viewers to watch the "real" lives of people on TV, but once these viewers cut off their TV and cut on their computer, they become the focus of reality web surfing. Cookies allow on-line companies to gather a great deal of information about consumers and possibly link this information with the person's name, address, social security number, and other personally identifiable information. While the people on television know the cameras are taping their every move, many on-line consumers have no knowledge of how companies monitor their behavior.

Today this Committee revisits the issue of on-line privacy. Estimates are that 137 million Americans can access the Internet and about 300 million people worldwide. America, with almost double the number of net users, is the world leader, and the Federal Trade Commission has recommended that these users need adequate privacy protection when surfing the web.

I would like to remind the Committee of some statements in the FTC report:

92 percent of consumers are concerned and 67 percent are "very concerned" about the misuse of their personal information online;

57 percent of Internet users have decided not to purchase online due to privacy concerns;

79 percent of consumers identified the ability to be removed from a site's mailing list a "very important" criterion in assessing a site's privacy protections, and

79 percent of Internet users believe that a procedure allowing the consumer to see the information companies have stored about them is "absolutely essential" or "very important."

S. 2606, of which I am a co-sponsor, addresses these issues raised by the FTC report. It allows customers to "opt-in" in order for websites to use their personally identifiable information and "opt-out" for use of non-personal information. S. 2606 also requires that consumers have access to the information collected about them by a website and the ability to correct it. It requires that consumers be aware of how collected information will be used and that everything is adequately protected.

Reality programs belong in a world in which people know their actions are being taped. They do not belong in a world in which many users are not aware of the vast amounts of information collected about them. Notice, consent, access, and security are the recommendations of the FTC report, and they are guiding principles of S. 2606. I look forward to the testimony that will be offered here today.

PREPARED STATEMENT OF SCOTT COOPER, HEWLETT-PACKARD CO., MANAGER, TECHNOLOGY POLICY

Legislative questions about opt-in and opt-out

Levels of data collection affected by opt-in/opt-out strategies

The HP privacy policy is one external manifestation of HP company strategy and vision to make the web a friendly place for customers, inspiring trust. resulting in positive benefits and experiences, and e-commerce growth.

When discussing privacy and opt-in/opt-out practices, its important to address the scope and nature in applying these practices. The terms are often used to cover different aspects of data collection and use that differ in the level of privacy protection offered and the value proposition between customers and businesses. These practices (opt-in, opt-out) should be evaluated in relation to sharing personal data with 3rd parties, customer contact strategies using personal data and the collection itself of personal data.

A. Data sharing with 3rd parties

1. Personal data. HP policy is not to sell or rent our customer data. In the case of HP relationships with a few strategic partners, HP policy is that customers must opt-in to share their personal data. We believe this approach respects the trust and boundaries that customers expect when providing their personal data to a company. This policy applies to offline and online data. Customer feedback to HP is very positive regarding these policies.

2. Aggregated (non-personal) data. HP occasionally shares aggregate, non-personal data with a few strategic business partners for the purpose of understanding web navigation and usage. This is how we analyze design effectiveness, usability and usage trends of joint programs or services offered, ultimately measuring successes (or the lack of). These measures drive billing and payment between business partners. HP receives aggregated non-personal data through the HP ad banners placed on web sites. We do not accept personal data from these sources or link the non-personal data to HP-held personal data. HP receives virtually no customer feedback on this level of data sharing.

B. Contact based on data collection

The most common discussion regarding opt-in and opt-out relates to direct contact from a company to a customer. When discussing this, it is important to remember the scope which includes marketing contact, support contact and administrative contact.

Marketing contact refers to programs and information directed at customers or potential customers about new products and services. Besides product information, features and benefits, this includes special offers, promotions and sweepstakes. It may include market research/customer surveys.

Support contact refers to information and solutions directed at customers to solve functional, repair issues or improve performance and usability. This includes software drivers, news and information, diagnostic analysis/tools and product upgrade data.

Administrative contact refers to information directed to customers as part of a process or transaction, such as order confirmation, contract renewals and records management.

In all types of contact the approaches will vary from direct person-to-person telephone (call center), email, or hardcopy mail.

Customers have views and concerns about marketing contact different from support contact. In general, support-related contact is not an issue for customers, given the correct assumption that it is collected only for support purposes, but NOT specific to one transaction or interaction. In cases where support-related personal data is used for marketing contact, then the issues become the same as general marketing contact. Some customers view the use of support contact personal data for marketing purposes as a violation of trust even when they are clearly informed that this is a possibility. The vast majority of customers expect, value and even demand administrative contact.

In evaluating opt-in for HP, we have focused largely on marketing contact and secondarily on support contact. In some contact the boundaries between marketing and support contact are blurred—for example where is the difference between sending information about new products as compared to product upgrade notices that correct functionality or prevent repair problems? In general, we believe the difference is how the contact is initiated. With a support situation there is often a true real need from a customer who explicitly or implicitly (through diagnostics tools that generate support alarms) initiate contact to HP.

Lets focus on the challenges of implementing an opt-in process for marketing contact by using HP Subscription Services (InfoAgent) as an example.

HP Subscription Services, through the HP InfoAgent technology, provide the means for HP customers the opportunity to sign up (subscribe) to a variety of software updates, support and marketing newsletters, focused in the consumer peripheral space. Specifically, software drivers (e.g. for a HP DeskJet printer, etc.), Support tools, resources and tips by product category (e.g. for HP DeskJet or HP LaserJet printers, etc) and product news, solutions and promotions by product category (e.g. for HP ScanJet, etc.).

HP Subscription Services represents *at most 25 percent* of all possible HP-related news and information sources available to/sent to HP customers. When a customer subscribes, it can only happen as a specific action on their part. Although it is not characterized this way on the HP web site, I would call this a functional opt-in.

When the customer subscribes, HP asks the customer if he/she is interested in receiving other related information from HP. In the past, the box next to this question was pre-checked, indicating a "YES". This is an opt-out.

Recently, HP changed the box next to this contact question to leave it blank instead of pre-checked. This is a passive and poorly designed opt-in. This particular approach drives much of the marketing communities' (HP and otherwise) complaint about opt-in. If the contact question is vague and/or if the customer is not REQUIRED to respond, the results can be just as ineffective as the opt-out. Subscription rates typically drop by 50–75 percent, mostly due to "no action" (unanswered) on the part of the customer. Ultimately this becomes then not a technology issue but a business rule issue. In an opt-out business model, the are those unanswered OK to contact? Most would say yes. In an opt-in business model the answer to the "OK to contact" question is most likely no. But an additional process (with business rules) must be created to confirm the customers' intent.

Our next step is to move to an "active opt-in" approach. We believe if implemented properly, that a single, active opt-in works well with regard to engaging trust and creating leading customer experience. The new contact question will be:

"May HP contact you from time to time about products or services of interest to you:

__Yes__No Postal Mail

__Yes__No E-Mail

__Yes__No Telephone

__Do Not Contact me"

As we implement this privacy/contact question today, we are working to resolve across HP several issues around how to interpret and manage customer responses to this question and in context with other places this question may be asked. How to set business rules to apply interpretation of existing customer data not collected in this question format, such as how to handle data where the privacy/contact data is "unknown" (customer inaction, not asked, etc)? How should we interpret a "yes" in postal mail with a "do not contact me" also checked.

A customer could easily have multiple records with HP (product registration, new subscription signup, etc) and continue to add them. How should conflicting answers to the question be interpreted? By date? Are there exceptions in certain HP business segments or functions? How should the data be linked with other data from the customer gathered offline through hardcopy product registration, tradeshows, promotional offer responses, call centers, support centers, and sales representatives? We've just begun to develop a detailed decision matrix to apply business and data processing rules to these questions.

Our objective is to ask this privacy/contact question at each point of data collection. Additionally we must find answers to issues about customer notice and intent. A fundamental question for HP Subscription services is that if a customer comes in who has registered (a product) and subscribed at other times to several newsletters and software drivers, and this time marks "do not contact me". . . . Does that response apply to that specific registration event or does it cancel every other subscription and software driver? We have hundreds of customers today that subscribe through this service to dozens of drivers and several newsletters. Part of the answer is in better customer notice, explaining what will happen when "do not contact me" is marked. But there is significant concern about customer satisfaction. Does a "do not contact me" apply to other subscription and registration areas in HP . . . on the web, through a call center, for support? Or does it apply just to that particular product/service space? How exactly should we apply and interpret customer responses across the whole of HP, for the other 75 percent of possible destinations where a customer may choose to give information, subscribe and so on?

HP has hundreds of customer databases and few are linked in any meaningful way. Our long term vision, to be implemented over the next few years, is that all major customer databases will be linked through a top-level customer identification application. A few major databases link today but many others remain. Linking requires software and business process redesign in many HP organizations. Every database has different data standards and system architectures that must be rationalized.

So while the vision is to "know our customer" as they move through different HP environments: call center, web, support, marketing, sales (and as he/she desires to be known); the ability to have one common view of a given customer and therefore manage privacy/contact choices (among other things) is a mix of human-managed manual processes tied to many individual, decentralized systems/databases.

We're excited about the move to opt-in because we believe it's the right thing to do for HP customers in a marketing context. We believe it is a competitive differentiator. Clearly, the implementation is more complex than the old default opt-out approach. Our fist aim is in the consumer space and for email. Other customer segments and contact approaches are still under discussion. As part of HP consumer business CRM (Customer Relationship Management), we plan to make all type of contact, as per the question, opt-in. Our business customer approach may be somewhat different, whether for solution developers, small-medium businesses or support delivery.

Opt-in (and even opt-out) is much more about business process and behavior than technology, but all must work together and be compatible at all levels. The example above represents one set of business processes and systems out of hundreds. HP wants to do this because we think it's important. We want to do it right so that customer privacy choices are honored, customer relationships and satisfaction is enhanced and customers will be able to receive information that helps their business or personal use of HP equipment be effective. Imagine applying the issues described in the example across hundreds of databases and business processes in HP.

Opt-in is difficult because many companies, like HP, do not have the computer and database architecture or resources to manage the change, at least not rapidly. To accommodate the business, process and technology change requires time and resources. It requires a major business process re-engineering. AND, its tougher in the US than Europe because in the US, the web systems, technology and processes are already in built vs. those in Europe, still in the embryonic stage of web commerce.

Opt-in is difficult because companies fear the loss of valuable customers and their means to communicate with them, inhibiting revenue and eroding brand value.

Opt-in is difficult because opt-out has a tong tradition in the U.S. that many feel is more appropriate to U.S. culture.

Opt-in has limited practicality for support or administrative contact and would negatively impact customer satisfaction and experience across the board. Opt-out makes more sense for support or administrative contact.

Even when opt-in is well in place, HP must still have an opt-out process, so that customers can remove themselves from contact/databases they originally opted-in to.

Opt-in for aggregated non-personal data is impractical and would negatively impact customer experience, customer satisfaction and web-site/e-commerce use. It would be an experience comparable or worse than turning on "notify all cookies" option in your web browser. And what would be the comparable process in regard to offline data? When the implementation of P3P technology becomes pervasive on both web sites and user tools, customers and a web site could engage in a better experience based on personal choice.

HP does believe customers should be given an easy simple way to opt-out of unknown 3 party cookies, like those from advertisers. HP.com policy prevents the placement of advertising on our web sections. HP does obtain aggregate data only reports from advertising banners (and print ads) placed on other web sites (publications) for the purpose of understanding web effectiveness.

C. Collection of data in general

1. Personal data. Customers can go anywhere on hp.com without the requirement to provide personal data. As described above in section B, certain specific types of services do require varying levels of personal information. Opt-in at this level doesn't apply in a practical way because the customer chooses to engage in a specific transaction to start the process. This applies to non-web (offline) services such as call center activity, trade shows and market research.

2. Aggregated data. HP.com collects aggregate, non-personal data used to understand web navigation, ease of use, popular sections, unpopular sections and so on. This data is generally kept within the specific hp.com web section rather than any kind of broad sharing across the whole of hp. Broad sharing across hp would be interesting, but is not a top priority, may not be relevant and would be expensive functionality to build. Applying opt-in, or even opt-out practices at this level would be hugely annoying, cumbersome and a just plain awful customer experience.

Offline aggregate data collection is common, examples are market research, product warranty databases, support diagnostic tools, and sales representative records. There is no practical application of opt-in/opt-out practices here.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ERNEST F. HOLLINGS TO GEORGE VRADENBURG, AMERICA ONLINE, INC.

Question. While more and more companies are adopting Opt-in, you claim Opt-in is impractical and will interfere with the functionality of the Internet and even with the economic viability of certain companies. Please provide the Committee with a memorandum explaining in detail the reasons behind these claims. What are the problems you believe will be realized? What specifically are you or other Internet companies doing now that Opt-in will prevent? What are the economic costs you fear will occur? Please be specific, answer each of these questions, explain your reasoning in detail, and provide examples for each of your answers.

Answer. AOL supports a comprehensive approach to online privacy that will ensure that consumers are provided with meaningful notice and choice about the collection and use of their personal data by online companies. We believe that, in most situations, the specific approach to choice should be determined by the marketplace and the demands of consumers; in some instances, the marketplace will require companies to use an "opt-in" approach, and in other cases an "opt-out" approach may be appropriate. As we work through this issue in the marketplace and in Congress, we should design a system that best serves consumers, rather than by a "one-size-fits-all" regulatory regime. Indeed, we believe that "choice" can be provided in many different ways, and that it is not even possible to force all choice mechanisms into the opt-in or opt-out category, because many choice mechanisms actually have characteristics of both categories.

For example, although subscribers to the AOL service must "opt-in" to the AOL Terms of Service—which includes the AOL privacy policy—as a condition of AOL membership, the choices offered within that privacy policy for the use of personal data for marketing purposes are provided in the form of an "opt-out." Under AOL's current privacy policy, which is considered to be among the most robust in the online industry, new subscribers to the AOL service are provided with a complete explanation of how their personal data can be collected and used. Where members do not want their data to be used or disclosed to third parties for marketing purposes, they are given clear instructions on how to opt-out of such uses, so that they are able to maintain complete control over the use of their personal information. AOL members can change these marketing preferences at any time, and may easily access the AOL privacy at any time by typing in the keyword "privacy." We believe the AOL policy is a prime example of how a meaningful "choice" mechanism can empower consumers to protect their own privacy online, as well as provide consumers with the ability to receive maximum benefit from the online medium.

In examining this question, it is critical to understand exactly what is meant by the term "opt-in." We presume that "opt-in" clearly cannot apply to information collection in cases where such information is collected voluntarily from the consumer and is required for the provision of a particular service. For instance, AOL members may choose to provide us with information about their stock portfolio so that they can receive personalized financial information or stock quotes on the AOL service. However, there is no formal "opt-in" for this feature; rather, consumers can simply choose to provide the information and receive the service, or not to provide this information and not receive the service. Where information is collected as a condition of using a particular product or feature (i.e. registration information), there may not be any "choice" offered with respect to the collection of that information (beyond simply choosing not to use the service), although a company may offer the consumer choice as to whether and how that information is used for purposes other than providing the service itself.

Certain merchants may use information that you provide voluntarily, such as registration information or information about transactions conducted with that merchant, to customize their services to your particular interests or needs. For instance, an online bookseller might use information about the books you've purchased to provide you with recommendations for other books you might be interested in. Presumably, the information was initially collected with your permission (i.e. you chose to provide your name and address so that your book could be delivered directly to you). But must the merchant obtain affirmative consent for each additional use of that data, such as sending you personalized marketing offers or recommending products that might be of particular interest to you? The breadth of an opt-in requirement would determine the extent to which we and other companies would need to alter our business models. Depending on how an opt-in provision is structured, Web sites and online service providers might be required to recontact consumers in order to obtain consent in every instance when their data is used, to retrofit their systems to code data previously collected for the specific uses for which consumers consent,

to categorize and store the consents obtained, and to match any future uses of the data with these categories.

In general, we believe that there may be some practical business, technological, and convenience issues associated with an opt-in model that could make such a model inappropriate as a governmental mandate for all non-sensitive information, and could actually reduce the value of the online medium to consumers. An opt-out approach—not an opt-in—is widely used today in both the online and offline marketplace, and creates the proper balance between protecting privacy and allowing consumers to enjoy the benefits of personalization and customization. Under an opt-out approach, the default always favors "free information flow," a goal that maximizes the inherent strengths of the medium and its potential to improve consumers lives.

By contrast, a mandatory opt-in system sets the default rule to "no information flow," undermining the innovation and growth of the medium while making it more inconvenient for the average consumer to engage in e-commerce transactions. More importantly, a mandatory opt-in requirement would not account for technological developments that will allow consumers to access the Internet or exercise choice in completely new ways. For example, the shift from PC-based Internet access to wireless Web access via a small handheld device is likely to make opt-in prior to information collection extraordinarily difficult, if not impossible, in certain circumstances. As Internet usage expands to a new array of handheld and portable devices, the idea of forcing consumers to click through screens upon screens of marketing preference questions becomes much less feasible and could easily turn many consumers away from these new platforms by making the online registration process extremely complex and difficult to navigate.

In fact, it is entirely possible that a more complicated process could actually confuse or overwhelm users, especially those novice Internet users who comprise a vast segment of AOL's subscriber base. And for smaller companies, whose entire business model may rely on these new platforms or devices, such complexities could drastically reduce their ability to attract consumers and their ability to compete in the online marketplace. In short, there is no way to tell what new products, business models, or devices will emerge over the next few years or how those innovations will change the way that information is exchanged across the Internet. Creating a mandatory opt-in regime today would be as counterproductive as if Congress had tried to set tough auto safety standards in 1880. Until this medium reaches maturity, we won't even know the ways that consumers will want to exchange their information, let alone what restrictions should be placed on that exchange.

By setting the default rule against the collection of information in all situations, an opt-in rule would make it much more difficult for some companies to personalize their services and reach the consumers most likely to be interested in them. Under an opt-in regime, it will be far more difficult for consumers to set up personalized features and receive the many benefits of a tailored Internet experience. As a result, companies will not have the incentives to provide these features and take full advantage of the exciting new technologies available in the online environment to provide consumers with customized services. Additionally, as e-mail marketing is nearly cost free, limiting every advertiser's ability to reach a targeted audience might encourage some companies to send untargeted solicitations to far larger numbers of consumers. Such a requirement would inhibit companies' ability to tailor their marketing efforts to consumer preferences, and could limit the effectiveness of their customer service and customer relations efforts.

Furthermore, more onerous opt-in regulation could make it harder for new entrants to find their "niche" in the Internet marketplace through innovative business models, and would likely reduce the availability of "free" content on the Web that may be supported in large part by advertising and marketing dollars. Because the average consumer is more likely to choose whatever "default" option is offered in an online transaction, an over-regulatory privacy regime could severely limit companies' ability to balance consumer costs with advertising revenue, which could ultimately lead to an increase in consumer prices and a decrease in the diversity and richness of content and services that can be offered to consumers. A more sensible model is to allow companies the flexibility to provide privacy options in the manner that works best for each particular business model, while ensuring that consumers are always fully informed of all their privacy choices.

Ultimately, we believe that true privacy protection rests on the fundamental principles of notice and choice, and that it is not necessary to mandate exactly how such choice must be provided under every business model. Both opt-in and opt-out approaches allow consumers to exercise choice about how their information may and may not be used, but there may be other approaches to choice available as well. In some cases, "opt-in" may be the most appropriate choice mechanism. For example,

we support an opt-in approach for the collection and use of sensitive data such as medical, and financial information, and for children's personal information. Indeed, that is precisely why AOL supported the passage of the Children's Online Privacy Protection Act (COPPA), which addressed the unique concerns raised by the collection and use of children's information, and why we have joined the Hi-Ethics (Health Internet Ethics) Coalition, a group of the most widely used health Internet sites committed to providing the highest standards of privacy protection for health-related information.

But it is the marketplace—businesses and consumers together—that must determine how choice can best be provided in each particular instance. We should not get caught up in a debate over the terminology of "opt-in" and "opt-out," but should focus rather on the ultimate goal of a choice requirement, which is to empower consumers to control their personal data while maximizing the value of the online medium to consumers. As long as consumers have a clear understanding of what information is being collected about them, how it may be used, and how they may limit its use and disclosure, consumers will be able to exercise control over their privacy while still enjoying the full benefits of customization and personalization that the Internet can provide.

We agree that privacy policies that are buried in fine print or written in incomprehensible legalese do not constitute adequate notice and choice, and to the extent that some companies try to defend such practices as consistent with an "opt-out" model, such practices should be strictly prohibited. However, where consumers are properly informed of their options for controlling the use of their personal data, it is unnecessary and potentially harmful to mandate a particular mechanism for providing choice to consumers in all circumstances. Baseline requirements backed up by market-led technological solutions will provide businesses and consumers with enough flexibility to adapt to the changing online marketplace while ensuring that consumer privacy is appropriately safeguarded.

SIMSON L. GARFINKEL LETTER TO HON. JOHN MCCAIN

SIMSON L. GARFINKEL
Cambridge, MA, October 3, 2000

Hon. JOHN MCCAIN,
Chairman,
Committee on Commerce, Science and Transportation,
Washington, DC.

Subject: *Is it a violation of a privacy for lists of campaign contributors to be sold?*

Dear Senator McCain:

Thank you for giving me the opportunity to testify before your Committee earlier today. I would like to apologize to you for my inability to answer your final question, and I would like to attempt to do so now.

You asked me, roughly paraphrased, *Is it a violation of a privacy for lists of campaign contributors to be sold?* This is a deep question. Instead of stumbling through several answers, I simply should have asked your leave to send you an answer in writing.

Please allow me, Mr. McCain, to answer your question now:

Lists of campaign contributors that are sold do violate the privacy of those contributors, if the lists are used in a manner that is inconsistent with the purpose for which the information was collected.

Clearly, the privacy of campaign contributors is violated when their names and that information is made publicly available. Thus, my first answer to your question was that, as a democracy, we have decided that this violation of privacy is preferable to the corrosive power of secret money in politics. You rightfully said that that you knew all about the disclosure laws, and that was not the question that you were asking me.

Once we have made the decision to make campaign contribution information public, the next question is "how will this information be used." My second answer to your question was that this information should not be sold by businesses, but given freely in electronic form by the federal government. You again told me that I was not answering the question that you were asking.

In fact, you were asking if *the selling* of this information *by third parties* further violates the privacy of the campaign contributors.

The answer to that question depends on what is done with the information:

- If the information is used to perform an analysis of the role of money in politics, or to correlate donations with voting patterns, *its does not* further violate the contributors' privacy; this is the reason that the information was originally collected.
- If the information is used to solicit the contributors for donations to museums, or public radio, or to join a country club, then *it does violate* the contributors' privacy; these uses run counter to the original reason that the information was collected.

I believe this analysis shows the importance of passing a national data protection act. Since 1973, the third item of the Code of Fair Information Practices has held that "[t]here must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent." I believe that adopting these principles into US law is the best way to protect the privacy interests of campaign contributors, and indeed of all Americans.

Thank you for your time.

Sincerely,

SIMSON L. GARFINKEL

○