S. HRG. 112–302

THE STATE OF ONLINE CONSUMER PRIVACY

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MARCH 16, 2011

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

U.S. GOVERNMENT PRINTING OFFICE

73–308 PDF WASHINGTON : 2012

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

DANIEL K. INOUYE, Hawaii	KAY BAILEY HUTCHISON, Texas, *Ranking*
JOHN F. KERRY, Massachusetts	OLYMPIA J. SNOWE, Maine
BARBARA BOXER, California	JOHN ENSIGN, Nevada
BILL NELSON, Florida	JIM DEMINT, South Carolina
MARIA CANTWELL, Washington	JOHN THUNE, South Dakota
FRANK R. LAUTENBERG, New Jersey	ROGER F. WICKER, Mississippi
MARK PRYOR, Arkansas	JOHNNY ISAKSON, Georgia
CLAIRE MCCASKILL, Missouri	ROY BLUNT, Missouri
AMY KLOBUCHAR, Minnesota	JOHN BOOZMAN, Arkansas
TOM UDALL, New Mexico	PATRICK J. TOOMEY, Pennsylvania
MARK WARNER, Virginia	MARCO RUBIO, Florida
MARK BEGICH, Alaska	KELLY AYOTTE, New Hampshire

ELLEN L. DONESKI, *Staff Director*
JAMES REID, *Deputy Staff Director*
BRUCE H. ANDREWS, *General Counsel*
ANN BEGEMAN, *Republican Staff Director*
BRIAN M. HENDRICKS, *Republican General Counsel*

CONTENTS

WITNESSES

APPENDIX

THE STATE OF ONLINE CONSUMER PRIVACY

WEDNESDAY, MARCH 16, 2011

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

The Committee met, pursuant to notice, at 10:05 a.m. in room SR–253, Russell Senate Office Building, Hon. Mark Pryor, presiding.

OPENING STATEMENT OF HON. MARK PRYOR, U.S. SENATOR FROM ARKANSAS

Senator PRYOR [presiding]. I will go ahead and call this to order. I want to thank everyone for being here. And we have several witnesses today, and we're going to have a great hearing. And I want to thank everyone.

First, I want to thank the Commerce Committee staff for pulling this hearing together. They really have pulled together an excellent panel, two panels of witnesses.

One thing that Senator Kerry and I were just talking about is the Senate is supposed to vote at 10:30. And based on Senate time, we don't know if that means 10:30, 10:45, 11, whatever. But we're supposed to vote at 10:30. So at some point we're going to have to swap the gavel back and forth and race and vote and come back. But we'll try to keep the hearing going during that time.

Also I know that Senator Kerry has really been a leader on this type of legislation, looking at privacy concerns and has been working on a bill and so we would like to hear from him in just a few moments on that.

What I thought I would do is just give a very brief statement. And I know that Senator Hutchison is on the way and other Senators are on the way. We might dispense with the opening statements for all the Senators, if that's OK, except I thought I might call on Senator Kerry for just a few moments to talk about his legislation and then go onto the panel. And once Senator Hutchison shows up we'll certainly recognize her for her opening statement.

But let me just say that as we start today I want to welcome everyone to the Commerce Committee's hearing on "The State of Online Consumer Privacy." This is a very challenging endeavor. We want to balance the free Internet, you know, the ability to access free content and services for all users, with concerns that are raised about user's privacy and general information collection practices online.

So consumers can conduct research and read online newspapers. They can write e-mails and respond to each other in real time.

Some of them will be worried about how their information is being collected online. Some of them may be willing to surrender some information in exchange for the free content. Others don't have any idea this is going on.

So this is a real challenge. As many good things as we can say about the Internet and how it has really revolutionized information, and it's been so great in so many ways, privacy is an area that we need to keep focused on and try to balance these interests and try to make sure that it's a good place to be and a good place to conduct business.

So our first panel is going to be the Federal Trade Commission and the Department of Commerce.

Our second panel we'll hear from consumer advocates, technology specialists and members of the business community. Their insights and experience are valuable and very much appreciated.

I don't know if everyone knows the polling data, but recently Common Sense Media published some results that said 85 percent of parents say they're more concerned about online privacy than they were 5 years ago.

Seventy-five percent of parents don't think social networking sites do a good job of protecting their children's online privacy.

Ninety-one percent of parents think search engines and social networking sites should not be able to share kid's physical location with other companies until parents give authorization.

So these are just a few of the issues that we'll hear about today. And that as the Senate Commerce Committee and the Senate as a whole and the Congress as a whole moves through this Congress we'll try to work through these issues as best we can.

Again, Senator Hutchison is on the way. And we'll recognize her in a few moments for her opening statement. But until she gets here, Senator Kerry would you like to say a few words?

[The prepared statement of Senator Pryor follows:]

PREPARED STATEMENT OF HON. MARK PRYOR, U.S. SENATOR FROM ARKANSAS

Welcome to the Commerce Committee's hearing on "The State of Online Consumer Privacy."

Today we meet to discuss a challenging endeavor: how to balance a free Internet—the ability to access free content and services for all users—with concerns raised about users' privacy and general information collection practices online.

Consumers can conduct research and read online newspapers. They can write e-mails and respond to each other in real time. Some of them may be worried about how their information is being collected online. Some of them may be willing to surrender some information in exchange for free content.

I look forward to listening to all sides to determine how best to negotiate these perspectives: consumers' privacy concerns with a desire to preserve a robust and thriving Internet experience for all users.

First, we'll hear from the Federal Trade Commission and the Department of Commerce, both of which recently issued reports on consumer privacy and data security. I look forward to examining their findings.

On the second panel, we'll hear from consumer advocates, technology specialists and members of the business community. Their insights and experience are valuable and appreciated.

While industry has dedicated much time to developing basic self-regulatory principles and their efforts are a great starting point, they alone have not eased peoples' concerns about the collection of their personal information from on-line sources. And they will not, alone, prevent abuses from unscrupulous people and organizations.

This is particularly true when it comes to information collected on-line about kids. The supporting statistics are clear. According to Common Sense Media:

- 85 percent of parents say they are more concerned about online privacy than they were 5 years ago;
- 75 percent of parents don't think social networking sites do a good job of protecting children's online privacy;
- 91 percent of parents think search engines and social networking sites should not be able to share kids' physical location with other companies until parents give authorization.

The Federal Trade Commission stressed in its December staff report the importance of improving transparency and consumer choice in the online privacy arena.

Incomprehensible privacy policies and user agreements are out. Better disclosures, better consumer choice and improved safety features are in.

Of course, one of the most elusive challenges we face as a society is how to address the seemingly permanent nature of written comments and information shared on the Internet. In other words, what will new kinds of information "sharing" mean for our children's future—and for their reputations?

Will they be discriminated against with insurers or future employers based on financial, health or personal data they disclosed online when they were teenagers—due to an assumption that the information they shared would be protected—or based on an assumption that they were controlling who could see that information?

Is it clearly explained to them that when they download certain applications or "apps" on their phones or computers, they may be allowing those "apps" to access their personal information—or their specific geographic location at any point in time?

Many people in their teens and twenties now may well opt to share this kind of information—thinking that the privacy trade-offs are well worth it—but they should go into those choices with their eyes open.

Behavioral advertising has transformed the advertising industry. That isn't going to change. In fact, if anything, it will increase as more and more varied types of retailers and services do business online.

However, there's an inherent trade-off between free online content and the sale of personal information that keeps it free. We need to discuss the proper balance and think about whether this trade-off will remain relevant into the future.

Finally, one of the most important questions and one I'm focused on this year is whether we should treat adults and children differently online and have different requirements for the collection and dissemination of their information.

These questions will engage the attention of this Committee during the 112th Congress and for a long time to come. I will be working over the coming months in an effort to address several of these issues.

And nothing is off the table. I welcome the witnesses with us today and I look forward to hearing their testimony.

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

Senator KERRY. Thank you, Mr. Chairman. I would like to just for a sec.

First of all thanks for having this hearing with Senator Rockefeller, I know, wanted to be here, but was unable to be.

And thanks for your leadership and stewardship on these issues.

I must say I was impressed by the energy and amount of—we're talking about the social network. It was a hell of a social network in here before this hearing started.

[Laughter.]

Senator KERRY. A lot of chatter.

As we all know modern technology allows private entities to observe the activities and actions of Americans on a scale that is unimaginable. And there's no general law of commerce to govern that surveillance. And that's why I intend, along with other colleagues, to propose one, a commercial privacy bill of rights.

The purpose of the legislation, I want to emphasize, is not to discourage information sharing but rather to encourage it. But under

a common code of conduct that respects the rights of both the people sharing the information and the legitimate organizations collecting and using it on fair terms and conditions. I think the folks that we've been working with, many of them here today in the industries, know that throughout my tenure on this Committee and now as Chair of the Communications Subcommittee, I have worked hard to protect the innovation and open architecture of the net.

I've worked hard to fight for net neutrality. I've worked hard to prevent taxation and other things. So I believe in this now vital resource for our country in so many ways. But it is important to recognize that increasingly the American people have concerns and express those concerns.

Every single app that any one of us applies to our smartphone or child applies to it is an observational opportunity for a private company. And, amazingly, Internet users collectively sent 107 trillion, that's with a "t," e-mail messages in 2010. Each of those messages is a scanable entity for key words that indicate the interests or patterns of the people who send them.

Facebook started 2010 with 350 million users and ended it with more than 600 million, almost all of which are sharing information broadly whether they realize it or not. And the collection and use of information offline from grocery stores to hotels to airlines has also reached a record high enhancing the data businesses collect online.

So on the positive side, all of this information sharing is generating enormous economic activity. And we like that. We want that. And it encourages all kinds of innovation. And we want that.

But it's also created new opportunities for unethical collectors of information, unwilling to abide by fair information practice principles. And the question can be asked, why should they? Because, you know, there's no law that requires that they do. That has understandably generated a lot of anxiety among Americans about protecting their identity, protecting their personal information, protecting their habits. Protecting the choices that they make which they think they're making in the privacy of their relationship to their keyboard and to their computer or to their phone or whatever instrument they're using, iPad, otherwise.

People have asked so what's the problem that this legislation would seek to solve? Well under current law there are companies today engaged in the practice of harvesting information from websites and elsewhere and using and selling the information without the consent and/or notification or knowledge of the people to whom that information pertains. There are also companies engaged in the practice of using and collecting information that are not building privacy into the design of their services and as a result they lack the appropriate procedures and protections to ensure people's information is secured and being treated fairly. Once a person's information is collected there are no legal restrictions on the further distribution other than those that the collector chooses to impose on themselves.

And lastly, Americans cannot today demand that someone who has collected their information stop using it.

Each of these activities is a problem that Americans are asking us to address. Now I've long thought that baseline privacy protec-

tions in law were sort of a matter of common sense. And over the last 6 months I've reached out to our colleagues on both sides of the aisle, to privacy experts at firms, in academia and to the advocacy community with one simple goal—to figure out why we haven't reached a consensus on a national standard for the treatment of people's information and what we can do to establish one.

And let me just say thank you to many of the people here today. There's been a very positive reaction to this, a concerted effort. The Obama Administration, the Commerce Department, others are working diligently to try to help mold this, shape it. And I've been impressed by the cooperative atmosphere within which everybody is working.

Many of the companies that have rejected legislation in the past have made massive investments in privacy protection for their own customers and at their own firms. A fair share of them now have Chief Privacy Officers, who care deeply about the issue. And they've spent a lot of time thinking about it.

These are serious people. Many of them here. Some of them will testify today. And they believe people's information is deserving of respect and protection not just because it makes good business sense to protect your customers but also because I believe they think it's the right thing to do. And it's in keeping with a sort of value system and ethic that we share here in America about individuality and privacy.

The entire goal of the drafting process that we're using to write a commercial privacy bill of rights is to win pro-privacy, pro-innovation experts over to the side of establishing a common code of conduct so that their customers are not just protected when working with them, but generally protected in the course of commerce. And I think we all benefit by that. I believe that gaining these allies will depend on our willingness to recognize and respect the obvious good that can come from appropriate collection and the use of data while also allowing for experimentation and flexibility in the implementation of privacy practices through the establishment of safe harbor programs.

So we approach this with a real open mind. And I think people will acknowledge a fair amount of reasonableness and flexibility. But we can't let the status quo stand. We can't continue to allow the collectors of people's information to dictate the level of privacy protection that Americans will get when they engage in commerce. And we can't continue to let the firms that provide no protections, provide misleading statements in some cases, about protection, about a protection that they can change at will, at whim, at fancy or allow them just to send the information along to others without regard to where it goes or under what conditions that it goes there.

So my—Mr. Chairman, I hope we're going to establish clear and flexible rules for behavior in our legislation. And if not, I think everybody understands that enforcement agencies are going to step up and react against unfair and/or deceptive practices with cases that will be built sort of individually as you go along with less clear direction than we could provide if we do this in a sensible, legislative way. If we don't act, the world's largest markets will continue to impose on our innovators their own rules for private e-protec-

tion. And I believe those rules could well wind up being less flexible and less innovative than what I will be proposing.

So I look forward to working with the witnesses here today. And I thank you very much, Mr. Chairman, for allowing me to make that statement.

Senator PRYOR. Thank you.

Senator Isakson?

STATEMENT OF HON. JOHNNY ISAKSON, U.S. SENATOR FROM GEORGIA

Senator ISAKSON. Thank you, Mr. Chairman. I'll be brief but I can't help but think as I was listening to Senator Kerry speak, I ran a company for 22 years and we did about $1.2 million in advertising in various mediums to sell our product. And we would always pick the medium whether it was TV or radio or classified newspaper or display in a magazine by trying to pick the medium we thought the most people would be potential customers for our product would actually go to. And that provided anonymity for the potential customer and made me do a lot of thinking.

What the Internet has done and technology has done it's allowed that anonymous information that was subject to analysts and guesses to become a potential commodity that could actually be sold for purposes other than that determination. So I think it's at a very appropriate time that the Commerce Committee look at this, because of the expanse of the Internet, the expanse of the information and what is taking place in the revolution that it's brought to American marketing.

So I look forward to being a part of the Committee, a part of the work. And look forward to working with Senator Kerry, Senator Pryor and the others on the Committee to find the right message to send and the right road to go down.

Thank you, Mr. Chairman.

Senator PRYOR. Thank you.

Now our first panel here both of these witnesses we have extraordinary bios and lists of accomplishments that we could discuss and we will submit for the record.

But what I'd like to do is just simply introduce them as the Honorable Jon D. Leibowitz, Chairman of the Federal Trade Commission.

And the Honorable Lawrence E. Strickling, the Administrator of the National Telecommunications and Information Administration.

Chairman Leibowitz?

STATEMENT OF HON. JON D. LEIBOWITZ, CHAIRMAN, FEDERAL TRADE COMMISSION

Mr. LEIBOWITZ. Thank you, Chairman Pryor. And Senator Kerry, Senator Isakson and let me also mention Senator Rockefeller, thank you for your leadership on privacy issues as well as for giving me the opportunity to be here with Larry Strickling from the Department of Commerce. Our two agencies have a very long history of cooperation, and we are eager to build on that as we work together to protect consumer privacy while ensuring business growth and innovation.

As you know, over the past several decades the FTC has protected privacy through law enforcement, through education and through policy efforts. Just this week we announced our first major enforcement effort aimed at abusive behavioral marketing practices. We charged the online advertising network Chitika with violating the FTC Act by offering consumers the ability to opt-out of targeted advertising but without telling them that the opt-out vanished in 10 days.

That vanishing opt-out, a 10-day vanishing opt-out, is not only wrong, it is unacceptable. Consumers deserve meaningful and not illusory control over what companies do with their personal information. Chitika has agreed to an order that requires it to destroy personal data it collected and provide an opt-out on all ads that's effective for at least 5 years.

This case, and it is the first of many more privacy enforcement cases you'll see from us, should send a strong signal to the online ad industry. The FTC will not tolerate attempts to subvert consumer choice. And overall we have brought well over 100 spam and spyware cases and 30 data security cases over the last 10 years.

Turning to the policy front. As I heard in your opening statements recognizing the real benefits of information collection, the status quo, as you said, Senator Kerry, isn't acceptable. We released a report on consumer privacy in December designed to reduce privacy burdens on both businesses and consumers alike while ensuring business growth and continuing Internet innovation. The report made three primary recommendations.

First, companies need to bake in privacy protections like data security and accuracy into all of their activities. We call that privacy by design.

Second, choices about privacy of personal data should be presented to consumers in a simple way, and at the time they are making decisions about that data.

And third, transparency needs to be improved. Privacy notices must be clearer, shorter and more standardized, otherwise no one will read them. And indeed very few people actually do.

The comment period on the proposed new framework just closed and we received 446 comments, which may be a record for us. And we expect to issue a final report later this year.

To further the idea of simplifying choices for consumers, the report recommended a Do Not Track mechanism. Now while that name sounds similar to our Do Not Call registry, which the government runs, we're looking instead to the private sector to create a way for consumers to choose whether to allow their Internet surfing to be monitored. Simply put you should have a choice, all of us should have a choice about whether third parties, all invisible to us, can trail us around the Internet as we shop or search for information about say, a medical diagnosis.

This goes back to your point about the deanonymization of information here and over the last 10 years when you're thinking about the Internet. Do Not Track will give all Americans a choice about whether to be followed online. More than that, when data is protected consumers will more readily trust companies in the marketplace and that encourages business growth and business innovation.

Now stakeholders have responded very, very positively to our call for Do Not Track. Two of the largest browser companies, Microsoft and Mozilla, rolled out new mechanisms to allow consumers control over the use of their personal information for online behavioral advertising. The industry has now demonstrated that Do Not Track is feasible so the discussion turns to which approach is best.

One promising effort involves an industry coalition comprised of media and ad marketing companies in an association known as the Digital Advertising Alliance. The Alliance has developed an icon which they hope will be deployed industry wide that will display in targeted advertisements and link to more information and choices. For my part, I still remain concerned that the current proposal won't result in a permanent opt-out for all ad networks. And it doesn't allow consumers to control collection of their personal data just the blocking of ads that go back to them.

But many of the Alliance's members want to go further to protect consumers. My understanding—and actually it's in today's *Wall Street Journal* as well—is that there's a sort of insurgent group of more than 30 companies that wants to prohibit most types of tracking and embrace the Mozilla header. And so we're cautiously optimistic that the Alliance is moving in the right direction.

Mr. Chairman, I ask for unanimous consent for an additional minute.

Senator PRYOR. Sure. Absolutely.

Mr. LEIBOWITZ. So from my perspective I'm sort of agnostic as to whether the private sector should implement Do Not Track or if Congress should require it. I think sometimes it's easier for the private sector to do it. But we do need to make sure that Do Not Track isn't just an empty slogan but that it really works for the American people.

There are five critical principles that we believe should be included in any robust, effective Do Not Track mechanism.

One, Do Not Track should be universal so the consumers don't have to repeatedly make choices on a company by company basis.

Two, Do Not Track should be easy to find and easy to use.

Three, any choices offered should be persistent and should not be deleted if for example, a consumer clears his or her "cookies" or turns off a computer.

Four, Do Not Track should not only allow consumers to opt-out of advertising, it should allow them to opt-out of tracking all together. And personally, from my perspective, I don't mind getting targeted ads. I think there's a real benefit to that. But people ought to be given a choice about whether or not they want to be tracked.

And finally, it should be effective and enforceable without technical loopholes.

We hope to continue to see the private sector develop tools that meet these standards more broadly. We're hopeful that American businesses will step up their efforts. And we've started to see them protect consumer privacy by applying the consensus principles from our report: privacy by design, transparency and consumer choice. Working together with this Committee, and with the Department of Commerce, we believe we can make that happen.

So I thank you for this hearing.

[The prepared statement of Mr. Leibowitz follows:]

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, I am Jon Leibowitz, Chairman of the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on privacy.[1]

Privacy has been an important component of the Commission's consumer protection mission for 40 years. During this time, the Commission has employed a variety of strategies to protect consumer privacy, including law enforcement, regulation, outreach to consumers and businesses, and policy initiatives.[2]

Over the years, the Commission's goal in the privacy arena has remained constant: to protect consumers' personal information and ensure that they have the confidence to take advantage of the many benefits offered by the dynamic and ever-changing marketplace. To meet this objective, the Commission has periodically re-examined its approach to privacy to ensure that it keeps pace with advances in technology and changing business practices as well as to ensure that incentives for American innovation are maintained. The latest effort in this process is a Preliminary FTC Staff Report, released in December, which proposes a framework for protecting consumer privacy in this era of rapid technological change. This proposed framework is intended to inform policymakers, including Congress, as they develop solutions, policies, and potential laws governing privacy, and guide and motivate industry as it develops more robust and effective best practices and self-regulatory guidelines.

This testimony begins by describing the Commission's recent efforts to protect consumer privacy through law enforcement, education, and policy initiatives. It then sets forth some highlights from the Staff Report on consumer privacy, and concludes with a discussion of issues related to a universal choice mechanism for behavioral tracking, commonly referred to as "Do Not Track".

I. The FTC's Efforts to Protect Consumer Privacy

A. Enforcement

The Commission continues to pursue an aggressive and bipartisan privacy enforcement agenda. In the last 15 years, it has brought 32 data security cases; 64 cases against companies for improperly calling consumers on the Do Not Call registry; 86 cases against companies for violating the Fair Credit Reporting Act ("FCRA");[3] 97 spam cases; 15 spyware (or nuisance adware) cases; and 15 cases against companies for violating the Children's Online Privacy Protection Act ("COPPA"). Where the FTC has authority to seek civil penalties, it has aggressively done so. It has obtained $60 million in civil penalties in Do Not Call cases, $21 million in civil penalties under the FCRA, $5.7 million under the CAN–SPAM Act,[4] and $3.2 million under COPPA. Where the Commission does not have authority to seek civil penalties, as in the data security and spyware areas, it has sought such authority from Congress. In addition, the Commission has brought numerous cases against companies for violating the FTC Act by making deceptive claims about the privacy protection they afford to the information they collect, which has the effect of undermining consumer choices on privacy. This testimony describes four such cases that the Commission has brought within the past several months.

Just this week, the Commission announced its first online behavioral advertising case against an online network advertiser, Chitika, that acts as an intermediary between website publishers and advertisers. The Commission alleged that Chitika violated the FTC Act by offering consumers the ability to opt-out of the collection of information to be used for targeted advertising—without telling them that the opt-out lasted only 10 days.[5] The Commission's order prohibits Chitika from making future privacy misrepresentations. It also requires Chitika to provide consumers with an effective opt-out mechanism, link to this opt-out mechanism in its advertisements, and provide a notice on its website for consumers who may have opted out

---

[1] This written statement represents the views of the Federal Trade Commission. Commissioner Kovacic dissents. His concerns about the Commission's testimony, and the report by its staff, are set forth in his statement on the latter. In particular, he believes that the endorsement of a Do Not Track mechanism by staff (in the report) and the Commission (in this testimony) is premature. My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or of any other Commissioner.

[2] Information on the FTC's privacy initiatives generally may be found at *http://business.ftc.gov/privacy-and-security*.

[3] 15 U.S.C. §§ 1681e–i.

[4] 15 U.S.C. §§ 7701–7713.

[5] *Chitika, Inc.*, FTC File No. 102 3087 (Mar. 14, 2011) (consent order accepted for public comment).

when Chitika's opt-out mechanism was ineffective. Finally, the order requires Chitika to destroy any data that can be associated with a consumer that it collected during the time its opt-out mechanism was ineffective.

Second, earlier this month, the Commission approved a final consent order in a case involving the social networking service Twitter.[6] On one level, Twitter is a traditional data security case—the FTC charged that serious lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter. As a result, hackers had access to private "tweets" and non-public user information and took over user accounts, including among others, those of President Obama and Rupert Murdoch. On another level, the case stands for the proposition that social networking services must honor the commitments they make to keep their users' communications private. The order prohibits misrepresentations about the extent to which Twitter protects the privacy of communications, requires Twitter to maintain reasonable security, and mandates independent, comprehensive audits of Twitter's security practices.[7]

Third, in December, the Commission announced a case against EchoMetrix, a company selling a software program called Sentry Parental Controls that enables parents to monitor their children's activities online. The Commission alleged that EchoMetrix sold certain information that it collected from children via this software to third parties for marketing purposes, without telling parents. The Commission's order prohibits the company from sharing information gathered from its monitoring software and requires the company to destroy any such information in its database of marketing information.[8]

Finally, in September, the Commission settled a case against U.S. Search, a data broker that maintained an online service, which allowed consumers to search for information about others. The company allowed consumers to opt-out of having their information appear in search results, for a fee of $10. Although 4,000 consumers paid the fee and opted out, their personal information still appeared in search results. The Commission's settlement requires U.S. Search to disclose limitations on its opt-out offer, and to provide refunds to consumers who had previously opted out.[9]

In addition to these privacy enforcement actions, the Commission has been aggressive on the data security front to ensure that companies protect the sensitive data they collect about consumers. In February 2011, three companies that resell consumers' credit reports agreed to settle FTC charges that they did not take reasonable steps to protect consumers' personal information, which allowed computer hackers to access more than 1,800 credit reports via their clients' computer networks. These are the first cases the FTC has brought against credit report resellers for their failure to ensure that the companies to whom they provide consumer re-

---

[6] *Twitter, Inc.,* FTC File No. 092 3093 (Mar. 11, 2011) (consent order) (resolving allegations that Twitter deceived its customers by failing to honor their choices to designate certain "tweets" as private).

[7] Many of the Commission's earliest consumer privacy cases similarly held companies accountable for their privacy statements and practices. *See, e.g., GeoCities, Inc.,* FTC Docket No. C–3850 (Feb. 5, 1999) (consent order) (alleging that company misrepresented the purposes for which it was collecting personal information from both children and adults); *Liberty Fin. Cos.*, FTC Docket No. C–3891 (Aug. 12, 1999) (consent order) (alleging that site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously); *FTC* v. *ReverseAuction.com, Inc.*, No. 00–0032 (D.D.C. Jan. 10, 2000) (consent order) (alleging that online auctionsite obtained consumer data from competitor site and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business); *FTC* v. *Toysmart.com LLC*, 00–CV–11341–RGS (D. Mass. filed July 10, 2000) (alleging site attempted to sell personal customer information, despite the representation in its privacy policy that such information would never be disclosed to a third party); *FTC* v. *Rennert*, No. CV–S–00–0861–JBR (D. Nev. July 24, 2000) (consent order) (alleging that defendants misrepresented their security practices and how they would use consumer information); *Educ. Research Ctr. of Am., Inc.*; *Student Marketing Grp., Inc.*, FTC Docket No. C–4079 (May 6, 2003) (consent order) (alleging that personal data collected from students for educational purposes was sold to commercial marketers); *The Nat'l Research Ctr. for College & Univ. Admissions*, FTC Docket No. C–4071 (Jun. 28, 2003) (consent order) (same); *Gateway Learning Corp*., FTC Docket No. C–4120 (Sept. 10, 2004) (consent order) (alleging that company rented customer information to list brokers in violation of its privacy policy); *Vision I Props., LLC*, FTC Docket No. C–4135 (Apr. 19, 2005) (consent order) (alleging that a service provider disclosed customer information in violation of merchant privacy policies). *Sears Holdings Mgmt. Corp.*, FTC Docket No. C–4264 (Aug. 31, 2009) (consent order).

[8] *FTC* v. *Echometrix, Inc.*, No. CV10–5516 (E.D.N.Y. Nov. 30, 2010) (consent order).

[9] *US Search, Inc.*, FTC File No. 102 3131 (Sept. 22, 2010) (consent order accepted for public comment).

ports maintain reasonable security.[10] The Commission alleged that the resellers violated the FCRA, the Gramm-Leach-Bliley Safeguards Rule, and Section 5 of the FTC Act. The consent orders bar the companies from violating these laws, require them to implement comprehensive information security programs, and require them to obtain independent audits, every other year for 20 years.

B. Consumer and Business Education

The FTC has done groundbreaking outreach to businesses and consumers in the area of consumer privacy. For example, the Commission's well-known OnGuard Online website educates consumers about spam, spyware, phishing, peer-to-peer ("P2P") file sharing, social networking, laptop security, and identity theft.[11] The FTC has developed additional resources specifically for children, parents, and teachers to help children stay safe online. In response to the Broadband Data Improvement Act of 2008, the FTC produced the brochure Net Cetera: Chatting with Kids About Being Online to give adults practical tips to help children navigate the online world.[12] The publication includes information about how parents should talk to children about online privacy, sexting, and cyberbullying. In less than 1 year, the Commission already has distributed more than 7 million copies of Net Cetera to schools and communities nationwide. The Commission also offers specific guidance to young people concerning certain types of Internet services, including, for example, social networking and video and photo sharing.[13]

Most recently, the FTC released a consumer education publication on the safe use of wi-fi hot spots.[14] The publication, available on the FTC and Onguard Online websites, explains that when using wireless networks, consumers should convey personal information only if it is encrypted—either through an encrypted website or a secure network. The piece notes that an encrypted website is one whose URL begins with "https", rather than "http"; it further notes that in order to be secure, a Wi-Fi network must be password-protected.

Business education is also an important priority for the FTC. For example, the Commission developed a widely-distributed guide to help small and medium-sized businesses implement appropriate data security for the personal information they collect and maintain.[15] The FTC also develops business education materials to respond to specific emerging issues, such as a recent brochure on security risks associated with P2P file-sharing software.[16]

C. Policy and Rulemaking Initiatives

The Commission's efforts with respect to privacy include public workshops and reports to examine the implications of new technologies on consumer privacy. For example, in November 2007, the Commission held a two-day Town Hall event to discuss the privacy implications of online behavioral advertising.[17] Based upon the Town Hall discussions, staff released for public comment a set of proposed principles to encourage industry members to improve their behavioral advertising practices.[18] Thereafter, in February 2009, staff released a report ("OBA Report") setting forth the following revised principles based on the comments received: (1) transparency and consumer control; (2) reasonable security and limited retention for consumer data; (3) affirmative express consent for material retroactive changes to privacy policies; and (4) affirmative express consent for the use of sensitive data.[19]

---

[10] *SettlementOne Credit Corp.*, File No. 082 3208; *ACRAnet, Inc.*, File No. 092 3088; and *Fajilan and Associates, Inc.*, File No. 092 3089 (Feb. 3, 2011) (consent orders accepted for public comment).

[11] *See http://www.onguardonline.gov/topics/social-networking-sites.aspx.* Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alertaena Línea have attracted nearly 12 million unique visits.

[12] *See* Press Release, FTC, *OnGuardOnline.gov* Off to a Fast Start with Online Child Safety Campaign (Mar. 31, 2010), available at *http://www.ftc.gov/opa/2010/03/netcetera.shtm*.

[13] *See http://www.onguardonline.gov/topics/social-networking-sites.aspx; http://www.onguardonline.gov/topics/net-cetera-mobile-phones.aspx*.

[14] *See http://www.onguardonline.gov/topics/hotspots.aspx*.

[15] *See Protecting Personal Information: A Guide For Business, available at http://www.ftc.gov/infosecurity*.

[16] *See generally http://business.ftc.gov/privacy-and-security*.

[17] FTC Town Hall, *Ehavioral Advertising: Tracking, Targeting, & Technology* (Nov.1–2, 2007), available at *http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml*.

[18] *See* FTC Staff, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles* (Dec. 20, 2007), available at *http://www.ftc.gov/os/2007/12/P859900stmt.pdf*.

[19] *See FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising* (Feb. 2009), available at *http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf,* at 33–37, 46.

Continued

The Commission also reviews its rules periodically to ensure that they are appropriately updated in light of changes in the marketplace. For example, the Commission is currently reviewing its rule implementing the COPPA and anticipates completing that review in the coming months.[20]

II. Privacy Roundtables and Report

The Commission also recently conducted a series of public roundtables on consumer privacy,[21] which took place in December 2009, and January and March 2010. The roundtables served to explore the effectiveness of current privacy approaches in addressing the challenges of the rapidly evolving market for consumer information, including consideration of the risks and benefits of consumer information collection and use; consumer expectations surrounding various information management practices; and the adequacy of existing legal and self-regulatory regimes to address privacy interests. Staff issued a preliminary privacy report in December 2010,[22] which discusses the major themes that emerged from these roundtables, including the ubiquitous collection and use of consumer data; consumers' lack of understanding and ability to make informed choices about the collection and use of their data; the importance of privacy to many consumers; the significant benefits enabled by the increasing flow of information; and the blurring of the distinction between personally identifiable information and supposedly anonymous or de-identified information.[23]

At the roundtables, stakeholders across the board emphasized the need to improve the transparency of businesses' data practices, simplify the ability of consumers to exercise choices about how their information is collected and used, and ensure that businesses take privacy-protective measures as they develop and implement systems that involve consumer information. At the same time, the roundtable commenters and participants urged regulators to be cautious about restricting the exchange and use of consumer data in order to preserve the substantial consumer benefits made possible through the flow of information. Based on these comments, the preliminary staff privacy report proposed a new framework to guide policymakers and industry as they consider further steps to improve consumer privacy protection.

A. The Proposed Framework

The proposed framework included three main concepts. First, FTC staff proposed that companies should adopt a "privacy by design" approach by building privacy protections into their everyday business practices. Such protections include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer in use, and implementing reasonable procedures to promote data accuracy. Companies also should implement and enforce procedurally sound privacy practices throughout their organizations, including, for example, assigning personnel to oversee privacy issues, training employees on privacy issues, and conducting privacy reviews when developing new products and services. Such concepts are not new, but the time has come for industry to implement them systematically. Implementation can be scaled, however, to each company's business operations. For example, the Staff Report recommended that companies that collect and use small amounts of nonsensitive consumer data should not have to devote the same level of resources to implementing privacy programs as companies that collect vast amounts of consumer data or data of a sensitive nature.

Second, the Commission staff proposed that companies provide simpler and more streamlined choices to consumers about their data practices. Under this approach, consumer choice would not be necessary for a limited set of "commonly accepted" data practices, thus allowing clearer, more meaningful choice with respect to practices of greater concern. This component of the proposed framework reflects the concept that consumers reasonably expect companies to engage in certain practices

---

The revisions primarily concerned the principles' scope and application to specific business models. *Id.* at 20–30.

[20] *See http://business.ftc.gov/documents/coppa-rulemaking-and-rule-reviews*; Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 17 Fed. Reg. 17089 (Apr. 5, 2010), available at *http://www.ftc.gov/os/fedreg/2010/april/P104503coppa-rule.pdf*.

[21] *See* Press Release, FTC, FTC to Host Public Roundtables to Address Evolving Privacy Issues (Sept. 15, 2009), available at *http://www.ftc.gov/opa/2009/09/privacyrt.shtm*.

[22] *See A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), available at *http://www.ftc.gov/os/2010/12/101201privacyreport.pdf*. Commissioners Kovacic and Rosch issued concurring statements available at *http://www.ftc.gov/os/2010/12/101201privacyreport.pdf* at Appendix D and Appendix E, respectively.

[23] *Id.* at 22–38.

namely, product and service fulfillment, internal operations such as assessing the quality of services offered, fraud prevention, legal compliance, and first-party marketing. Some of these practices, such as a retailer's collection of a consumer's address solely to deliver a product the consumer ordered, are obvious from the context of the transaction, and therefore, consumers' consent to them can be inferred. Others are sufficiently accepted or necessary for public policy reasons that companies need not request consent to engage in them. The Staff Report suggested that by clarifying those practices for which consumer consent is unnecessary, companies will be able to streamline their communications with consumers, which will reduce the burden and confusion on consumers and businesses alike.

For data practices that are not "commonly accepted," consumers should have the ability to make informed and meaningful choices. To be most effective, choices should be clearly and concisely described and offered at a time and in a context in which the consumer is making a decision about his or her data. Depending upon the particular business model, this may entail a "just-in-time" approach, in which the company seeks consent at the point a consumer enters his personal data or before he accepts a product or service. One way to facilitate consumer choice is to provide it in a uniform and comprehensive way. Such an approach has been proposed for behavioral advertising, whereby consumers would be able to choose whether to allow the collection and use of data regarding their online searching and browsing activities. This idea is discussed further below.

Third, the Staff Report proposed a number of measures that companies should take to make their data practices more transparent to consumers. For instance, in addition to providing the contextual disclosures described above, companies should improve their privacy notices so that consumers, advocacy groups, regulators, and others can compare data practices and choices across companies, thus promoting competition among companies. The staff also proposed providing consumers with reasonable access to the data that companies maintain about them, particularly for non-consumer-facing entities such as data brokers. Because of the significant costs associated with access, the Staff Report noted that the extent of access should be proportional to both the sensitivity of the data and its intended use. In addition, the Staff Report stated that companies must provide prominent disclosures and obtain affirmative consent before using data in a materially different manner than claimed when the data was collected.

Finally, the Staff Report proposed that stakeholders undertake a broad effort to educate consumers about commercial data practices and the choices available to them. Increasing consumer understanding of the commercial collection and use of their information is important to both empowering consumers to make informed choices regarding their privacy and facilitating competition on privacy across companies. In addition to proposing these broad principles, the staff sought comment from all interested parties to help guide further development and refinement of the proposed framework through February 18, 2011. Close to 450 comments were received and staff expects to issue a final report this year.

B. Do Not Track

As noted above, the Staff Report included a recommendation to implement a universal choice mechanism for behavioral tracking, including behavioral advertising, often referred to as "Do Not Track."[24] Although behavioral tracking benefits consumers by helping support online content and services and allowing personalized advertising that many consumers value, the practice remains largely invisible to most consumers. Some surveys[25] show that certain consumers who are aware of the practice are uncomfortable with it.[26] A recent *USA Today*/Gallup poll found that 47

[24] *See FTC Staff Report, supra note 22. See also* Rosch concurring statement, *id.*, in which Commissioner Rosch supported a Do Not Track mechanism only if it were "technically feasible" and implemented in a fashion that provides informed consumer choice regarding all the attributes of such a mechanism. To clarify, Commissioner Rosch continues to believe that a variety of questions need to be answered prior to the endorsement of any particular Do Not Track mechanism.

[25] Consumer survey evidence, by itself, has limitations. For instance, the way questions are presented may affect survey results. Also, while survey evidence may reveal a consumer's stated attitudes about privacy, survey evidence does not necessarily reveal what actions a consumer will take in real-world situations. The Commission does not endorse the reliability or methodology of any surveys discussed herein.

[26] *See, e.g., Transcript of December 7, 2009, FTC Privacy Roundtable,* Remarks of Alan Westin of Columbia University, at 93–94, available at *http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdf; Written Comment of Berkeley Center for Law & Technology, Americans Reject Tailored Advertising and Three Activities that Enable*

Continued

percent of consumers would like to choose which advertisers may deliver them targeted advertisements and 37 percent would like to receive no targeted advertisements at all.[27] In another poll, 80 percent of consumers supported a Do Not Track option.[28] In addition, according to a recent *Wall Street Journal* article, because of concerns that third-party tracking may be intrusive, some websites are increasing their scrutiny of such third-party tracking on their sites.[29]

In light of the concerns expressed about online tracking, the Staff Report recommended a Do Not Track mechanism. A robust, effective Do Not Track system would ensure that consumers can opt-out once, rather than having to exercise choices on a company-by-company or transaction-by-transaction basis. Such a universal mechanism could be accomplished through legislation or potentially through robust, enforceable self-regulation.

The FTC repeatedly has called on stakeholders to develop and implement better tools to allow consumers to control the collection and use of their online browsing data.[30] Industry participants have begun to respond to this call. Two major browser vendors, Microsoft and Mozilla, have recently announced the development of new choice mechanisms for online behavioral advertising that seek to provide increased transparency, greater consumer control, and improved ease of use.[31] Just as important, the World Wide Web Consortium (W3C) has accepted a submission by Microsoft to consider a technical standard for a universal choice mechanism.The W3C announced an April 2011 workshop to begin the public dialogue with relevant stakeholders regarding how to incorporate do not track preferences into Internet browsing so websites can respect a user's preference not to be tracked.[32] Finally, just last week, Stanford's Center for Internet and Society and Mozilla jointly submitted a proposal to the Internet Engineering Task Force outlining a header-based Do Not Track mechanism and discussing how web services should respond to such a mechanism.[33]

The online advertising industry has also made progress in this area. For example, an industry coalition comprised of media and marketing associations, known as the Digital Advertising Alliance, has developed self-regulatory guidelines and an opt-out mechanism for behavioral advertising.[34] The coalition has developed an icon to display in or near targeted advertisements that links to more information and choices

---

It, cmt. #544506–00113, available at *http://www.ftc.gov/os/comments/privacyroundtable/544506–00113.pdf; Written Comment of Craig Wills, Personalized Approach to Web Privacy Awareness, Attitudes and Actions,* cmt. #544506–00119, available at *http://www.ftc.gov/os/comments/privacyroundtable/544506-00119.pdf; Written Comment of Alan Westin, How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings,* cmt. #544506–00052, available at *http://www.ftc.gov/os/comments/privacyroundtable/544506-00052.pdf; see also Poll: Consumers Concerned About Internet Privacy, Consumers Union,* available at *http://www.consumersunion.org/pub/core__tele com__and__utilities/006189.html*.

[27] *See U.S. Internet Users Ready to Limit Online Tracking for Ads* (Dec. 21, 2010), available at *http://www.gallup.com/poll/145337/internet-users-ready-limit-online-tracking-ads.aspx*.

[28] *See* News Release, Consumer Watchdog, Americans Favor Broad Range Of Online Privacy Protections for Consumers (Jul. 27, 2010), available at *http://www.consumerwatchdog.org/newsrelease/consumer-watchdog-poll-finds-concern-about-g oogles-wi-spy-snooping*.

[29] Jessica Vascellaro, *Websites Rein in Tracking Tools,* WALL ST. J., Nov. 9, 2010, available at *http://online.wsj.com/article/SB10001424052748703957804575602730678670278.html*.

[30] *See e.g.*, Do Not Track: Hearing before the Subcomm. On Commerce, Trade and Consumer Prot. of the H. Comm. On Energy and Commerce, 111th Cong. (Dec. 2, 2010), available at *http://www.ftc.gov/os/testimony/101202donottrack.pdf* (prepared statement of the FTC, Commissioner Kovacic dissenting).

[31] *See* Press Release, Microsoft, Providing Windows Customers with More Choice and Control of Their Privacy Online with Internet Explorer 9 (Dec. 7, 2010), available at *http://www.microsoft.com/presspass/features/2010/dec10/12-07ie9privacyqa.mspx*; Mozilla Blog, Mozilla Firefox 4 Beta, now including "Do Not Track" capabilities, *http://blog.mozilla.com/blog/2011/02/08/mozilla-firefox–4-beta-now-including-do-not-track-cap abilities/* (Feb. 8, 2011).

[32] *See* W3C Blog, Do Not Track at W3C, *http://www.w3.org/QA/2011/02/do__not__track__at__w3c.html* (Feb. 24, 2011).

[33] *See* Do Not Track: A Universal Third-Party Web Tracking Opt Out (Mar. 7, 2011), available at *http://tools.ietf.org/html/draft-mayer-do-not-track–00*; *see also http://firstpersoncookie.wordpress.com/2011/03/09/mozilla-makes-joint-submission-to-ietf-on-d nt/*.

[34] *See* Press Release, Interactive Advertising Bureau, Major Marketing Media Trade Groups Launch Program to Give Consumers Enhanced Control over Collection and Use of Web Viewing Data for Online Behavioral Advertising (Oct. 4, 2010), available at *http://www.iab.net/about__the__iab/recent__press__releases/press__release__archive/press__release/pr–100410*; Tony Romm and Kim Hart, Political Intel: FTC Chairman on Self-Regulatory Ad Effort, POLITICO Forums, *http://dyn.politico.com/members/forums/thread.cfm?catid=24&subcatid=78&threadid=4611665* (Oct. 11, 2010).

and has pledged to implement this effort industry-wide.[35] The coalition reports that adoption of the icon and simplified disclosures grew dramatically at the end of last year.[36] In addition, Google has developed a browser add-on that can be used to block targeted advertisements from companies that participate in the Digital Advertising Alliance.[37]

These recent industry efforts to improve consumer control are promising, but they are still in the embryonic stage, and their effectiveness remains to be seen. As industry continues to explore technical options and implement self-regulatory programs, and Congress continues to examine Do Not Track, several issues should be considered. First, any Do Not Track system should be implemented universally, so that consumers do not have to repeatedly opt-out of tracking on different sites. Second, the choice mechanism should be easy to find, easy to understand, and easy to use. Third, any choices offered should be persistent and should not be deleted if, for example, consumers clear their cookies or update their browsers. Fourth, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes.[38]

Finally, it is important to emphasize what is meant by "tracking" as stakeholders continue to consider "Do Not Track" approaches. Consumers certainly may want to opt-out of more than targeted advertising—they may want to opt-out of the creation and use of behavioral profiles for any secondary purposes. For example, they may want to be sure that their browsing behavior is not used to make employment or insurance decisions about them. They may also want to opt-out of having their browsing behavior sold to data brokers for unspecified future uses. At the same time, no system that allows for unrestricted web browsing can or should prohibit information collection entirely. As noted the Staff Report, information collection is necessary for fraud prevention and other commonly accepted practices, such as capping the number of times a consumer sees a particular advertisement. The limited nature of that collection, however, is qualitatively different from the collection of information to track and profile consumers as they browse the web. Given these considerations, an effective Do Not Track system would go beyond simply opting consumers out of receiving targeted advertisements; it would opt them out of collection of behavioral data for all purposes that are not commonly accepted.

Commission staff will monitor further industry innovation in this area, which may build upon existing industry initiatives and incorporate elements of the different mechanisms being proposed today.

III. Conclusion

Thank you for the opportunity to provide the Commission's views. We look forward to continuing this important dialogue with Congress and this Committee.

Senator PRYOR. Mr. Strickling?

---

[35] The coalition has stated that providing consumers with choices about online advertising is essential to building the trust necessary for the marketplace to grow. *See Interactive Advertising Bureau, supra* note 34.

[36] *See Written Comment of the Direct Marketing Assoc. Responding to Preliminary Staff Report*, cmt. #00449, at 21.

[37] *See* Google Chrome Web Store, Keep My Opt-Outs, available at *https://chrome.google.com/webstore/detail/hhnjdplhmcnkiecampfdgfjilccfpfoe*; *see also* Google Public Policy Blog, Keep your opt-outs *http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html* (Jan. 24, 2011).

[38] For example, consumers may believe they have opted out of tracking if they block third-party cookies on their browsers; yet they may still be tracked through Flash cookies or other mechanisms.

A Flash cookie, or a Flash local shared object, is a data file that is stored on a consumer's computer by a website that uses Adobe's Flash player technology. Like a regular http cookie, a Flash cookie can store information about a consumer's online activities. Unlike regular cookies, Flash cookies are stored in an area not controlled by the browser. Thus, when a consumer deletes or clears the cookies from his browser using tools provided through the browser, this may not delete Flash cookies stored on his computer.

Recently, a researcher released a software tool that demonstrates several technical mechanisms in addition to Flash cookies that websites can use to persistently track consumers, even if they have attempted to prevent such tracking through existing tools. *See http://samy.pl/evercookie; see also* Tanzina Vega, *New Web Code Draws Concerns Over Privacy Risks,* THE NEW YORK TIMES, Oct. 10, 2010, available at *http://www.nytimes.com/2010/10/11/business/media/11privacy.html*.

STATEMENT OF HON. LAWRENCE E. STRICKLING, ASSISTANT SECRETARY FOR COMMUNICATIONS AND INFORMATION, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

Mr. STRICKLING. Thank you, Chairman Pryor, Senators Kerry and Isakson. It's a pleasure to be here today to testify on behalf of the Department of Commerce to discuss the state of online consumer privacy. And I welcome the opportunity to discuss how we can better protect consumer data privacy in this rapidly evolving Internet economy. And in doing so I'm quite pleased to testify here today with Chairman Jon Leibowitz of the Federal Trade Commission.

As the principal advisor to the President on communications and information policy, the NTIA has been hard at work over the last 2 years with Secretary Locke's Internet Policy Task Force, Department of Commerce General Counsel Cam Kerry, and colleagues throughout the Executive Branch, to conduct a broad assessment of how well our current policy framework for consumer data is serving consumers, businesses and other participants in the Internet economy.

I would also like to thank, in particular, the Federal Trade Commission for its collaboration with us and its leadership over the years in addressing this important issue.

To guide the overall agenda of the Internet Policy Task Force, which includes issues in addition to privacy, we have focused on two key principles.

The first is the idea of trust. It's imperative for the sustainability and continued growth of the Internet that we preserve the trust of all actors on the Internet. And nowhere is this clearer than in the context of consumer privacy. If users do not trust that their personal information is safe on the Internet they'll be reluctant to adopt new services.

Our second principle is that we want to encourage multi-stakeholder processes to address key Internet issues. We want stakeholders to come together to deal with these issues in ways that display the flexibility, speed and efficiency that often are lacking with more traditional regulatory responses.

These two principles inform the new framework for addressing online privacy that the Department proposed in its privacy "Green Paper" last December. The key elements of this framework include the following:

First, we recommended the establishment of a set of Fair Information Practice Principles as the foundation for the protection of consumer privacy in the Internet economy. These principles will set a baseline of consistent, comprehensible data privacy protection in new and established commercial contexts.

Second, to promote flexibility and speed to address privacy issues as they arise, the "Green Paper" recommended that the Department engage actively with industry and consumer groups to develop enforceable codes of conduct.

And third, consistent with the FTC's existing enforcement role in the protection of privacy, the "Green Paper" recommends strengthening the Commission's authority to enforce these baseline privacy principles.

We received roughly 100 comments on the "Green Paper" and we are working hard to prepare a final document later this spring as a statement of Administration policy in this area. But, as we have reviewed the comments and we continued our discussions, I can report today that the Administration now recommends that Congress enact legislation to provide a firm legal foundation supporting specific aspects of this new policy.

We specifically recommend that any legislation to provide a stronger statutory framework to protect consumer privacy should contain three key elements.

First, it should create baseline consumer data privacy protections—as Senator Kerry referred to it, a consumer bill of rights—that are enforceable at law. Specifically, we support making a comprehensive set of FIPPs the basis of this law. This set of agreed-upon principles would provide clear privacy protections for personal data in the commercial context in which existing privacy laws do not apply or offer adequate protection.

Second, legislation should provide the FTC with the authority to enforce any baseline protections. Granting the FTC explicit authority to enforce baseline privacy principles will strengthen its role in consumer data privacy protection and enforcement, resulting in better protection for consumers.

Third, legislation should create a framework that provides incentives for the development of enforceable codes of conduct as well as continued innovation around privacy protections. These codes can allow industry and government to adapt rapidly to a fast evolving online marketplace. And one incentive we urge Congress to consider is to give the FTC the authority to offer a safe harbor for companies that implement codes of conduct that are consistent with the baseline protections.

This statutory framework is designed to be flexible, to keep its requirements well-tailored, and to provide a basis for greater interoperability with other countries' privacy laws.

Working together with Congress, the FTC, the Executive Office of the President and other stakeholders, I am confident in our ability to provide consumers with meaningful privacy protections in the Internet economy, backed by effective enforcement that could adapt to changes in technology, market conditions, and consumer expectations. Establishing and maintaining this dynamic consumer data privacy framework is not a one shot game, and it will require the ongoing engagement of all stakeholders. The Department and the Administration are firmly committed to that engagement.

With or without legislation, the Department and NTIA will continue to make consumer data privacy a top priority. We will convene Internet stakeholders to discuss how best to encourage the development of privacy codes of conduct. The Department will support the Administration's efforts to encourage global interoperability by stepping up our engagement in international policy-making bodies. And we will continue to work with Congress and all other stakeholders to develop consensus on reforms to our consumer data privacy policy framework.

I look forward to working with this Committee on this important issue, starting with answering any questions you have for me today. Thank you.

[The prepared statement of Mr. Strickling follows:]

PREPARED STATEMENT OF HON. LAWRENCE E. STRICKLING, ASSISTANT SECRETARY FOR COMMUNICATIONS AND INFORMATION, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

I. Introduction

Chairman Rockefeller, Ranking Member Hutchison, distinguished Committee Members, thank you for the opportunity to testify on behalf of the Department of Commerce ("Department") to discuss Internet privacy policy reform. I welcome the opportunity to discuss how we can better protect consumer data privacy in the rapidly evolving Internet Age. In doing so, I am pleased to testify here today with Jonathan Leibowitz, the Chairman of the Federal Trade Commission (FTC).

As the principal advisor to the President on communications and information policy, the National Telecommunications and Information Administration (NTIA) has been hard at work over the last 2 years with Secretary Locke's Internet Policy Task Force and colleagues throughout the Executive Branch to conduct a broad assessment of how well our current consumer data privacy policy framework serves consumers, businesses, and other participants in the Internet economy. Over the same period of time, the Internet Policy Task Force has engaged, formally and informally, with a broad array of stakeholders, including companies, consumer advocates, academic privacy experts, and other government agencies. We identified privacy as a key issue in strengthening consumer trust, which, in turn, is critical to realizing the full potential for innovation and growth of the Internet. Our work culminated in the release of the Task Force's "Green Paper" on consumer data privacy in the Internet economy on December 16, 2010. The Green Paper made ten separate recommendations about how to strengthen consumer data privacy protections in ways that also promote innovation, but it also brought to light many additional questions.

We sought public comment on these recommendations, and we have been busy considering the roughly 100 written responses that were filed. One general conclusion to be drawn from the comments is that the commenters believe that American consumers should have stronger privacy protections, and the companies that run our Internet economy should have clearer rules of the road to guide their uses of data about consumers.

II. Stakeholders' Perspectives on Our Current Consumer Data Privacy Framework

The Internet economy is sparking tremendous innovation. During the past fifteen years, networked information technologies—personal computers, mobile phones, wireless connections and other devices—have been transforming our social, political and economic landscape. A decade ago, going online meant accessing the Internet on a computer in your home. Today,"going online" includes smartphones, portable games, and interactive TVs, with numerous companies developing global computing platforms in the "cloud."

The Internet is also an essential platform for economic growth, both domestically and globally. Almost any transaction you can think of is being conducted online—from consumers paying their utility bills and people purchasing books, movies and clothes, to major corporations paying their vendors and selling to their customers. According to the U.S. Census Bureau, domestic online transactions currently total about $3.7 trillion annually.[1] Internet commerce is a leading source of job growth as well, with the number of domestic IT jobs growing by 26 percent from 1998 to 2008, four times faster than U.S. employment as a whole.[2] By 2018, IT employment is expected to grow by another 22 percent.[3]

As powerful and exciting as these developments are, they also raise new privacy issues. The large-scale collection, analysis, and storage of personal information is becoming more central to the Internet economy. These activities help to make the online economy more efficient and companies more responsive to their customer needs. Yet these same practices also give rise to growing unease among consumers, who are unsure about how data about their activities and transactions are collected, used, and stored.[4] A basic element of our current consumer data privacy framework

---

[1] U.S. Census Bureau, Commerce Department, "E-Stats," May 27, 2010, available at *http://www.census.gov/econ/estats/2008/2008reportfinal.pdf*.

[2] Commerce Secretary Gary Locke, Remarks on Cybersecurity and Innovation, Georgetown University, Washington, D.C. (September 23, 2010).

[3] *Id.*

[4] According to a recent survey, 83 percent of adults say they are "more concerned about online privacy than they were 5 years ago." Common Sense Media, Online Privacy: What Does It Mean

is the privacy policy. As we mentioned in the Green Paper, these lengthy, dense, and legalistic documents do not appear to be effective in informing consumers of their online privacy choices. Surveys show that most Americans incorrectly believe that a website that has an online privacy policy is prohibited from selling personal information it collects from customers.[5] In addition, many consumers believe that having a privacy policy guarantees strong privacy rights, which is not necessarily the case.[6]

The difficulty of understanding a single privacy policy, however, is modest when compared to the problem of comprehending how personal data flows in today's online environment. A recent study found that 36 of the 50 most-visited websites state in their privacy policies that they allow third-party tracking.[7] This same study found that a few prominent sites allow more than 20 different third-party tracking mechanisms in the course of a month. One site even allowed 100 such mechanisms.[8] As the study points out, the privacy policy of the site that an individual actually visits typically does not apply to these third parties.[9] In other words, to fully understand the privacy implications of using a particular site, individuals will often have to begin by considering the privacy policies of many other entities that could gain access to data about them.

As Americans begin using smartphones and other mobile Internet devices in addition to, or instead of, laptop and desktop computers, the difficulties of understanding personal data flow become even more acute. The small screens that enable us to carry blogs, social networks, and video around in our pockets pose a new challenge to presenting consumers with information about personal data collection and use. These devices may also make location information available, which opens the door to an amazing array of new applications and services, but also adds further complexity to consumer data privacy issues.[10] Assuring consumers that their privacy interests will be protected in this rapidly changing environment is our core challenge.

During the Department's outreach to stakeholders, we received comments from consumer groups, industry, and leading privacy scholars, all of whom agreed that large proportions of Americans do not fully understand and appreciate what information is being collected about them, and how they are able to stop certain practices from taking place.[11] Several consumer advocacy and civil liberties groups expressed these concerns. These groups supported the Department's overall recommendation to develop stronger privacy protections for personal data in the commercial setting. One group expressed this shared view about a basic lack of transparency particularly well:

> [C]onsumers face a continuum of risk to personal privacy, ranging from minor nuisances to improper disclosures of sensitive information and identity theft. Such unscrupulous practices, carried out without the consumers' knowledge or consent, lead to diminished consumer trust in Internet data practices, thus stunting growth and innovation.[12]

Moreover, many consumer groups made a strong economic case for consumer data privacy reform. Simply put, the inability to distinguish among companies' privacy practices may lead consumers to conclude that all companies engage in equally invasive practices. As one group noted, "even companies willing to adopt the most

---

to Parents and Kids (2010), available at *http://www.commonsensemedia.org/sites/default/files/privacypoll.pdf* (last visited March 5, 2011).

[5] Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathaniel Good & Jens Grossklags, *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: JOURNAL OF LAW & POLICY 723 (2007), available at *http://www.is-journal.org/*.

[6] Chris Jay Hoofnagle & Jennifer King, Research Report: What Californians Understand About Privacy Offline (2008), available at *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075*.

[7] Joshua Gomez, Travis Pinnick, and Ashkan Soltani, *Know Privacy*, at 27, June 1, 2009, available at *http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf*.

[8] *Id.* at 26.

[9] *Id.*

[10] *See, e.g.*, Frank Groeneveld, Barry Borsboom, and Boy van Amstel, Over-sharing and Location Awareness, Feb. 24, 2010, *http://www.cdt.org/blogs/cdt/over-sharing-and-location-awareness* (discussing, in the context of their project called "Please Rob Me," how adding location information to information posted on social networking sites can have unintended consequences).

[11] All comments that the Department received in response to the Green Paper are available at *http://www.ntia.doc.gov/comments/101214614–0614–01/*.

[12] Consumers Union, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 2.

stringent privacy policies find that overseas customers are skeptical of those assurances because of the lack of U.S. privacy laws to back them up." [13]

Interestingly, industry shares these views in many respects. Some of the leading innovators in the Internet economy see things the same way. In comments, a leading IT company refuted the argument that baseline consumer data privacy protections would slow innovation: "We disagree with the arguments some have advocated against the adoption of legislation, particularly that privacy legislation would stifle innovation and would hinder the growth of new technologies by small businesses. Instead, we believe that well-crafted legislation can actually enable small business e-commerce growth." [14] Other companies reiterated the call for Federal privacy legislation; one argued that "dramatic and rapid technological advances are testing how the fundamental principles that underpin consumer privacy and data protection law—such as notice, consent, reasonable security, and data retention—should apply." [15] Another stressed that "consumer-facing companies . . . have powerful market incentives to protect user privacy, and must respond to user demands in order to remain competitive." [16] To ensure continued consumer trust, this company "strongly supports the development of a comprehensive privacy framework for commercial actors . . . that create[s] a baseline for privacy regulation that is flexible, scalable, and proportional." [17] In short, uncertainty over keeping the trust of consumers online is as unsettling for some businesses as it is for consumers.

Commenters were not unanimous in their support for legislation, and some expressed opposition to enacting baseline consumer data privacy legislation. Some commenters asserted that legislation is appropriate only where "particularly sensitive privacy interests" are concerned.[18] Others argued that a legislative framework would be "too inflexible," [19] a "one size fits all" [20] collection of rules that will become "static." [21] The Department took these concerns seriously when developing the Green Paper's Dynamic Privacy Framework for consumer data. A central feature of the Framework is an emphasis on developing industry-specific, enforceable codes of conduct that establish how Fair Information Practice Principles (FIPPs) apply in a given commercial context. And these concerns are reflected in the contours of the recommendations in this testimony.

Thus, based on an initial review of comments, the Department sees a shared set of principles that could help to inform our efforts to reform consumer data privacy in the Internet economy. The general agreement of commenters appears to rest on two tenets. First, to harness the full power of the Internet age, we need to establish norms and ground rules that promote innovative uses of information while respecting consumers' legitimate privacy interests. Second, as we go about establishing these privacy guidelines, we also need to be careful to avoid creating an overly complicated regulatory environment.

III. Strengthening Our Consumer Data Privacy Framework Through Baseline Protections

Exactly three months ago, the Department published its Green Paper, which contained a set of preliminary policy recommendations to enhance consumer protection, strengthen online trust, and bolster the Internet economy. The paper made ten recommendations and sought comment on a set of additional questions. In response to the paper, the Department received thoughtful and well-researched comments from over a hundred stakeholders representing industry, consumer groups, and academia.

Having carefully reviewed all stakeholder comments to the Green Paper, the Department has concluded that the U.S. consumer data privacy framework will benefit from legislation to establish a clearer set of rules for the road for businesses and

---

[13] Center for Democracy and Technology, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 3.

[14] Intel, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 3.

[15] Microsoft, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 1.

[16] Google, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 2.

[17] *Id.*

[18] Financial Services Forum, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 8.

[19] American Association of Advertising Agencies *et al.,* Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 1.

[20] Direct Marketing Ass'n, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 4; *see also* American Business Media, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 4; Computer & Communications Industry Association, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 18; Keller & Heckman, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011 at 1.

[21] Business Software Alliance, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 4.

consumers, while preserving the innovation and free flow of information that are hallmarks of the Internet. The Department's privacy Green Paper—much like the staff report of the Federal Trade Commission (FTC)—highlights the need for stronger privacy protections for American consumers. As pointed out in the Commerce report, the United States has a range of data privacy laws that apply to individual sectors of the economy, such as health care, consumer credit, and personal finance. But these laws may not offer protection to some of the data uses associated with consumers' activities in the Internet economy. An overarching set of privacy principles on which consumers and businesses can rely could create a stronger foundation for consumer trust in the Internet by providing this broadly applicable framework.

Legislation to provide a stronger statutory framework to protect consumers' online privacy interests should contain three key elements. First, the Administration recommends that legislation set forth baseline consumer data privacy protections—that is, a "consumer privacy bill of rights." Second, legislation should provide the FTC with the authority to enforce any baseline protections. Third, legislation should create a framework that provides incentives for the development of codes of conduct as well as continued innovation around privacy protections, which could include providing the FTC with the authority to offer a safe harbor for companies that implement codes of conduct that are consistent with the baseline protections. This statutory framework is designed to be flexible, to keep its requirements well-tailored, and to provide a basis for greater interoperability with other countries' privacy laws.

A. Enacting a Consumer Privacy Bill of Rights

The Administration urges Congress to enact a "consumer privacy bill of rights" to provide baseline consumer data privacy protections. Legislation should consider statutory baseline protections for consumer data privacy that are enforceable at law and are based on a comprehensive set of FIPPs. Comprehensive FIPPs, a collection of agreed-upon principles for the handling of consumer information, would provide clear privacy protections for personal data in commercial contexts that are not covered by existing Federal privacy laws or otherwise require additional protection. To borrow from one of the responses we received, baseline FIPPs are something that consumers want, companies need, and the economy will appreciate.[22]

The Administration recommends that the baseline should be broad and flexible enough to allow consumer privacy protection and business practices to adapt as new technologies and services emerge. As noted by two privacy scholars, "[b]roadly worded legislation . . . motivates firms to produce an industry code of conduct as a way to construe and clarify the statutory scheme. Thus, baseline privacy legislation and incentives for industry to develop codes of conduct can go hand-in-hand."[23]

Finally, a baseline law holds the promise of making our consumer data privacy framework more interoperable with international frameworks. Again, leading Internet innovators support baseline legislation as a means of achieving this objective. For example, a leading online company noted that "FIPPs is a common language used by many governments worldwide, so use of similar terminology will enhance opportunities for agreement and practical approaches to data policy."[24] A Web standards organization stated that "[e]stablishing baseline commercial data privacy principles contribute[s] to the further harmonization of the global e-commerce market at least for the countries attached to the OECD, and improve[s] the transatlantic relations on online services of all sorts."[25] Other comments, which represent a wide variety of American companies, consumer advocates, and academic scholars, also supported this position, often noting that improving global interoperability could benefit companies by reducing their compliance burdens overseas.[26]

---

[22] *See* Comment of Hewlett-Packard Co. on Notice of Inquiry, at 2, June 14, 2010, available at *http://www.ntia.doc.gov/comments/100402174–0175–01/attachments/HP%20Comments%2E pdf*.

[23] Professors Ira Rubinstein and Dennis Hirsch, Comment to the Department Privacy Green Paper, January 28, 2011, available at *http://www.ntia.doc.gov/comments/101214614–0614–01/comment.cfm?e=D120453B-FB2B–4034–962C-C0A352328531*.

[24] Yahoo!, Comment to the Department Privacy Green Paper, January 28, 2011, available at *http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=F6A50C0B–00CC-44A6-B475-FE218170CA02*.

[25] World Wide Web Consortium, Comment to the Department Privacy Green Paper, January 28, 2011, available at *http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/ResponseW3C.pdf*.

[26] *See, e.g.,* Professors Ira Rubinstein and Dennis Hirsch, Comment to the Department Privacy Green Paper, January 28, 2011, available at *http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=D120453B-FB2B-4034-962C-C0A352328531*; Intel, Comment to Depart-

Continued

The Green Paper suggested that comprehensive FIPPs can serve as a basis for stronger consumer trust while also providing the flexibility necessary to define more detailed rules that are appropriate for the relationships and personal data exchanges that arise in a specific commercial context. The FIPPs that the Green Paper presented for discussion were transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing. We received many thoughtful comments on how each of these principles might apply to the commercial context, and we are continuing to assess whether these principles provide the right framework for online consumer data privacy. The Administration looks forward to working further with Congress and stakeholders to define these baseline protections.

B. Implementing Enforceable Codes of Conduct Developed Through Multi-Stakeholder Processes

To encourage specific but adaptable rules for businesses and consumers in the implementation of baseline privacy principles, the Administration recommends a framework that can promptly address specific privacy issues as they emerge. In this framework, stakeholders from the commercial, consumer advocacy and academic sectors, as well as the FTC and other government agencies would come together to develop enforceable best practices or codes of conduct based on the principles in baseline legislation. This process would allow stakeholders to develop codes of conduct that address privacy issues in emerging technologies and business practices, without the need for additional legislation. In this framework, the FTC could have the authority to provide appropriate incentives, such as a safe harbor, for business to develop and adopt codes of conduct. Compliance with an approved code of conduct might be deemed compliance with the statutory FIPPs. Of those stakeholders that supported legislation, most one telecommunication company's conclusions that "[a]s the Green Paper observes, such a safe harbor provision will reinforce the industry's incentives to develop self-governance practices that address emerging issues, and to follow such practices."[27] In addition, legislation should ensure that stakeholders have appropriate incentives to revise enforceable codes of conduct as changes in technology, market conditions, and consumer expectations warrant.

This recommendation reflects the Department's view that government must support policy development processes that are nimble enough to respond quickly to consumer data privacy issues as they emerge and that incorporate the perspectives of all stakeholders. Industry, consumer groups, and civil society, as well as the government, all have vital roles to play in putting baseline privacy protections into practice in the United States. A leading IT company captured this multi-stakeholder perspective well, commenting that "no single entity can achieve the goal of building trust . . . as it is clearly a shared responsibility. There is a role for governments, industry, and Non-Governmental Organizations/advocacy groups (NGO's) working together to form a 'triangle of trust.'"[28] A multi-stakeholder strategy for implementation ensures that government establishes the base of this trust triangle. Such a strategy will be critical to ensure that we end up with a framework that is rational, that provides businesses with better information about what consumers expect (and vice versa), but that is also dynamic. Below, I explain in greater detail the leading role that the Department of Commerce could play in putting this multi-stakeholder model into practice.

C. Strengthening the FTC's Authority

The independent expertise of the FTC is another key element of this framework. In addition to its leadership in developing consumer data privacy policy, the FTC plays a vital role as the Nation's independent consumer privacy enforcement authority. Granting the FTC explicit authority to enforce baseline privacy principles would strengthen its role in consumer data privacy policy and enforcement, resulting in better protection for consumers and evolving standards that can adapt to a rapidly evolving online marketplace.

---

ment Privacy Green Paper, January 28, 2011, available at *http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/Intel%20Corp%20Dept%20Commerce%20green%20paper%20comment.pdf* ("Intel supports Federal legislation based on the Fair Information Practices (FIPs) as described in the 1980 Organization for Economic Co-Operation and Development (OECD) Privacy Guidelines.")

[27] Verizon, Comment to the Department Privacy Green Paper, January 28, 2011, available at *http://www.ntia.doc.gov/comments/101214614–0614–01/comment.cfm?e=6BFB924F-75DD-4472-94F3-F76DB8EE0376*.

[28] Intel, Comment to Department Privacy Green Paper, January 28, 2011, available at *http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/Intel%20Corp%20Dept%20Commerce%20green%20paper%20comment.pdf*.

D. Establishing Limiting Principles on Consumer Data Privacy Legislation

As the Committee considers these recommendations, we would also like to provide our thoughts on limitations that Congress should observe in crafting consumer data that strengthens consumer privacy protections and encourages continuing innovation. Legislation should not add duplicative or overly burdensome regulatory requirements to businesses that are already adhering to the principles in baseline consumer data privacy legislation. Legislation should be technology-neutral, so that it allows firms flexibility in deciding how to comply with its requirements and encourages business models that are consistent with baseline principles but use personal data in ways that we have not yet contemplated. And, domestic privacy legislation should provide a basis for greater transnational cooperation on consumer privacy enforcement issues, as well as more streamlined cross-border data flows and reduced compliance burdens for U.S. businesses facing numerous foreign privacy laws.

IV. The Department's and NTIA's Next Steps on Internet Privacy Policy

With or without legislation, the Department and NTIA will continue to make consumer data privacy on the Internet a top priority. We will convene Internet stakeholders to discuss how best to encourage the development of privacy codes of conduct. And, the Department will support the Administration's efforts to encourage global interoperability by stepping up our engagement in international policymaking bodies. Finally, we will continue to work with Congress and all stakeholders to develop consensus on reforms to our consumer data privacy policy framework.

A. Convening Voluntary Efforts to Define Baseline Privacy Protections

The Department of Commerce can play a leading role in bringing stakeholders together rapidly to develop enforceable codes of conduct, in order to provide greater certainty for businesses and necessary protections for consumers. The Green Paper notes that the Department—and particularly NTIA—has the necessary expertise and can work with others in government to convene companies, consumer groups, academics, and Federal and State government agencies. It will be important to bring NTIA's experience to bear in these activities, since NTIA can work with other agencies and provide a center of consumer data privacy policy expertise. The Department received significant stakeholder support for the recommendation that it play a central role in convening stakeholders. A broad array of organizations, including consumer groups, companies, and industry groups announced their support for the Department to help coordinate outreach to stakeholders to work together on enforceable codes of conduct.[29]

Indeed, the Department is pleased to be part of an Administration effort in which this approach to protecting consumer data privacy may be immediately useful: The National Strategy for Trusted Identities in Cyberspace (NSTIC).[30] The NSTIC, which is a separate Administration initiative being developed in close consultation with the private sector, and is not part of the legislative proposal discussed in this testimony, envisions enhancing online privacy and security through services that provide credentials that improve upon the username and password schemes that are common online. The NSTIC proposes a system that would provide individuals the option of obtaining a strong credential to use in sensitive online transactions. The NSTIC calls for the participants in this digital identity marketplace to implement privacy protections that are based on the FIPPs. Developing enforceable codes of conduct through multi-stakeholder processes is one way that the Department can work with the private sector to implement these protections.

We thank you, Chairman Rockefeller, for supporting the announcement that the Department of Commerce will host the National Program Office to coordinate the Federal activities to implement NSTIC. With the leadership of the private sector, the Department is ready and willing to support the implementation of NSTIC by leveraging the tremendous resources of NTIA and the National Institute of Standards and Technology.

B. Encouraging Global Interoperability

Consistent with the general goal of decreasing regulatory barriers to trade and commerce, the Department will work with our allies and trading partners to reduce barriers to cross-border data flow by increasing the global interoperability of privacy frameworks. While the privacy laws across the globe have substantive differences,

---

[29] *See, e.g.*, Comments of Center for Democracy and Technology; Comments of Consumers Union; Comments of Microsoft; Comments of Walmart; Comments of Intel; Comments of Google; Comments of Facebook; Comments of Interactive Advertising Bureau; and Comments of Yahoo!

[30] For further information, see NIST, About NSTIC, *http://www.nist.gov/nstic/* (last visited Mar. 14, 2011).

these laws are frequently based on similar fundamental values. The Department will work with our allies to find practical means of bridging differences, especially those that are often more a matter of form than substance.

The Department will work with other agencies to ensure that global privacy interoperability builds on accountability, mutual recognition and reciprocity, and enforcement cooperation principles pioneered in the Organisation for Economic Cooperation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC). Agreements with other privacy authorities around the world (coordinated by key actors in the Federal Government) could reduce significant business global compliance costs.

C. Developing Further Administration Views on U.S. Internet Policy

Finally, we are working to ensure that our work on consumer data privacy policy complements and informs other Internet policy development efforts that are underway in the Department and throughout the Administration. An invaluable mechanism for making this happen is the Privacy and Internet Policy Subcommittee of the National Science and Technology Council. The Subcommittee, which the White House announced last fall, is chaired by Commerce Department General Counsel Cameron Kerry and Justice Department's Assistant Attorney General Christopher Schroeder. The Subcommittee provides a forum for Federal agencies and key White House offices to coordinate and exchange ideas on how to promote a broad, visible, forward-looking commitment to a consistent set of Internet policy principles. These core principles—all of which apply to the consumer data privacy context—include facilitating transparency, promoting cooperation, strengthening multi-stakeholder governance models, and building trust in online environments.

The Subcommittee has already provided the substantive policy discussions that led to the legislative reform recommendations that I am presenting today. The Department of Commerce looks forward to continuing to work with this Committee.

V. Conclusion

In the end, the Obama Administration's goal is to advance the domestic and global dialogues in ways that will protect consumers and innovation, and to provide leadership on information privacy policy, regulation, and legislation.

Working together with Congress, the FTC, the Executive Office of the President, and other stakeholders, I am confident in our ability to provide consumers with meaningful privacy protections in the Internet economy, backed by effective enforcement, that can adapt to changes in technology, market conditions, and consumer expectations. Establishing and maintaining this dynamic consumer data privacy framework is not a one-shot game; it will require the ongoing engagement of all stakeholders. The Department and the Administration are firmly committed to that engagement. The legislative approach that I have outlined today would lend extremely valuable support to the dynamic framework that we envision. I welcome any questions you have for me. Thank you.

Senator PRYOR. Thank you.

Chairman Leibowitz, let me start with you if I may. And that is in your opening statement you mention this new icon that online advertisers are using. My understanding is that just came online just, you know, last several weeks at some point. Are you encouraged by what you see or is it too early to know if that's going to work?

Mr. LEIBOWITZ. Well I would say we are encouraged by what we are seeing. I would say the industry has been working in good faith on this icon notion probably for the last 2 years. I think you'll have someone testifying on the next panel about that.

I would say that the pace of moving forward has become far more rapid since the summer hearings this Committee held and the House Energy and Commerce Committee held in the fall and since we released our report in December. So it is promising from our perspective. The majority of Commissioners would like to see a Do Not Track mechanism that includes a prohibition on tracking, not just sending ads back to consumers.

But there are important developments really just in the last few days, including a number of members of that Digital Advertising Alliance who would like to see restrictions on tracking except for fraud purposes. So, yes.

Senator PRYOR. Thank you.

Mr. Strickling, I think I saw yesterday, maybe last night, a story that the White House is talking about a privacy bill of rights or—do you anticipate that they'll come forward with a proposal, with a bill or is this more just general concepts that, you know, we can expect to see from the White House?

Mr. STRICKLING. Yes, sir. The "Green Paper" was put out in December. And we are currently working to develop a more complete and what we hope will be an Administration statement of policy later this spring. What I testified to this morning is that the Administration is now at the point of recommending that this be dealt with in legislation.

We will continue to flesh out the particulars as we complete our overall policy paper. But we're prepared to start working with this Committee and other Members of Congress on those specifics now.

Senator PRYOR. Thank you.

Mr. Leibowitz, I have some questions for you about Do Not Track, but I think what I'd like to do is go to Senator Isakson since the vote just started and allow Senator Isakson to ask and then Senator Kerry.

Go ahead.

Senator ISAKSON. Thank you, Mr. Chairman.

Mr. Leibowitz, in your—on page two of your prepared testimony you have the number of cases you brought over the last 15 years in various categories, spam, fair credit reporting act, etcetera, children's protection. Is that volume by category proportionate to the number of complaints that you get or is it just?

Mr. LEIBOWITZ. Well, we keep a complaint database, Consumer Sentinel, and that's one way and a very important way in which we develop cases. There are other ways as well. It's not a perfect symmetry, but we like to think it's in proportion to the need to bring cases. As you know we're a very small agency. So we try to leverage our limited resources.

But we think we try to go where the harm is or is going to be. And so we think it's reflective of that. But let me—I'll get you some consumer complaints.

[The Federal Trade Commission submitted to the Committee, after this hearing, the Federal Trade Commission *Consumer Sentinel Network Data Book,* January–December 2010, published March 2011. It is available at *http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf*. The executive summary follows.]

Executive Summary
Consumer Sentinel Network Data Book

January–December 2010

- The Consumer Sentinel Network (CSN) contains over 6.1 million complaints dating from calendar year 2006 through calendar year 2010. There are over 7.8 million do-not-call complaints from this same time period.
- The CSN received over 1.3 million complaints during calendar year 2010: 54 percent fraud complaints; 19 percent identity theft complaints; and 27 percent other types of complaints.

- Identity theft was the number one complaint category in the CSN for calendar year 2010 with 19 percent of the overall complaints, followed by Debt Collection (11 percent); Internet Services (5 percent); Prizes, Sweepstakes and Lotteries (5 percent); Shop-at-Home and Catalog Sales (4 percent); Impostor Scams (4 percent); Internet Auction (4 percent); Foreign Money Offers and Counterfeit Check Scams (3 percent); Telephone and Mobile Services (3 percent); and Credit Cards (2 percent). The complete ranking of all thirty complaint categories is listed on page six of this report.

Fraud

- A total of 725,087 CSN 2010 complaints were fraud-related. Consumers reported paying over $1.7 billion in those fraud complaints; the median amount paid was $594. Eighty-six percent of the consumers who reported a fraud-related complaint also reported an amount paid.
- Sixty percent of all fraud-related complaints reported the method of initial contact. Of those complaints, 45 percent said e-mail, while another 11 percent said an Internet website. Only 10 percent of those consumers reported mail as the initial point of contact.
- Colorado is the state with the highest per capita rate of reported fraud and other types of complaints, followed by Maryland and Nevada.

Identity Theft

- Government documents/benefits fraud (19 percent) was the most common form of reported identity theft, followed by credit card fraud (15 percent), phone or utilities fraud (14 percent), and employment fraud (11 percent). Other significant categories of identity theft reported by victims were bank fraud (10 percent) and loan fraud (4 percent).
- Government documents/benefits fraud increased 4 percentage points since calendar year 2008; identity theft-related credit card fraud, on the other hand, declined 5 percentage points since calendar year 2008.
- Forty-two percent of identity theft complainants reported whether they contacted law enforcement. Of those victims, 72 percent notified a police department. Sixty-two percent indicated a report was taken.
- Florida is the state with the highest per capita rate of reported identity theft complaints, followed by Arizona and California.

Mr. LEIBOWITZ. As you know being a member of this Committee, sometimes you'll see something you'll read about or a Commissioner will and that will go into the investigative process. So there are all different ways we bring cases.

Senator ISAKSON. That is exactly where I was going with my follow up question. In most federal enforcement agencies the cases they pursue are in response to complaints from citizens. But you also—do you also monitor news media and reports and then follow up based on whether or not it appears to fall under your responsibility?

Mr. LEIBOWITZ. Sure, we do. And in fact we brought a very important antitrust case because Senator Klobuchar raised it at a hearing maybe a year ago. This was on a merger involving a drug used for children with heart defects. And so it comes from a lot of places.

You know, we're a very bipartisan agency. All the Commissioners have ideas of about what we should be doing and it all is channeled into our investigative and our enforcement efforts.

Senator ISAKSON. Where does the volume of penalties, I mean, $60 million in civil penalties, $21 million in civil penalties and five. It looks like to me it's about $80 million in civil penalties you collect over the year. Where does that money go? Back into the agency or back to the general treasury?

Mr. LEIBOWITZ. It goes back to Treasury. And then more often we will try to get redress for consumers. One of the things that we

try to obtain in the financial reform legislation was the ability to get civil penalties for violations of our standard unfair and deceptive acts or practices authority. And it didn't make it into the final legislation.

It was something that Caspar Weinberger actually supported when he was the FTC Chair back in the early 1970s. And we hope to come back and revisit that going forward. But as a result, we have limited fining authority. It usually goes back to Treasury.

Senator ISAKSON. I'm assuming based on what I've heard in the testimony that probably the most effective way to protect the consumer would be give them a mechanism to protect themselves. You talked about the icon where you can just elect——

Mr. LEIBOWITZ. Yes.

Senator ISAKSON.—whether or not your information can be shared or not. Do we know if technologically that—I think technologically anything can be done now, but is that doable?

Mr. LEIBOWITZ. Yes, that is doable. And the only question is about exactly which way to do it.

Senator ISAKSON. Thank you, Mr. Chairman.

Senator PRYOR. Thank you.

Senator Kerry?

Senator KERRY. Thank you, Mr. Chairman.

Chairman Leibowitz, I want to try—a lot has been discussed about the Do Not Track proposal. And I want to try to hone in on it a little bit. Is it your judgment that if a company comes up with a pretty strict policy which has broad privacy protections and adequate opt in, et cetera, et cetera, and opt-out or out, do you think then that the Do Not Track is still necessary?

Mr. LEIBOWITZ. At this point I think we do, because if individual companies have individual practices that may support a baseline consumer or commercial bill of rights here, I think that is a great idea it may not mean that every company has that. And I think what we're trying to do, like you, is develop a baseline for privacy protection for consumers.

So from my perspective a Do Not Track mechanism that's easy to implement, going back to Senator Isakson's point, could be an important choice mechanism for consumers and an important way to protect privacy for consumers who want to limit tracking.

Senator KERRY. So in terms of the potential harm or protection depending on which way you look at it, that you're trying to provide the consumer if you had a Do Not Track it doesn't mean that they're going to get no advertising like a Do Not Call means you're not going to get any calls. It simply means you're not going to get customized advertising. But you'll still get bombarded by advertising.

Mr. LEIBOWITZ. You will still get advertising. It may not be targeted. But again, from our perspective——

Senator KERRY. So the analogy to Do Not Call is not an appropriate one. Would you——

Mr. LEIBOWITZ. Yes, it's very different than Do Not Call.

Senator KERRY. OK.

Mr. LEIBOWITZ. It's very different from Do Not Call. It's also not government run as we run the Do Not Call list.

Senator KERRY. OK.

So then is there an assumption therefore that if you had a standard and you had a code and you had a strong privacy offering that the tracking is per se bad?

Mr. LEIBOWITZ. No, we don't think tracking is per se bad at all. We think most consumers won't mind being tracked. They get more personalized advertising.

We just think consumers ought to have the ability to opt out of that kind of tracking. I mean, the analogy we sometimes use is if you're walking around a mall, someone shouldn't be sort of tracking—following you around even if they don't know who you are and sending e-mails off to the stores in front of you saying well, that's Jon Leibowitz. He's interested in buying a Madras jacket in his usual green and red colors.

You know, you should have the right not to be followed around if you don't want to be followed around.

Senator KERRY. So if a firm has a very strong policy, a privacy policy and then you have another firm that doesn't have a very strong kind of policy.

Mr. LEIBOWITZ. Right.

Senator KERRY. You're going to treat them both the same in the context of the Do Not Track.

Mr. LEIBOWITZ. Well.

Senator KERRY. There's no virtue to having the stronger policy and therefore allowing the tracking to take place in the context of that stronger policy.

Mr. LEIBOWITZ. Well, stronger policy outside of Do Not Track may have many virtues, right? It will include privacy by design. It will include readable privacy notices. They'll be transparency. They'll be more choice.

But my sense is that a lot of the most responsible companies support a Do Not Track notion for third party cookies. And so I think there's an enormous benefit to having a baseline FIPPs privacy protection and then negotiated industry codes. We're working with the Commerce Department on that.

But we also think there's a value in having the ability to opt-out of targeted advertising or maybe targeted advertising for just sensitive information like medical searches or financial information.

Senator KERRY. With respect to the *Wall Street Journal* series on the issue of what they know. I assume you followed that?

What did you draw from that? What came out of that in your judgment?

Mr. LEIBOWITZ. So let me say a few general things and some specific things.

So generally, what came out of that—and it was a series of stories, as you know, last summer, and then many follow-ups.

One is that some companies have very good privacy practices, but many of them do not. And it results in an enormous amount of information being collected about consumers that's invisible to consumers and not on the sites that they're on, but by cookies and software embedded in consumer's computers. And so it really was a motivation for us to step up our enforcement efforts and to write our privacy report.

And then more specifically, we're having a debate about whether to propose a Do Not Track mechanism. And one of the issues we

had internally in the Commission was: is it technologically feasible? And of course, one of the stories, as you know, was about Microsoft having developed this and the balancing act they did between their privacy advocates and engineers on the one hand and their marketers. And how they resolved it was they sort of split the difference.

And so we knew then that Do Not Track was technologically feasible. And Microsoft to its credit has stepped up and endorsed the concept since our report.

Senator KERRY. Thank you.

[Laughter.]

STATEMENT OF HON. CLAIRE MCCASKILL, U.S. SENATOR FROM MISSOURI

Senator MCCASKILL. Thank you, Mr. Chairman.

I—you know when you talk about privacy it's in the same category as motherhood and apple pie in this country. And I think we've got a real problem here because what most Americans don't understand and frankly, what maybe, unfortunately, two Members of Congress don't understand is we have monetized the Internet with behavior marketing. It is an amazing amount of free information that is immediately accessible because of behaviorally marketing. So I guess, you know, it equals money.

And so I guess my first question is have—does anybody know? Do either of you know what the cost is going to be in terms of the economic vibrancy of the Internet for some of the things that are being considered? And isn't it fair to envision that a Do Not Track in fairness since behavioral marketing is money, isn't it fair to think that some of these companies are going to charge for that?

Mr. LEIBOWITZ. For opting out of tracking?

Senator MCCASKILL. Yes.

Mr. LEIBOWITZ. We have not seen that yet even in the——

Senator MCCASKILL. But we haven't passed any laws yet.

Mr. LEIBOWITZ. No, but to their credit, there is a major group of companies, called the Digital Advertising Alliance, that's in the process of offering some sort of free opt-out. Now we think it should go a little further. But no one has talked about monetizing that.

And I think that's a good thing. And I think it's a recognition also that businesses understand that if you put some limits on tracking or you have some privacy protections as the Commerce Department envisions—and I'm supportive of that though you don't necessarily need to be—the sky won't fall down on Internet commerce. It's going to continue. And indeed if consumers have more trust in the Internet, they're going to do more business on the Internet too.

Senator MCCASKILL. Do you think that there is envisioned where we draw the line? For example, we would never dream of telling Slim Fast they couldn't advertise on Oprah, right? Behavioral marketing. They know that there are mostly women that are watching that show. And they know that most of their product is consumed by women. And so they are behaviorally marketing to that segment.

How will we draw the line between what kind of behavioral marketing is fair and what kind of behavioral marketing invades privacy?

Mr. LEIBOWITZ. Well, I think you've raised a really important point. And I don't know if you were here when Senator Isakson was speaking. He used to run a company. They advertised. And he pointed out that there's a difference between advertising on the Internet where you can figure out things about people, not from classic PI, personal information, but from the aggregated enormous amounts of information.

And so it's different than advertising on Oprah or advertising on TV. And that seems to me, that's a point where we want to ensure privacy protections for consumers. And I think that the Department—I don't speak for the Department of Commerce, but I assume that you do.

Mr. STRICKLING. And I would just add to the comments the Chairman has made that in our discussions we find a very strong level of support among industry to create this baseline of protections. The baseline though, it's fair to call it a bill of rights. I mean what we have in mind is not unlike the Bill of Rights, a concise statement of the right that the consumer has, and then relying on industry, working with consumer groups, working with other experts in the field, to come up with these codes of conduct that provide more specificity.

We think, in that regard, we don't have to see the government drawing some of these very difficult lines and imposing them as regulation as long as we're providing adequate oversight of this process by which industry, working with all stakeholders, develops appropriate codes. We think we can get to a regime that will greatly improve privacy for consumers and still meet the needs of businesses who want to continue to see the growth of the Internet.

Mr. LEIBOWITZ. If I can just follow up briefly. And you're right. I don't think most American consumers understand where their information is going, how it's been monetized, how it's been traded. But in another sort of bedrock level, I think they get the issues of Internet privacy.

There was a poll by a group called Consumer Watchdog that found 80 percent of Americans wanted to see a Do Not Track option. I think Common Sense Media had a poll that you mentioned, talking about greater concern that parents had over their kids.

Senator MCCASKILL. Right.

Mr. LEIBOWITZ. About Internet privacy and safety. Gallup had a poll that also reflected this. So I think at some level Americans understand.

Senator MCCASKILL. I agree. And I don't mean to cut you off. But I don't want to miss this vote and while I'm going to try to come back—I just think we've got to be very careful about the unintended consequences.

We know the good guys are going to try to do this right. We know the bad guys, it's going to be very hard to regulate them in a way that makes sense. So what I don't want to do is handcuff the good guys because with all due respect, I mean, you know, if we think we're doing a really good job in consumer oversight of the commerce in this country right now. You know, I mean, don't get

me started on the ads I see on cable TV that I just need to get my government benefit and all of the things that are out there that are not being adequately policed.

So I just want to make sure that we don't kill the goose that laid the golden egg here under the rubric of the very laudable notion of privacy. I just think that we've got to go very carefully, make sure that we think about the unintended consequences and most importantly, think about the bad guys that aren't going to pay any attention to your code of conduct.

And consumers are going to continue to not have confidence in the Internet as long as those bad guys are out there. So I just—I think we've got to be very careful and not go too fast, too far, without thinking about what may be down the line.

Mr. STRICKLING. If I could respond quickly to that. I think the proposal that we've made answers your concern. It would have legislation that would create a baseline of these fair information practice principles. And those are some of the things that the Chairman mentioned earlier, things like transparency and disclosure, what level of consent.

I'm confident that if, in doing so, the Congress also gives the FTC the enforcement authority to enforce that they're going to be able to go after the bad guys based on that baseline. But what the baseline allows though is the flexibility to the good guys, as you call them, to craft the more specific protections that they need to have to allow them to run their businesses.

Senator MCCASKILL. I agree. I will just tell you that I have a feeling that, Mr. Leibowitz, that your budget is not going to grow enormously over the next decade. And you've got plenty of work to do over there.

And frankly a lot of work that needs to be done that you can't do now. And if we're going to add to your work load and at the same time do something that is going to minimize the amazing things we've done on the Internet, I just think we've got to make sure America buys into that agreement.

Mr. LEIBOWITZ. Yes, I agree with that.

Senator PRYOR. Let me interrupt here just for a second because this vote is about to close. And Senator, we need to run over there and vote. So what I'll do is recess this for just a few moments. Let us go do these two votes. And then we'll reconvene in just a few minutes.

Thank you.

[Recess.]

Senator PRYOR. I'll reconvene the hearing. I want to thank everyone for being patient with us and we had those two votes. And my understanding is we have a few Senators on the way back over. But I know that Senator Klobuchar wanted to ask questions of this first panel.

So Senator Klobuchar?

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Well, thank you very much, Chairman. Thank you for holding this hearing. And thank you to our two witnesses and as well as the second panel.

But thank you, Chairman Leibowitz and Administrator Strickling. It is great to be here with you on an important topic. And I wanted to focus a little bit on websites with teens and children maybe because I walked into my daughter's room last night and she was webcasting with her friend. And luckily they were working on their homework. And the interview she's doing with Senator Murkowski which will be I'm sure, devastating to Senator Murkowski.

But I wanted to ask you a few questions on this. A recent *Wall Street Journal* article examined 50 websites popular with teens and children to see what tracking tools they installed on a test computer. As a group the sites used over 4,000 cookies, beacons and other pieces of tracking technology. That it actually 30 percent more than were found in a similar analysis of adult websites which is rather disturbing I think that there were more of these being used on children's websites.

Can you describe your agency's experiences dealing with tracking of children and teens online? And what do you think needs to be done here?

Mr. LEIBOWITZ. Well, I think there's no doubt that there's an extraordinary amount of monetizing of teen information. As you know, from your daughter, who I believe is a very responsible 15 year old. And I know from my children that they spend a lot of time online.

And so one of the recommendations in our report discusses the need for a kind of enhanced consent for children. We're taking comments on that.

But of course one of the other issues with teens is often, they act impulsively. They put things online that they never expect will remain there. When a privacy policy of a social network switches from something that protects privacy to something that has less privacy protections sometimes kids don't realize or teens don't realize that a lot of information that they thought was private will be put online.

So it's a very important issue for us. And we are studying it.

Senator KLOBUCHAR. OK. Anything you would like to add, Administrator?

Mr. STRICKLING. No.

Senator KLOBUCHAR. As we talk about privacy I wondered Chairman Leibowitz, if the FTC has looked into the issue of privacy notifications on smartphones. As you can imagine those are smaller letters and harder to read, yet they access the same type of information and also have the same kind of privacy concerns as other larger computer screens.

Mr. LEIBOWITZ. Well, I believe in our report we looked at mobile phones. We've done a number of hearings on mobile issues because, you're right. In terms of privacy policies they're much harder to read. In terms of applications for children, of course, you wrote to us about a particular application. And we were glad to see that the alleged malefactors have improved their app standards.

These are all very, very important issues and particularly in the mobile space. We're going to try to see how we can encourage more consumer choice and more transparency. So few people and certainly so few children understand the terms of service. You need

to have easy-to-understand terms of service for children or parents who have a lot of information that's taken from kids and that's placed online—information that perhaps parents wouldn't want their kids to share, and kids or teens may not want to share themselves.

Senator KLOBUCHAR. Administrator?

Mr. STRICKLING. I think what I'd like to say in response to both of the examples you've given is the fact that it's impossible for us to predict today what the privacy issue is going to be 6 months or 12 months from now. And that's why the framework that the Administration is proposing for legislation to use codes of conduct that will be prepared by this multi-stakeholder group of industry is very important because it gives you the speed and the flexibility to respond to these types of issues when they arise. If we're chasing after these issues and trying to write regulations in a more formal way that perhaps take a year to write, we can't possibly stay up on the issues that arise.

Senator KLOBUCHAR. So the argument—yes.

Mr. STRICKLING. And so overall I think this again is further demonstration of the need to have an industry-based, actually a full multi-stakeholder process to work on these codes of conduct and to deal with these issues when they arise. And indeed that in effect is what, you know, Chairman Leibowitz and the FTC are doing on an individual issue basis, is assembling the parties to get them to talk about these issues and nudging them in the right direction. And I think that's the appropriate model we want going forward.

Senator KLOBUCHAR. I think that's the name of Cass Sunstein's book—*Nudge*.

Mr. LEIBOWITZ. *Nudge*.

Senator KLOBUCHAR. So that's all——

Mr. LEIBOWITZ. Not noodge, not noodge. *Nudge*.

Senator KLOBUCHAR. It looks like you want to add something. But I just want—Chairman Leibowitz, but I wanted to follow up on that. It would seem to me just one of the problems is, as we all know under the best circumstance it takes so long for us to get these laws done. So clearly if we can get these voluntary codes of conduct that would respect the development of the technology and also not interfere with the development of the technology would be key as long as we actually get these voluntary codes of conduct.

Mr. Chairman?

Mr. LEIBOWITZ. Yes. And I wanted to check to our Bureau Director to make sure I could say this. We have multiple investigations going on of inadequate notice on mobile and to kids. And apparently in one of the investigations we're doing, the privacy notice on mobile was 151 or 152 clicks or screens away.

[Laughter.]

Mr. LEIBOWITZ. So I think the reasonable consumer will not——

Senator KLOBUCHAR. You're kidding. So you mean if they wanted to find the privacy notice they had to click 152 times to get to the window that——

Mr. LEIBOWITZ. 106 or 107 because the first time you may not have to click. But yes.

Senator KLOBUCHAR. OK. Well I get it. Well, thank you for clarifying that for the record.

[Laughter.]

Senator KLOBUCHAR. Alright. Thank you to both of you. And I appreciate the way that this is moving. I think it's the right way. Thank you.

Senator PRYOR. Thank you both for joining us today. There are several Senators who either had to come and go or expressed an interest in being here. And probably we'll leave the record open for a couple weeks to allow Senators to ask questions. We'd appreciate a quick response.

But thank you all for being here today. And I'll go ahead and introduce our second panel.

Mr. LEIBOWITZ. Thank you, Mr. Chairman.

Senator PRYOR. Oh, thank you very much. Thank you.

We'll go ahead and bring up our second panel. And the staff as always will do a quick switch, switcheroo here. And bring the second panel forward with their name tags.

And as they are doing this what I'll do is I'll go ahead and introduce the members of the second panel. And then once they get situated I'll just call on them as we go down the row.

First would be Erich Andersen, Vice President and Deputy General Counsel of Microsoft.

Second will be John Montgomery, Chief Operating Officer of GroupM Interaction.

Third will be Ashkan Soltani, Researcher and Consultant.

Fourth will be Barbara Lawler, Chief Privacy Officer for Intuit.

And the fifth, last but certainly not least, will be Chris Calabrese, Legislative Counsel with the American Civil Liberties Union.

So as we're getting set up here. And I see water is getting poured and charts are getting established. Just one moment we will go ahead and call on Mr. Andersen whenever we are ready. So, Mr. Andersen, go ahead.

STATEMENT OF ERICH D. ANDERSEN, DEPUTY GENERAL COUNSEL, MICROSOFT CORPORATION

Mr. ANDERSEN. OK. Thank you, Mr. Chairman.

Mr. Chairman and honorable members of the Committee, my name is Erich Andersen and I'm the Deputy General Counsel of Microsoft's Windows Division. Thank you for inviting me to testify today about the state of online privacy. We applaud the leadership that the Committee has shown on this issue.

I also want to endorse Assistant Secretary Strickling's call for federal privacy legislation.

Legislation can be an important component of a multipronged approach to privacy but also includes technology tools, industry initiatives and consumer education. At Microsoft consumer trust is vital to our business. And privacy is a critical component to earning and maintaining that trust. In all our service offerings we strive to be transparent about our privacy practices, offer meaningful privacy choices and protect the security of the data that we store.

In my role for the Windows Division, I've worked with our software team to develop privacy enhancing features for Windows and Internet Explorer. We have groups working on similar efforts throughout Microsoft including for our Bing search engine, Xbox

gaming platform and our advertising services. The different ways that we engage with consumers give us a unique perspective on the privacy discussion. In light of our experience we believe that a combination of technology tools, industry initiatives, consumer education and legislation is needed to protect privacy and promote innovation.

Let me briefly explain the importance of technology. At Microsoft we have implemented privacy by design. We engineer privacy into our products and services from the outset. And we consider privacy throughout the product life cycle.

One example of where we put this principle into practice is the privacy features we've developed for Internet Explorer. The most recent version of Internet Explorer, IE 9 was released this week. And it offers a ground breaking new tool called tracking protection.

This Do Not Track feature allows consumers to decide which sites can receive their data and blocks content from sites that they view as engaged in tracking providing consumers with greater control over their online experiences. We're very proud that Internet Explorer was the first major browser to respond to the FTC's recent call for a Do Not Track mechanism. We look forward to working with all stakeholders to implement Do Not Track tools in a meaningful way for consumers and businesses alike.

Industry initiatives can be effective in complementing technology tools. For instance, we've long partnered with the Network Advertising Initiative to develop principles governing online behavioral advertising. We're continuing to collaborate with members of the Digital Advertising Alliance and others in the advertising industry to implement guidelines and best practices to help ensure that consumers understand and can easily opt-out of behavioral advertising.

The third element of a comprehensive approach to privacy is consumer education. We agree with the FTC and the Commerce Department that consumers need a better understanding of data practices. That's why we provide consumers with clear information about our own practices and offer choices about what data will be collected and how it will be used. We've also partnered with consumer advocates and government agencies to develop educational materials on consumer privacy and data security.

The last critical element is federal privacy legislation. Legislation is needed because the current sectoral approach to privacy regulation is confusing to consumers and it's costly for businesses. We believe that legislation should establish a common set of privacy and security requirements that are not specific to any one technology, industry or business model.

For particular industries or business models industry initiatives should co-exist with or should build on top of the baseline obligations of the law. Online advertising is a perfect example. Baseline federal privacy requirements around user notice, control and security can complement industry initiatives and innovative technology tools.

In conclusion, Microsoft is committed to working with you to protect consumer privacy in a way that complements technical and industry based measures and promotes continued innovation. Thank

you for giving us this opportunity to testify today. I look forward to answering any questions you may have.

[The prepared statement of Mr. Andersen follows:]

PREPARED STATEMENT OF ERICH ANDERSEN, DEPUTY GENERAL COUNSEL, MICROSOFT CORPORATION

Chairman Rockefeller, Ranking Member Hutchison, and honorable Members of the Committee, my name is Erich Andersen, and I am Deputy General Counsel of Microsoft's Windows Division. Thank you for the opportunity to share Microsoft's views on an issue that needs the attention of Congress and the work of this Committee: the adoption of meaningful privacy legislation that protects individuals' privacy while complementing technological and industry-based measures and promoting continued innovation. We appreciate the leadership that the Committee has shown on this issue, and we are committed to working collaboratively with you, the Federal Trade Commission, the Department of Commerce, consumer groups, and other stakeholders to achieve this important balance.

In my role for the Windows Division, I have worked with our software team to develop privacy-enhancing features and tools for Windows and Internet Explorer. We have teams working on similar efforts throughout Microsoft—for instance, in the Bing search team, the online advertising division, the Xbox group, and our cloud computing group. Our goal across Microsoft is to build trust with consumers by giving them the tools they want to make them productive and enrich their computing experience. Privacy is a critical component of earning and maintaining that trust. In all of our service offerings, we strive to be transparent about our privacy practices, offer meaningful privacy choices, and protect the security of the data we store.

The multiple contexts in which we engage with consumers give us a unique perspective on the privacy discussion. For example, as a website operator, an ad network, and a browser manufacturer, we have a deep understanding of the roles that different participants in the digital ecosystem play in safeguarding consumer privacy. Also, based on our longstanding involvement in the privacy debate, we recognize that the combined efforts of industry and government are required to effectively balance the need to protect consumers' privacy interests and promote innovation. In light of our experience, we recommend a multi-pronged approach that includes legislation, industry self-regulation, technology tools, and consumer education.

Today, I will explain why we believe that each of these four elements is important for protecting consumer privacy, and I will highlight steps that Microsoft has taken in each area. But first I would like to start with a discussion of how technology has reshaped consumers' engagement online and their privacy expectations.

I. Protecting Privacy While Enabling Innovation

The explosive growth of the Internet, cloud computing, the proliferation of computers and handheld mobile devices, and the expansion of e-commerce, e-government, e-health, and other web-based services have brought tremendous social and economic benefits. At the same time, however, technology has fundamentally redefined how, where, and by whom data is collected, used, and shared. The challenge that industry and government must address together is how to best protect consumers' privacy while enabling businesses to develop a wide range of innovative products and services.

Consider, for example, online advertising. Online advertising is the fuel that powers the Internet and drives the digital economy. Over $25 billion was spent on online advertising in 2010.[1] Millions of websites are able to offer their content and services for free because of the revenue they derive from advertising online. For small and medium-sized businesses in particular, online advertising has created new opportunities to inform consumers about their products and services. One study estimates that the advertising-supported Internet ecosystem is responsible for creating 3.1 million American jobs, and that the dollar value of these wages totals approximately $300 billion.[2] Consumers also benefit—not only because online advertising enables the free services and content they enjoy, but because the ads they see are more likely to be relevant. Simply put, the richness and vibrancy of the modern Internet experience is due in large part to the success of online advertising.

---

[1] Kristen Schweizer, *U.S. Web Advertising Exceeds Newspaper Print Ads in 2010, eMarketer Says,* BLOOMBERG (Dec. 20, 2010), *http://www.bloomberg.com/news/2010-12-20/u-s-web-ads-exceed-newspaper-print-ads-in-2010-emarketer-says.html*.

[2] Hamilton Consultants, Inc., *Economic Value of the Advertising-Supported Internet Ecosystem* 4 (June 20, 2009), *http://www.iab.net/media/file/Economic-Value-Report.pdf*.

The collection of data to serve ads on the Internet also has important privacy implications. When Justice Louis Brandeis famously defined privacy as "the right to be let alone" in 1890,[3] he could not have foreseen how technology would revolutionize our world. An individual planning a trip to Boston can now go online to compare airfares, book a hotel room, map out restaurant recommendations that are convenient to her itinerary, and poll her network of friends for suggestions about things to do during her trip. Every day, people generate billions of page views, transactions, downloads, and search queries—a mountain of data, across a myriad of different devices, that reveals valuable information about users' interests. As one of Microsoft's senior executives recently recognized, industry can and must do better in addressing the fact that consumers often do not understand the ways in which their data is bought, sold, bartered, exchanged, traded, and used.[4]

In the digital era, privacy is no longer about being "let alone." Privacy is about knowing what data is being collected and what is happening to it, having choices about how it is collected and used, and being confident that it is secure. These three principles—transparency, control, and security—underpin Microsoft's approach to privacy. They are also essential components of the thoughtful privacy frameworks recently advanced by the Federal Trade Commission (FTC) and the Department of Commerce.[5] We believe that the principles of transparency, control, and security should inform legislative, self-regulatory, technological, and educational initiatives to safeguard consumer privacy.

II. A Role for Congress and Comprehensive Privacy Legislation

As we focus on what can be improved, it is important to note that in the past year, significant progress has been made toward protecting individuals' privacy: technological solutions to empower consumers to control their personal information are now widely available, consumers are much more educated about the nature and scope of privacy risks, enforcement actions have been taken by the FTC, and legitimate industry practices are becoming better and more consistent. Federal legislation can be an effective *complement* to this strategy, providing an additional layer of protection for consumers and another tool for enforcement officials.

Historically, Congress has played an active role in protecting consumers online. Beginning in the late 1990s, Congress passed laws aimed at specific online harms and revised existing laws to account for the evolving ways in which technology was being used to collect, use, and share personal information. Examples include the Children's Online Privacy Protection Act of 1998, the privacy and security provisions for financial information in 1999's Gramm-Leach-Bliley Act, the CAN–SPAM Act of 2003, and the breach notification provisions for protected health information that were included in 2009's Health Information Technology for Economic and Clinical Health Act. Congress (and this Committee in particular) has also scrutinized important privacy-related issues such as online advertising, data security and breach notification, privacy in connection with broadband providers, spyware, and children's online safety.

Although the progress that has been made is notable and should not be overlooked, our view since 2005 has been that Congress should take the next step and enact comprehensive Federal privacy legislation. One of the key problems with the current sectoral approach to privacy regulations is that it makes compliance a complex and costly task for many organizations. According to one estimate, by 2009 there were over 300 Federal and state laws relating to privacy.[6] The sector-specific approach also creates confusion among consumers, and can result in gaps in the law for emerging sectors or business models.

---

[3] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193, 193 (1890).

[4] *See* Emily Steel, *Microsoft Executive Urges Online Ad Industry to Police Itself,* WALL ST. J. DIGITS BLOG (Feb. 28, 2011, 6:28 PM), *http://blogs.wsj.com/digits/2011/02/28/microsoft-executive-urges-online-ad-industry-to-police-itself/* (referencing comments by Rik van der Kooi, corporate vice president of Microsoft's Advertiser & Publisher Solutions group, at the annual leadership meeting of the Interactive Advertising Bureau).

[5] *See generally* Fed. Trade Comm'n, Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010) [hereinafter FTC Staff Report]; Internet Policy Task Force, Dep't of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 16, 2010) [hereinafter Commerce Report]. As we noted in comments filed with the FTC and the Commerce Department, we applaud the Commission's and Department's efforts to develop a robust privacy framework that will withstand rapid technological advances while fostering innovation.

[6] Lee Gomes, *The Hidden Cost of Privacy,* FORBES, June 8, 2009, available at *http://www.forbes.com/forbes/2009/0608/034-privacy-research-hidden-cost-of-privacy.html*.

What industry needs is Federal privacy legislation that sets forth baseline privacy protections for transparency, consumer control, and security that are not specific to any one technology, industry, or business model. Privacy protections that apply across sectors would provide consistent baseline protections for consumers, and simplify compliance for businesses that increasingly operate across those sectors. Baseline privacy protections would also promote accountability by ensuring that all businesses use, store, and share commercial data in responsible ways, while still encouraging companies to compete on the basis of more robust privacy practices. In addition, legislation would create legal certainty by preempting state laws that are inconsistent with Federal policy.

Microsoft is pleased to see that members in both chambers of Congress are taking up the issue of comprehensive privacy legislation in the current congressional session, and we also find it encouraging that some of these initiatives appear to have early bipartisan support. As these proposals advance through the legislative process, we note that any privacy legislation should be crafted with two goals in mind. First, the legislation must protect consumers' privacy and data security while enabling innovation and facilitating the productivity and cost-efficiency offered by new business models and computing paradigms. Second, the legislation should create privacy protections that can withstand the rapid pace of technological change so that consumer data is protected not only today, but also in the decades to come.

To achieve these two ends, any proposed legislation should be tested against certain fundamental criteria, among them:

- *Flexibility.* The legislation should permit businesses to adapt their policies and practices to match the contexts in which consumer data is used and shared and be sufficiently flexible to allow technological innovation to flourish.
- *Certainty.* The legislation should provide businesses with certainty about whether their privacy policies and practices comply with legal requirements.
- *Simplified data flows.* The legislation should seek to facilitate the interstate and international data flows that are necessary to enable more efficient, reliable, and secure delivery of services, including through harmonizing international privacy regimes and preempting a patchwork of state privacy laws.
- *Technology neutrality.* The legislation should avoid preferences for particular services, solutions, or mechanisms to provide notice, obtain choice, or protect consumer data.
- *Focus on substantive outcomes.* Instead of imposing prescriptive rules that may be of limited effect or that may burden businesses without yielding commensurate privacy benefits, the legislation should set privacy goals based on criteria established in current public policy, then permit businesses to adopt methods and practices to reach those goals in a manner that best serves their business models, technologies, and the demands of their customers.

We look forward to continuing to work with this Committee to craft legislation that meets these criteria.

III. A Role for Industry Self-Regulation and Best Practices

Legislation, while important, is only part of the solution. Legislation is an appropriate vehicle for setting baseline standards, but it must work in conjunction with industry self-regulation and best practices, technology solutions, and consumer education.

Industry self-regulation is a useful complement to legislation for two reasons. First, self-regulatory efforts can easily be tailored to the particular context in which data about individuals is collected and used. Consumers have different privacy expectations depending on whether they are interacting with retailers, application developers, social media platforms, search engines, Internet service providers, publishers, advertisers, ad networks, or data exchanges. Effective privacy protections should take into account consumers' reasonable expectations of privacy, and industry self-regulation offers a flexible tool for doing so. Second, self-regulatory efforts are generally well-positioned to keep pace with evolving technologies and business models. There is no question that technology, business models, and consumer adoption of online services will continue to change—and change rapidly. A decade ago, few consumers were publicly sharing their personal photographs and home videos, but today consumers regularly post these materials on social networking and online video websites without hesitation because they believe such services are valuable. In 2003 Facebook was just an idea in the mind of a Harvard undergraduate, but today there are companies whose entire business model is built around developing applications for Facebook and other social media platforms.

Given the complex and dynamic nature of the online ecosystem, crafting workable solutions requires engagement from multiple stakeholders. Microsoft has a history of working collaboratively with other companies to develop appropriate solutions that build on the principles of transparency, control, and security. For example, Microsoft is a strong supporter of the Self-Regulatory Program for Online Behavioral Advertising, which includes an educational website where consumers can learn about online advertising and choose not to have their information used for behavioral advertising. Additionally, data security is one of the focal points of the Program: participating organizations must agree to provide appropriate security for, and limit their retention of, data collected and used for behavioral advertising. In our multiple roles as a browser manufacturer, ad network, and website operator, we are coordinating with the Interactive Advertising Bureau and other participants in the Self-Regulatory Program to ensure that this important initiative is effective, enforceable, and broadly accepted. Consistent with our commitment to responsible industry leadership, we are also working at the World Wide Web Consortium, the standards-setting body for the Web, to develop an industry consensus about technical standards that can implemented across browsers to enable common tools for consumers to block tracking activities by third parties.

Transparency, control, and security are also essential concepts in Microsoft's Privacy Guidelines for Developing Software Products and Services, which are based on our internal privacy standards. We make these standards publicly available at *http://www.microsoft.com/privacy* for other organizations to use when developing and guiding their own product development processes. To encourage industry to adopt these guidelines, we have taught courses for others in industry to educate them on the standards.

IV. A Role for Technology Solutions

As a technology company, we naturally believe that technology has a key role to play in protecting consumer privacy. To ensure that we engineer privacy into our products from the outset and consider privacy issues throughout the project lifecycle, we have implemented internal policies and procedures that advance key principles such as transparency, control, and security.[7] For example, in individual business groups such as Windows, Office, and Xbox, we have a three-tier system of privacy managers, privacy leads, and privacy champs who help make sure that our products and services comply with our standards and applicable privacy laws. We also have a dedicated Trustworthy Computing team that works with business groups across the company to ensure that their products and services adhere to Microsoft's security and privacy policies. Although my colleagues in other divisions would be delighted to provide you with details about our initiatives for Bing, Kinect, and other products and services, I want to focus on our industry-leading browser, Microsoft's Internet Explorer.

Internet Explorer has really been a pioneering technology for protecting consumer privacy online. It was the first browser to introduce InPrivate Browsing, a feature that prevents a consumer's browsing history, temporary Internet files, form data, cookies, and usernames and passwords from being retained by the browser, thereby leaving virtually no evidence of the consumer's browsing history. Another feature in Internet Explorer 8, InPrivate Filtering, watches for third-party content that appears with high frequency across websites from companies that may be engaged in tracking activities, while still allowing consumers to view the content on the sites they've chosen to visit.

The InPrivate features were breakthroughs, but what I would like to highlight today is that Microsoft was the first of the major browser manufacturers to respond to the FTC's recent call for a persistent, browser-based "Do Not Track" mechanism.[8] The version of our browser that is being released this week, Internet Explorer 9, will offer an innovative new feature, "Tracking Protection," that allows consumers to decide which sites can receive their data and filters content from sites identified as privacy threats. Users will be able to create or download Tracking Protection Lists that identify websites which are, in the view of the list creator, trustworthy

---

[7] Both the FTC's proposed framework and legislation currently moving through Congress recognize the importance of a robust privacy by design program. We support these efforts to encourage industry to incorporate privacy protections into their data practices and to develop comprehensive privacy programs.

[8] *See* FTC Staff Report 66 ("Commission staff supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising, sometimes referred to as 'Do Not Track.' . . . The most practical method of providing uniform choice for online behavioral advertising would likely involve placing a setting similar to a persistent cookie on a consumer's browser and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements.")

or untrustworthy. If a site is listed as a "do not track" site on a Tracking Protection List, Internet Explorer 9 will block third-party content from that site, unless the user visits the site directly by clicking on a link or typing its web address. By limiting "calls" to third-party websites, Internet Explorer 9 limits the information these third-party sites can collect—without relying on the third-party sites to read, interpret, and honor a do-not-track signal. At the same time, Tracking Protection Lists can include "OK to call" entries that permit calls to specific sites, which allows consumers to create exceptions in a given list.

The Tracking Protection feature is highly customizable and can be adapted to specific user preferences because anyone on the Web (including consumer groups and privacy advocates, enterprises, security firms, and consumers) will be able to create and publish Tracking Protection Lists—they are simply files that can be uploaded to a website and made available to others via a link. Tracking Protection also supports user control: consumers can create or subscribe to more than one list if they wish, they can subscribe and unsubscribe to lists as they see fit, and a decision to subscribe to a list or lists will enable Tracking Protection across all browsing sessions until the consumer chooses to turn it off. Finally, Tracking Protection was designed with security in mind: because the Web evolves over time and third parties might migrate to new domain names, Internet Explorer 9 will automatically check for updates to a consumer's lists on a regular basis, helping ensure that the lists address the latest privacy and security threats.

V. A Role for Consumer Education

We agree with the FTC and the Commerce Department that there is a need for greater consumer education to increase consumer understanding of data practices and their privacy implications.[9] At Microsoft, we recognize that it is crucial to engage and educate consumers, to give them a voice and build a bridge to mutual understanding and benefit. That is why we provide consumers with clear information about our own practices and, where appropriate, offer choices about what data will be collected and how it will be used.

Microsoft was one of the first companies to adopt "layered" privacy notices. The Microsoft Online Privacy Statement provides consumers with the most important information about our privacy practices in a concise, one-page upfront summary with links to additional layers that describe in more detail our data collection and use practices, including the concepts of purpose specification and use limitation. Moreover, as noted above, we offer consumers easy ways to learn about online behavioral advertising and the privacy practices associated with the particular advertisements they receive, and to opt-out of behavioral advertising if they so choose.

We have also partnered with consumer advocates and government agencies to develop educational materials on consumer privacy and data security, such as:

- *National Cyber Security Alliance (NCSA).* Microsoft is part of this nonprofit public-private partnership that offers online safety and security information to the public on the *http://www.staysafeonline.org* website and through educational efforts such as National Cyber Security Awareness Month.
- *GetNetWise.* Microsoft supports this public education organization and website (*www.getnetwise.org*), which offers Internet users resources for making informed decisions about safer Internet use.
- *Internet Keep Safe Coalition* (*www.ikeepsafe.org*). Microsoft is a part of this partnership of Governors, attorneys general, public health and educational professionals, law enforcement, and industry leaders working together for the health and safety of youth online.
- *Stop. Think. Connect* (*http://safetyandsecuritymessaging.org*). Microsoft and a host of other organizations support this online safety campaign that promotes greater awareness and safer behavior on the Web.

We believe that such initiatives are important for ensuring that consumers understand the importance of protecting their privacy and security online, and are equipped with the tools to do so.

VI. Conclusion

Thank you for extending us an invitation to share our experience and recommendations with you. We commend the Committee for holding this hearing today, and we look forward to working with you to craft meaningful privacy protections that provide transparency, control, and security in a way that honors individ-

[9] *See* FTC Staff Report 78–79; Commerce Report 31–36.

uals' privacy expectations, complements existing technological and industry-based solutions, and promotes innovation.

Senator PRYOR. Thank you.

Mr. Montgomery?

STATEMENT OF JOHN MONTGOMERY, CHIEF OPERATING OFFICER, GROUPM INTERACTION

Mr. MONTGOMERY. Senator Pryor, members of the Committee, good morning and thank you for the opportunity to testify.

My name is John Montgomery. I'm the Chief Operating Officer of the North American operations of GroupM Interaction. GroupM is the world's leading, full service media investment operation employing over 17,000 employees in 81 countries. Our clients are some of the biggest brand advertisers in the world who we advise on where to place advertisements most effectively.

I begin my remarks where I believe the Committee's examination should begin with a review of the tremendous benefits provided by online advertising. While the Internet has revolutionized our lives in extraordinary and exciting ways and advertising is the fuel for the Internet economic engine. Behavioral advertising, also called interest based advertising, is an essential practice that delivers advertising based on consumer preferences or interests as inferred from data about online activities.

For example if a browser's activity suggested the user has a new baby we can show offers for baby products rather than retirement homes or sports cars. Consumers find such advertisements more relevant than random messages and advertisers are more likely to attract consumers that are interested in their products and services.

We at GroupM and our clients strongly believe in protecting consumer privacy. It's not only the right thing to do, but it's good for business. And I'm excited to share with the Committee the work that we've done to make sure that the consumers have both transparency and control to exercise their preferences in regard to online behavioral advertising.

GroupM has participated in an unprecedented cross industry effort by leading trade associations and companies that responds to the FTC's report that calls for self regulation on online behavioral advertising. This effort is being spearheaded by the leading associations that collectively represent the key elements of the Internet ecosystem, more than 5,000 companies in all. The FTC report set out a roadmap of key elements that should be included in self-regulation including transparency, consumer control and data security. And the major component of the program is the use of an icon that informs consumers that interest based advertising is occurring.

And to help create this icon GroupM mobilized our market leading advertising teams to invest the same design, testing, and market research in this icon as we would use for our Fortune 500 clients. Let me briefly show you how the principle works from a consumer's perspective. If I could refer you to the boards on my right.

Aboutads.info is a simple and effective "one stop" platform for consumers to opt-out of having their information collected and used for behavioral advertising purposes. Consumers can opt-out with the click of one button with respect to all participating companies.

And GroupM and hundreds of leading companies are working to advance compliance with the program.

Two other major elements of our implementation effort are education and enforcement. GroupM has partnered with the Interactive Advertising Bureau on a "Privacy Matters" education campaign to inform consumers about how they can manage their online experience and to explain how advertising supports the Internet. To date more than 600 million impressions are being delivered as part of this campaign.

And finally I want to emphasize that companies will be held accountable for complying with the principles just as the FTC recommended. All of us in advertising have a strong incentive to maintain accountability in order to foster consumer trust. The principles are enforceable through programs being administered by the Direct Marketing Association and the Council of Better Business Bureaus. These organizations have long-standing effective and respected compliance programs that they are leveraging to cover the principles. Any company that claims to comply but fails to do so could face FTC enforcement for deceptive acts or practices.

And whilst our program—whilst our progress has been exciting, our work continues. One of the major benefits of industry self regulation is the ability to respond quickly to changes to technology and business practices. For example recently, some policymakers have raised concerns that data collected for advertising purposes could be used as a basis for employment, credit or health insurance eligibility decisions.

I want to emphasize that these are hypothetical concerns that do not reflect actual business practice. But nevertheless industry is stepping forward to address these concerns. And we're expanding our guidelines to clarify and ensure that such practices are prohibited and will never occur.

The self regulatory principles owe much to the guidance of federal policymakers which have strengthened our independent commitment to consumer privacy and uniform choice. Now as you proceed in this dialogue it's vitally important to avoid mixed messages to consumers that could inhibit them from exercising their choice to the self-regulatory tool that's already available. We have to ensure that there's a single standard to make it simple for consumers. We do not want to add confusion to an already complex arena. Now I want to make it clear that we are working with a browser company such as Microsoft and Firefox and even Chrome, who are a part of the coalition to incorporate self-regulation and Do Not Track together.

So in conclusion, we believe that the program creates the right framework that encourages both innovation and privacy bringing the benefits for online services and privacy protection to consumers. Thank you, and I look forward to any questions.

[The prepared statement of Mr. Montgomery follows:]

PREPARED STATEMENT OF JOHN MONTGOMERY, CHIEF OPERATING OFFICER, NORTH AMERICA, GROUPM INTERACTION

I. Introduction

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, good morning and thank you for the opportunity to speak at this important hearing.

My name is John Montgomery and I am the Chief Operating Officer for the North American operations of GroupM Interaction ("GroupM"). Headquartered in New York City, GroupM is the world's leading full-service media investment management operation, employing over 17,000 employees in 81 countries. GroupM is the parent company of WPP's market-leading media communications agencies, including Maxus, MEC, Mindshare and Mediacom. Our clients are major global companies with brands that are household names. In the simplest terms, we advise clients on how to use advertising and where to place advertisements most effectively. Our business is built on the belief that both consumers and companies benefit when advertising provides timely and relevant information to those consumers who are most likely to be interested. While this philosophy is not new or unique to the Internet, online advertising has given us new tools to help our clients.

We at GroupM strongly believe in protecting consumer privacy. It is not only the right thing to do, but it is also good for business. We want to build consumer trust in the online experience, and therefore we believe that consumers should be able to choose whether and how their data is collected or used for online behavioral advertising. Our clients also want to provide these choices to maintain the confidence of their customers. Global companies work hard every day to protect their brands, and they recognize that their customers may have different preferences about online advertising.

My testimony today will describe how we have worked successfully with other industry leaders to give consumers these choices, and to create easy, uniform, and effective tools for them to exercise their choices. Our contributions illustrate the industry-wide collaboration and support behind this self-regulatory effort, which are truly impressive given our highly competitive marketplace.

II. Online Advertising Benefits Consumers and the Economy

I begin my remarks where I believe the Committee's examination should begin—with a review of the tremendous benefits provided by online advertising, especially behavioral advertising.

It is impossible to overstate the economic importance of the Internet today. Even in difficult times, e-commerce has continued to grow, thrive, and employ millions of Americans. The Internet is now the focus and a symbol of the United States' famed innovation, ingenuity, inventiveness, and entrepreneurial spirit, as well as the venture funding that follows. The Internet has already revolutionized our lives, and it continues to evolve in extraordinary and exciting ways. And as the Department of Commerce recently concluded, thus far the United States' approach to Internet policy has enabled the digital economy to flourish.[1]

Advertising helps to fuel the Internet economic engine. Revenues from online advertising support and facilitate e-commerce and subsidize the cost of content and services that consumers value, such as online newspapers, blogs, social networking sites, e-mail, and phone services. Because of advertising support, consumers can access a wealth of online resources for free or at a low cost. These resources have transformed our daily lives. Imagine parents who discover their child is sick at two o'clock in the morning. They can go online to look up basic medical information or find directions to the nearest doctor's office or emergency room. The Internet is now so established that we tend to take these resources for granted, but in fact they are largely supported by advertising.

Online advertising is equally vital to established businesses and new start-up companies. A study commissioned by the Interactive Advertising Bureau estimated that some three million Americans are employed due to the advertising-supported Internet.[2] Online advertising also fosters competition by making it easier for emerg-

---

[1] Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* at 1 (December 2010) (hereinafter "Commerce Policy Framework"), available at *http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf*.

[2] Hamilton Consultants, Inc. with Professors John Deighton and John Quelch, *Economic Value of the Advertising-Supported Internet Ecosystem*, at 4 (June 10, 2009), available at *http://www.iab.net/media/file/Economic-Value-Report.pdf*.

ing businesses to reach potential customers. In turn, these entrepreneurs spur existing market leaders to continue innovating.

Behavioral advertising is an essential form of online advertising. As the Committee knows, behavioral advertising, also called interest-based advertising, is delivered based on consumer preferences or interests as inferred from data about online activities. Consumers are likely to find behavioral advertisements more relevant than random messages, and advertisers are more likely to attract consumers that are interested in their products and services. For example, if a browser's activity suggests that the user has a new baby, we can show offers for baby products rather than retirement homes or sports cars. Websites also benefit because behavioral advertising garners better responses, allowing websites to earn more revenue—and support more content and services—for fewer advertisements.

At the same time, we recognize and respect that some consumers may prefer not to receive behavioral advertising. I am excited to share with the Committee the work we have done to make sure that consumers have both transparency and control to exercise their preferences in regard to online behavioral advertising.

III. Industry Self-Regulatory Principles Follow the Federal Trade Commission Roadmap

In February 2009, after an extended deliberative process, the Federal Trade Commission published a Staff Report that called upon industry to "redouble its efforts" to create self-regulation of online behavioral advertising.[3] The report set out a roadmap of several key elements that should be included in self-regulation, such as transparency, consumer control, and data security. The Commission also made clear that consumer tools to exercise choice should be easy to use, effective, uniform, and ubiquitous.

In the two years since the Commission's Staff Report, GroupM is pleased to have participated in an unprecedented cross-industry effort by leading trade associations and companies to respond to the Federal Trade Commission's endorsement of self-regulation. This effort has been spearheaded by the American Association of Advertising Agencies, the Association of National Advertisers, the Interactive Advertising Bureau, and the Direct Marketing Association, and also includes the American Advertising Federation, the Network Advertising Initiative, and other leading industry associations that represent components of the Internet ecosystem. These associations and the companies participating in the self-regulatory effort collectively account for the vast majority of online behavioral advertising. Following the roadmap set out by the Commission, we have worked diligently to develop standards, launch innovative tools, and educate consumers to make sure they have the choices they deserve.

In July 2009, just 5 months after the Federal Trade Commission's guidance, our coalition announced a groundbreaking set of Self-Regulatory Principles for Online Behavioral Advertising.[4] The Principles apply across the entire online advertising ecosystem. They address all of the key elements called for in the Federal Trade Commission's 2009 Staff Report, namely:

- Consumer education,
- Enhanced notice of data practices,
- Innovative choice mechanisms,
- Data security,
- Sensitive data protection,
- Consent for retroactive material policy changes, and
- Enforcement.

The Self-Regulatory Principles prescribe expectations for companies in each of these areas. They provide uniform definitions for key terms and include detailed Commentary to aid compliance.

GroupM believes that the Self-Regulatory Principles are comprehensive yet flexible enough to respond to the complex and rapidly evolving online advertising ecosystem. Most importantly, they are supported by all of the major industry stakeholders. We were pleased, therefore, that the Commerce Department's recent draft

---

[3] Federal Trade Commission Staff Report, *Self-Regulatory Principles for Online Behavioral Advertising* at 47 (February 2009), available at *http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf*.

[4] American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, and Council of Better Business Bureaus, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), available at *http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf*.

framework on privacy and innovation also favors voluntary and enforceable industry codes like our initiative.[5]

IV. Implementing Self-Regulation: Uniform Choice, Consumer Education, and Enforcement

Since releasing the Principles in July 2009, GroupM and other industry leaders have made significant investments in implementing the Principles across the Internet. A timeline of milestones is attached (Attachment 1). The development and launch of our Advertising Option Icon has been a key focus of this implementation phase, and I am very proud of GroupM's important contributions in this area. Advertisers who are adopting this icon for their advertisements are finding that the icon enhances a company's brand relating to its privacy stance. The icon is a win-win for consumers and businesses.

The Federal Trade Commission made clear, and we agree, that consumers should get notice of behavioral advertising practices that is uniform, ubiquitous, and "just in time" to make decisions. For uniformity, we also agreed that this notice should use a special graphic icon that would be memorable to consumers. To assist in the creation of this icon, GroupM mobilized our market-leading advertising teams to invest the same design, testing, and market research in this icon that we would use for our Fortune 500 clients. Our work was the basis for the Advertising Option Icon (Attachment 2), a simple but attention-grabbing graphic that we hope will become as universally familiar and recognizable as the recycling logo.

To make sure this notice is ubiquitous and "just in time," as recommended by the Federal Trade Commission, we reached the innovative solution of embedding the icon where data is collected and used for online behavioral advertising.

Let me briefly review how the Principles work from a consumer's perspective:

- First, an advertisement covered by the Principles is identified with the Advertising Option Icon, which appears in the advertisement right where the consumer will notice it (Attachment 3). The icon launched last December and has already been served in billions of advertisements, and we expect to reach the milestone of one trillion impressions by the end of this year.
- Clicking the Advertising Option Icon brings up a brief statement about online behavioral advertising, with a link to more information and opt-out choices.
- Interested consumers can click this link to visit AboutAds.info, an industry-sponsored website that provides consumer education (Attachment 4) and, most importantly, consumer choice (Attachment 5).

AboutAds.info is a simple and effective "one stop" platform for consumers to opt-out of having their information collected and used for behavioral advertising purposes. Consumers can opt-out with respect to all participating companies, or they can pick and choose which companies may collect and use their data.

The Federal Trade Commission has recently referred to this type of process as a "Do Not Track" system. We believe that our program provides "uniform notice and choice." Regardless of what terminology is used, our self-regulatory tools meet all of the policy goals that the Commission has publicly set forth. As implementation proceeds, no matter where consumers go online, they will see one memorable icon that leads to the same familiar and easy-to-use choice mechanism.

Companies can easily implement this uniform process and become compliant with the Self-Regulatory Principles by working with "approved providers" Evidon, TRUSTe, and DoubleVerify, which offer technical solutions for compliance. GroupM is working with Evidon to advance compliance in all of our offerings and agencies. Hundreds of leading companies are already compliant or in the process of complying.

Two other major elements of our implementation effort are education and enforcement. GroupM is strongly committed to consumer education and has made significant investments in this area. Our goal is to build consumer trust by helping consumers to understand and exercise their choices.

First, we have partnered with the Interactive Advertising Bureau on the "Privacy Matters" educational campaign to inform consumers about how they can manage their online experience and to explain how advertising supports the Internet. For this campaign, we used catchy and controversial slogans like "Advertising Is Creepy" to appeal to the consumers most interested in learning more. As part of this unparalleled effort, the Interactive Advertising Bureau's online publisher members have delivered close to 600 million online public service announcements. These announcements link to the "Privacy Matters" website (*http://www.iab.net/*

[5] Commerce Policy Framework at 5, 41–44.

privacymatters/), which features fun educational modules on advertising practices and safe Web browsing. Through January 2011, the results of this campaign have been excellent, with a click-through-rate that is substantially out-performing the standard range for public service campaigns.

GroupM has also supported the industry coalition effort to publicize the Self-Regulatory Principles and associated tools for businesses and consumers. This multi-faceted campaign, which supplements the consumer notice provided by the Advertising Option Icon, has included the launch of the AboutAds.info website, community outreach by the participating trade associations, a series of educational webinars to assist businesses with coming into compliance with the Principles, and the delivery of additional online public service announcements.

Finally, I want to emphasize that companies will be held accountable for complying with the Principles, just as the Federal Trade Commission recommended. The Principles are enforceable through programs being administered by the Direct Marketing Association and the Council of Better Business Bureaus.[6] These organizations have longstanding, effective, and respected compliance programs that they are leveraging to cover the Principles. The Council of Better Business Bureaus has created a new program and hired additional employees to administer the Principles. All of us in the advertising industry have a strong incentive to maintain accountability in order to foster consumer trust. In addition, any company that claims to comply, but fails to do so, could face Federal Trade Commission enforcement for deceptive acts or practices.

V. The Future of Self-Regulation

As I explained, the Self-Regulatory Principles include all of the elements set out in the Federal Trade Commission's 2009 roadmap. Less than 2 years after the Principles were announced, and thanks to strong investment by the business community, our implementation phase is gaining strong momentum. Every day, we are adding more members to the compliance programs, putting more Advertising Option Icons out on the Internet, and reaching more consumers with uniform notice and choice.

While our progress has been exciting, our work continues. One of the major benefits of industry self-regulation is its ability to respond quickly to changes in technology and business practices. For example, some policymakers have raised concerns that data collected for advertising purposes could be used as a basis for employment, credit, or health insurance eligibility decisions.[7] I want to emphasize that these are hypothetical concerns that do not reflect actual business practices. Nevertheless, industry is stepping forward to address these concerns and we are expanding our guidelines to clarify and ensure that such practices are prohibited and will never occur. This type of adaptability is essential to avoid stifling innovation in the complex and dynamic Internet environment. We welcome additional input from policymakers and we are committed to examining any future concerns that may arise.

The Self-Regulatory Principles owe much to the guidance of Federal policymakers, which has strengthened our independent commitment to consumer privacy and uniform choice. As we proceed in this dialogue, it is vitally important to avoid confusing or mixed messages to consumers that could inhibit them from exercising their choices through the self-regulatory tool that is already available. It is equally important to maintain incentives for the business community, which has already invested so much in self-regulation, to come into compliance with the Principles. GroupM and our partners look forward to continuing our efforts and working cooperatively with the Committee, the Federal Trade Commission, and the Department of Commerce as we move forward with implementing the Self-Regulatory Principles for Online Behavioral Advertising and discussing these important issues. We believe that this program creates the right framework that encourages both innovation and privacy, bringing the benefits of online services and privacy protection to consumers.

---

[6] Direct Marketing Association Press Release, "DMA Launches Enforcement for Online Behavioral Advertising" (January 31, 2011); Council of Better Business Bureaus Press Release, "Council Steps Up Enforcement of Interest-Based Advertising," (March 7, 2011).

[7] Representative Jackie Speier, "Do Not Track Our Online Data," *Politico* (March 4, 2011), available at *http://www.politico.com/news/stories/0311/50614.html*; Jon Leibowitz, "FTC Chairman: 'Do Not Track' Rules Would Help Web Thrive—Online commerce and personal privacy are not incompatible," *U.S. News* (January 3, 2011), available at *http://www.usnews.com/opinion/articles/2011/01/03/ftc-chairman-do-not-track-rules-would-help-web-thrive-jon-leibowitz*.

***

Thank you for inviting me to share GroupM's perspective on "The State of Online Consumer Privacy." I look forward to answering any questions that the Committee may have.

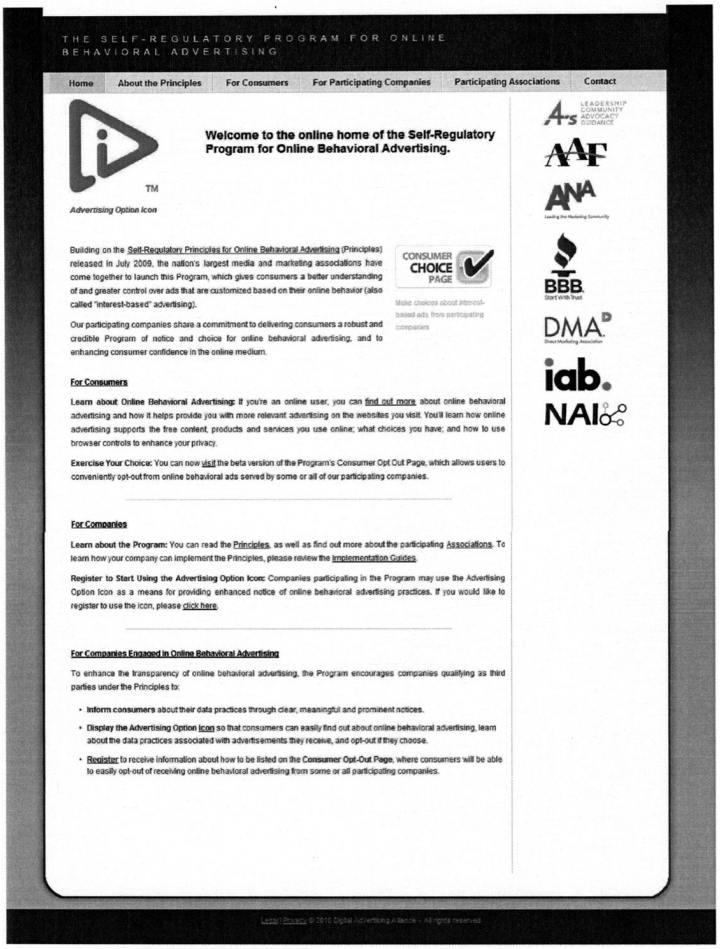
Attachment 1: Timeline of Industry Effort to Develop and Implement Self-Regulatory Principles for Online Behavioral Adverting

December 2007	Federal Trade Commission staff releases proposed principles to guide the development of industry self-regulation in the area of online behavioral advertising.
April 2008	Industry leaders file comments on Federal Trade Commission's proposals and convene task force to examine existing self- regulatory efforts.
October 2008	Industry coalition begins drafting new self-regulatory guidelines.
February 2009	Federal Trade Commission releases final Staff Report on *Self-Regulatory Principles for Online Behavioral Advertising*
July 2009	After building support among industry stakeholders, coalition releases cross-industry *Self-Regulatory Principles for Online Behavioral Advertising* ("Principles") that correspond to the guidelines in the FTC staff report.
August 2009	Coalition turns to enforcement, operational implementation, and educational planning.
November 2009	Interactive Advertising Bureau and Network Advertising Initiative lead effort to develop technical specifications for implementing enhanced notice through a link in or around an advertisement.
December 2009	Coalition launches "Privacy Matters" education campaign, which has been designed to educate consumers about how they can manage their online experience and to help consumers better understand and appreciate how online advertising supports the Internet.
January 2010	Coalition announces intention to provide enhanced notice to consumers through a link/icon embedded in online behavioral advertisements (or, if such notice is not delivered, on the Web page where the behavioral advertisement occurs).
March 2010	Coalition commences effort to operationalize the Principles, including providing business education webinars, trademarking distinctive Advertising Option Icon, and developing an industry- wide Website to deliver consumer education, provide information concerning parties engaged in online behavioral advertising, and offer consumer choice.
October 2010	AboutAds.info Website launches. Companies may register to use the Advertising Option Icon and acquire specific technical guidance for the icon's implementation and use. Coalition selects the first "approved provider" to offer technical solutions for compliance with the Principles.
November 2010	Coalition launches consumer-facing AboutAds,info Consumer Opt-Out Page, where consumers may easily opt-out of some or all of the interest-based advertisements they receive.
December 2010	Coalition selects two additional "approved provider" vendors.
January 2011	Direct Marketing Association enforcement program goes into effect.
February 2011	Principles and Communication Advisory Committee convenes to consider application of the Principles to mobile platforms, as well as ways to encourage international adoption of the icon and standards consistent with the Principles.
March 2011	Council of Better Business Bureaus enforcement program goes into effect. Accountability program selects vendor to provide technical platform to monitor participating companies' compliance with the Principles.

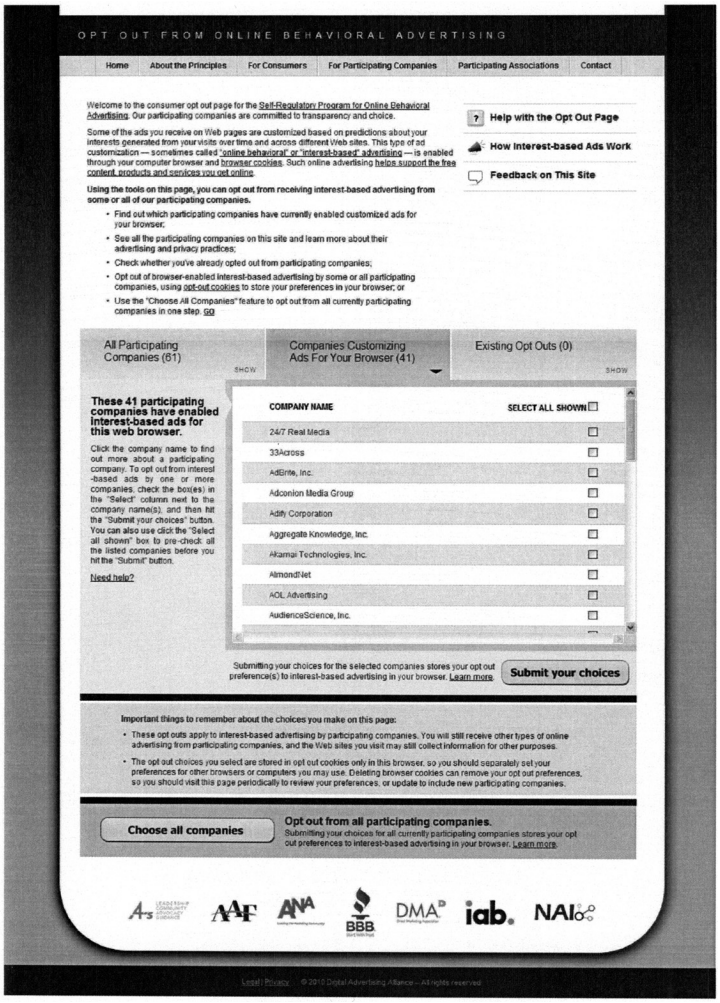
Attachment 2. Advertising Option Icon

Attachment 3. Sample Advertisement with Embedded Advertising Option Icon

Attachment 4. About Ads.info Home Page



Attachment 5. AboutAds.info Uniform Consumer Choice Page



Senator PRYOR. Thank you.
Mr. Soltani?

STATEMENT OF ASHKAN SOLTANI, INDEPENDENT PRIVACY RESEARCHER AND CONSULTANT

Mr. SOLTANI. Thank you. Senator Pryor and distinguished members of the Committee, thank you for the opportunity to testify about online consumer privacy and the state of web tracking. My name is Ashkan Soltani. I'm a technology researcher and consultant specializing in privacy and security on the Internet.

As background I served for a year as a technologist in the Division of Privacy and Identity Protection at the Federal Trade Com-

mission. I was also the primary technical consultant on the *Wall Street Journal's* "What they know" series. I should note the opinions here are my own and don't reflect the views of my previous employers.

In my testimony I will describe findings from my research about the pervasiveness of online tracking. I will discuss the extent to which consumers can control unwanted tracking. I will conclude with a description of the proposed Do Not Track mechanisms.

The practice of using third party services is very common on the web today. In 2009 I co-authored a study where we found an average of 12 third party trackers on the top 100 most visited websites. One site used roughly 100 different trackers. That means when a user visits that website 100 unseen entities are notified of that visit.

The very reason why online tracking is effective and why it raises privacy concerns is that the third-party entities can monitor user's behavior across multiple, unrelated websites. In our study one advertising service could track a user's web browsing activity down to approximately 90 percent of the websites we've examined. This company is not alone in its reach. Widgets from a single social networking company currently gather data across several million websites. These companies that were positioned to infer a great deal more than just the user's interests in automobiles or sporting goods. This unique vantage point enables them to collect the vast majority of a user's web browsing activity.

It's important to point out that online tracking is not limited to desktop computers. Mobile devices and smartphones raise unique privacy concerns because people always have them on their persons. Application and services running on these devices may have the ability to access precise location information providing third parties with intimate details about a user's habits.

Every major web browser includes a patchwork of privacy-enhancing technologies that are not enabled by default and that are often difficult to configure. Worse yet, even when properly configured online tracking companies have consistently devised ways to circumvent their function. As a result browser vendors and thus consumers are losing this game of privacy Whack-a-Mole.

Many ad services seek to temper privacy concerns by offering users a way to opt-out of behavioral advertising. However these opt-outs typically only allow users to opt out of receiving targeted ads not opt out of the underlying tracking fully. I don't think this is what most consumers would expect.

Finally, not all companies that engage in online tracking offer an opt-out. By my count only about a quarter of the online trackers I'm aware of have existing opt-out mechanisms.

Today's consumer choice mechanisms fail to provide users with meaningful control. Advocates and industry have been working to establish an easy to use tool to control online tracking commonly referred to as Do Not Track. Two separate but complementary approaches have been now advanced. And while I won't discuss them in technical detail here, I'm happy to answer any questions you might have about them.

To conclude, online tracking is pervasive on the Internet and it's an issue that's often difficult for users to understand. Even when

they do realize they are being tracked there's often very little that can be done. Consumers need more transparency into who is tracking them online, what information is being collected and how this information is being used, shared and sold.

There is a clear need for better privacy controls to prevent unwanted tracking. And industry has not delivered. To be effective privacy protections online will likely require both technology and policy working in tandem.

Thank you for inviting me today. And I hope that my testimony here is helpful. I'm grateful that the Committee has invited a technologist to participate since these issues can be deeply technical in nature. I look forward to helping you understand these nuances that make online tracking such an interesting and yet complex issue.

I'm happy to answer any questions.

[The prepared statement of Mr. Soltani follows:]

PREPARED STATEMENT OF ASHKAN SOLTANI,[1]
INDEPENDENT PRIVACY RESEARCHER AND CONSULTANT

Chairman Rockefeller, Ranking Member Hutchison, and the distinguished members of the Committee, thank you for the opportunity to testify about online consumer privacy and the state of tracking on the Web today.

My name is Ashkan Soltani. I am a technology researcher and consultant specializing in consumer privacy and security on the Internet. I have more than 15 years of experience as a technical consultant to Internet companies and Federal Government agencies. I received my Master's degree in Information Science from the University of California at Berkeley, where I conducted extensive research and published two major reports on the extent and means of online tracking. Last year, I served as a staff technologist in the Division of Privacy and Identity Protection at the Federal Trade Commission on investigations related to Internet technology and consumer privacy. I have also worked as the primary technical consultant on the *Wall Street Journal's What They Know* series investigating Internet privacy issues on the ground.

I have been asked to testify about the current state of online tracking from a technical perspective. I will describe the basics of how online tracking works and discuss some of my research that demonstrates how pervasive tracking is online today. I will then discuss the extent to which consumers are actually aware that they are being tracked online and whether they are able to meaningfully control unwanted tracking with existing industry-provided and browser-based mechanisms. Finally, I will discuss the Do Not Track proposals in light of these findings.

A. How Online Tracking Works

As an illustrative example to explain how consumers are tracked online, we can step through a typical Web browsing session. A user wants to look up information about cholesterol on WebMD, so he types "*www.webmd.com*" into his browser's location bar and navigates to a specific page on WebMD's site focused on cholesterol. The browser contacts the WebMD server to retrieve the contents of the page. Much of the page's content will be provided directly by WebMD itself, but some of the content may originate from other entities, such as an advertisement provided by an online advertising service such as Google's DoubleClick. As a result, although the browser's location bar will show "*www.webmd.com*," many other third party entities may have a presence on the website, and often it is unclear to the user which content comes from which provider.

A useful analogy may be to imagine a picture frame that has slots to display a number of different photos. WebMD provides the "frame" and a few of the "photos," while the rest of the "photos" are provided by third parties that WebMD has partnered with. This practice of embedding content from third party entities is nearly universal on the Web today. As I will explain below, it is primarily these third party entities that are capable of tracking users as they browse the Web.

[1] My oral and written testimony here today to the Committee represents my own personal views, and does not reflect the views of any of the organizations I have consulted or worked for in the past.

In this example, the WebMD page on cholesterol includes a third party online advertisement that is displayed at the top of the page. As the web browser fetches the ad, two things relevant to tracking typically occur. *First*, the company providing advertisements can attempt to uniquely identify the browser using a variety of technical mechanisms, which I will discuss below. The simplest and most common technique is to use a browser cookie. In this context, a cookie is a file containing a unique identifier that is placed on the user's computer by the third party ad service and is transmitted back to the service upon each subsequent ad request.[2] *Second*, the ad service can record detailed information about this interaction. The ad service may log the date and time of the ad request, which ad was displayed, and perhaps the details about the content of the WebMD page on which the ad was shown. Most importantly, the ad service can *link* all this information to the unique identifier, and collect this information together in a consumer data base.

Some time later, the user checks the weather by browsing to "*www.weather.com*." It turns out that the same third party ad service used by WebMD is also providing ads for the Weather Channel's site. As an ad loads in the margins of the Washington, D.C. forecast page, the ad service can again uniquely identify the user's browser, using the same cookie file that was previously stored. The ad service can now tie the user's browsing activity between the two sites together—the same browser that previously accessed health information about cholesterol also looked up the weather forecast in Washington, D.C. As the user continues to browse, this ad service can continue to follow the user's activity on the websites on which it has a presence. These activities are the essence of online tracking.

Web browsing interactions are generally described as being in one of two categories, *first party* or *third party*. A first party is typically defined as an entity whose site the user knowingly visits and whose Web address appears in the browser's location bar—in the scenario above, WebMD and then later, the Weather Channel. Users typically interact with a first party by directly typing its Web address into the location bar or by browsing to it from another site, for instance, by following a link from a search engine or a social network.

A third party is an entity that provides content that is included on a first party site, like the ad service in our earlier scenario. While some third party interactions are visible to the user, such as a displayed ad or an embedded video, it may not be clear that this content is being provided by someone other than the site they are visiting. However, other third party interactions may be *invisible* to the user. For example, a "web bug" is an imperceptible image placed on first party sites, but operated by third parties, for the express purpose of invisibly tracking users.[3] These third party tracking objects can only appear on a site with the knowledge and consent of the first party. As an example, ads from Google DoubleClick will only appear on Weather Channel pages if the Weather Channel explicitly decides to include DoubleClick on its site.

Note also that the same business entity can be both a first party or a third party, depending on the context. For instance, if a user browses directly to "*www.youtube.com*" to watch online videos, YouTube is a first party. But, if a first party site such as CNN.com embeds a YouTube video into one of its stories, YouTube is now a third party.

In our scenario, the ad service uses a standard browser cookie to link together two separate user interactions—one on WebMD and the other on the Weather Channel. Even though the cookie by itself does not usually identify the user by name, third party trackers are able to build a "browsing profile" that consists of data from numerous Web interactions over time from the same user.[4] This browsing profile has the potential to reveal quite a bit of information about the user's real world identity.[5]

Despite some claims that these collected browsing profiles are "anonymous," recent computer science research suggests that it is often quite easy to re-identify

---

[2] Cookies are text files that can store various types of information. For the purposes of tracking, they typically contain unique descriptors such as *user=1234567890* or *e-mail=john.doe @host.com*.

[3] Web bugs are sometimes also referred to as tracking pixels or web beacons. Web bugs are typically used to provide websites with information that will help them understand and optimize web usage, and typically track users.

[4] Of course, some browsers may be shared by multiple users, but often browsers will be used primarily by a single user. This is particularly salient in the case of mobile phones, where the sharing of devices is less common.

[5] Each data point may also reveal the time of each site access and in many cases the user's approximate geographic location based on his IP address. More advanced tracking techniques on a single page may be able to determine exactly how the user moves his mouse on the page or what text on the page gets highlighted and copied.

datasets that contain user information.[6] As the number of data points in a browsing profile increases, so too does the possibility that it can eventually be re-identified to reveal the user's actual identity, such as a name, e-mail address, or other personally identifiable information. For example, when a user purchases a product online, the merchant could decide to share the user's e-mail address—collected in the billing process—with a third-party ad service that is present on the purchase page. This issue can also arise with the use of social networks, whereby identifying information may leak to third party ad services.[7]

1. The State of Online Tracking

The practice of using third party services to add tracking and other functionality to a website is quite common. In our Berkeley *KnowPrivacy* study, we found an average of 12 trackers present on each of the top 100 most popular websites, with one having as many as 100 different trackers over the course of a month.[8] This means that when a user visits that website, potentially 100 entities—nearly all unseen by the user—will learn about the visit.

The very reason why online tracking is both effective and why it raises privacy concerns is that third party entities can track consumers across multiple unrelated first party websites. In our Berkeley study, we also found that some third party trackers have an extensive "reach" across a large number of first party sites. One advertising company was able to monitor activity on 91 of the top 100 most popular sites, as well as 88 percent of 350,000 sites sampled in our dataset, as of March 2009.[9] In 2010, a leading social network announced that their third party sharing widgets were present on 2.5 million websites[10] and growing at a rate of 10,000 sites per day.[11] In both these examples, the presence of third party objects generates a steady stream of data that flows to a single entity. These uniquely pervasive positions give these companies the capacity to infer a great deal more than just a user's interest in automobiles or sporting goods. Their tracking technologies reach the vast majority of every user's Web browsing activity.

It is important to point out that online tracking is not limited to Web browsers. Consumers are connecting to the Internet using a variety of devices that extend beyond what we consider a typical PC-and-browser setup. Mobile phones, televisions, set top boxes (such as a Tivo or a cable box), video game consoles and even some automobiles are now equipped with Internet connectivity and can leverage Web services which include online advertisement. Some of these platforms also allow applications written by third parties, the most prominent example being "app stores" on mobile smartphones.[12] Mobile devices, in particular, raise unique privacy concerns because consumers carry them nearly all of the time.[13] As such, applications and services running on the phone may have the ability to access precise geolocation information, using GPS technology, to learn even more intimate details about a consumer's physical habits.

---

[6] Narayanan, A., & Shmatikov, V. (2008). How to Break Anonymity of the Netflix Prize Dataset. In Proc. of 29th IEEE Symposium on Security and Privacy, Oakland, CA, May 2008, pp. 111–125. *and* Ohm, P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (2009, August 13). University of Colorado Law Legal Studies Research Paper No. 09–12. Available at SSRN: *http://ssrn.com/abstract=1450006*.

[7] Krishnamurthy, B. and Willis, C. (2009). On the leakage of personally identifiable information via online social networks. In Proceedings of the 2nd ACM workshop on Online social networks (WOSN '09). ACM, New York, NY, USA, 7–12. DOI=10.1145/1592665.1592668 from *http://doi.acm.org/10.1145/1592665.1592668*.

[8] Gomez, J., Pinnick, T., and Soltani, A. (2009, June 1). *KnowPrivacy* available at *http://knowprivacy.org/report/KnowPrivacy__Final__Report.pdf,* p.26.

[9] *Id.* p. 27.

[10] Constine, J. (2011, February 27). All of Facebook's Like Buttons on Third-Party Sites Now Publish a Full News Feed Story. Inside Facebook—Tracking Facebook and the Facebook Platform for Developers and Marketers from *http://www.insidefacebook.com/2011/02/27/like-button-full-story/*.

[11] Parr, B. (2010, October 26). 10,000 Websites Integrate with Facebook Every Day. Social Media News and Web Tips—Mashable—The Social Media Guide. from *http://mashable.com/2010/10/26/10000-websites-integrate-with-facebook-every-day/*.

[12] *The Wall Street Journal* reported that 47 of the 101 third party mobile applications tested transmitted location to third parties. 56 of the same apps transmitted unique device identifiers (UDIDs) which act similar to permanent cookies, and which users currently have no control over. See Thurm, S. (2011, December 17). IPhone and Android Apps Breach Privacy—*WSJ.com*. *The Wall Street Journal* from *http:// online.wsj.com/article/SB1*.

[13] Three in five mobile phone owners say they carry their phones at all times, even inside the home. See: Stanton, D. (2008, September 8). New Study Shows Mobile Phones Merging New, Established Roles. Knowledge Networks from *http://www.knowledgenetworks.com/news/releases/2008/091808__mobilephones.html*.

2. Existing Privacy Tools are Easily Circumvented

Every major Web browser includes privacy enhancing technologies that can be used by consumers to limit the extent to which they are tracked online. Unfortunately, these built-in tools, which include "private browsing modes" and cookie controls, only protect users from some tracking technologies, and do not provide consumers with the privacy protections they may reasonably expect.[14]

As one example, cookie blocking features in the major Web browsers do not always work in the same way, and even sophisticated users do not fully understand these intricacies.[15] This may cause consumers to have misplaced beliefs about the extent browsers are protecting them from tracking. But even when consumers do understand how these features work, sites have consistently devised new ways to track users and evade the protections of existing privacy tools.

In a study called *KnowPrivacy* published by my Berkeley colleagues and I in 2009,[16] we found that several ad services had deployed a new stealthy technique to *resurrect* tracking cookies, even after the user had used the available cookie deletion tools built into his browser. Ad services developed a way to "remember" the cookie file using another technology—Adobe's Flash Player—such that they could restore the cookie later, even after the user deleted it. This tracking technology—commonly called Flash cookies—is even *more* difficult for users to manage with existing privacy tools, when compared to standard cookie controls.[17]

Further, some ad services have shifted to new, cutting-edge tracking techniques, many of which are beyond the control of consumers.[18] While these are less well known, they are no less powerful—and in some cases more powerful—in their ability to track users' browsing activities. From a technical perspective, browser vendors—and thus consumers—are losing the game of privacy Whack-a-Mole. The ongoing development of new, hidden tracking techniques is far outpacing the ability of browser vendors to develop and deploy adequate defenses. As a result, consumers and the privacy controls available to them will likely fail to keep up.

B. Existing Consumer "Notice and Choice" Mechanisms

The current system of industry self-regulation stresses two complementary approaches regarding online tracking: *notice*, though privacy policies and in-ad enhancements, and choice, through ad preference managers and industry-provided opt-out tools.

1. Privacy Policies

For more than a decade, websites have routinely included privacy policies, typically linked to from the bottom of the front page. These documents are often long and difficult to read—most likely because they are written by lawyers, for lawyers—and have not helped consumers to stay informed about the degree of tracking on-

---

[14] Soghoian, C. (2010, December 9). Why Private Browsing Modes Do Not Deliver Real Privacy, Internet Architecture Board, Web Privacy Workshop, from *http://www.iab.org/about/workshops/privacy/papers/christopher__soghoian.pdf*.

[15] Not all browsers implement third party cookie blocking in the same way. Typically browsers allow third party cookies by default but if a user elects to configure their browser to block third party cookies, 3 of the 4 major browsers allow the third party cookies to be read if they were previously set, such as in a first party context. This is a small technical nuance, but it allows certain players to proceed as normal with regards to online tracking and potentially cause confusion for consumers as to the degree their privacy is protected. Additionally, it significantly effects whether certain players, *i.e.,* those that consumers have a first party relationship with, receive a competitive advantage over the lesser known websites.

[16] Soltani, A., Canty, S., Mayo, Q., Thomas, L., and Hoofnagle, C., Flash Cookies and Privacy (2009 August 10). *Available at SSRN http://ssrn.com/abstract=1446862*.

[17] Adobe has denounced the use of its Flash technology in order to restore tracking cookies. Although not yet widely deployed, the company has recently taken steps to work with major browser vendors in order to move Flash cookie privacy controls directly into the browser settings and allow users to manage them in a similar way as standard cookies. See Albanesius, C. (2011, March 8). Adobe Flash Player 10.3 Beta Adds Greater Control Over'Flash Cookies' PC Magazine. from *http://www.pcmag.com/article2/0,2817,2381650,00.asp*.

[18] In the past year, I have confirmed tracking by third party companies on widely used websites using mechanisms including but not limited to browser fingerprinting (*http://radar.oreilly.com/2011/03/device-identification-bluecava.html)*, cache cookies (*http://www.wired.com/epicenter/2009/08/flash-cookie≥researchers-spark-quantcast-change/*), CSS history profiling (*http://blogs.forbes.com/kashmirhill/2010/11/30/history-sniffing-how-youporn-checks-what-other-porn-sites-youve-visited-and-ad-networks-test≥the-quality-of-their-data/*), domain masquerading (*http://doi.acm.org/10.1145/1592665.1592668*), UDIDs (*http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html*), and HTML5 storage (*http://www.wired.com/threatlevel/2010/09/html5-safari-exploit/*) to track consumers in ways that are difficult or even impossible to control.

line.[19] Research has also shown that the majority of Americans incorrectly believe that the phrase "privacy policy"—and its mere presence on websites—signifies that their information will be kept private.[20]

While there is much data to suggest that consumers do not actually read or understand privacy policies, even if they did, many existing privacy policies often provide confusing or even conflicting information. In our *KnowPrivacy* study, we found that, among the top 50 most popular websites, many sites that claim to not share information with "third parties" later disclaim that they do share information with "affiliates", which sometimes number well over 2000 companies.[21]

2. Enhanced Notice for Online Ads

One emerging self-regulatory measure is "enhanced" or "robust" notice for online ads. The purpose of enhanced notice is to increase transparency—directly within the ad—into why the particular ad was chosen and what the attached terms and policies are. Although this is a commendable step forward, the question is how many users will notice. One self-regulatory firm noted that, during the first few months of the industry's initiative, the notice on only 0.004 percent of "enhanced" ads were clicked by users actually clicked through to the detailed explanatory text.[22] While the initiative is in its early days, this calls into question whether enhanced notice will be sufficient to deliver meaningful transparency.

3. Ad Preferences Managers

The advertising industry has also created online tools that allow users to view and modify marketing inferences made about them within "ad preferences managers." For example, an ad preferences tool may show the inferences made about the user's demographic information (such as age, income range, education, or geographic location), shopping interests (such as sports, technology, or politics), or even significant life events (such as "getting married soon" or "having a baby") based on the user's browsing activity. In many cases, these tools also allow consumers to opt-out of certain consumer marketing sectors from which they do not wish to receive targeted ads.

Like enhanced notice, ad preference managers improve transparency into the online ad serving ecosystem. But, these managers only present a high-level summary of the information collected by the ad service. Given their vantage point, third party ad services have the capability to make inferences or use the data for other, non-advertising-related purposes, that are not shown in the ad preference managers.[23] I'm not implying that specific companies are engaged in this practice, just that collection, retention, and correlation of this behavioral data *provides the capacity* for this these inferences to be made. More transparency is needed—outside the realm of online targeted ads—about the information that is collected by third parties and how they are used.

4. Cookie-based Choice Mechanisms

In addition to notice and transparency, many ad services provide users with the ability to opt-out. Currently, most opt-outs work using special opt-out cookies—one for each ad service—stored in the user's Web browser. The cookie-based opt-outs have been plagued by a number of problems, some of which have been addressed in recent years and others which persist today.

Once consumers realize they are being tracked, they must then begin the process of obtaining opt-out cookies from each tracking company. One self-regulatory tech-

---

[19] McDonald, A. and Cranor, L. (2008) The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society 2008 Privacy Year in Review issue. [Paper originally presented at TPRC 2008, Sept 26–28, 2008, Arlington, VA.] and Privacy Leadership Initiative. Privacy Notices Research Final Results. Conducted by Harris Intereactive, (2001 Dec) from *http://www.ftc.gov/bcp/workshops/glb/supporting/harris%20results.pdf*.

[20] Turow, J., Mulligan, D., and Hoofnagle C. (2007 Oct), Consumers Fundamentally Misunderstand the Online Advertising Marketplace, from *http://groups.ischool.berkeley.edu/samuelsonclinic/files/annenberg_samuelson_advertising.pdf*.

[21] Of the top 50 sites, all stated they collect IP address, 48 collect contact information such as name and e-mail address, and 39 collect click stream information. Bank of America had over 2,300 "affiliates". See Gomez *et al*. p 24 (previously cited) and *KnowPrivacy*, *http://knowprivacy.org/profiles/bankofamerica*.

[22] Evidon served over 11 billion impressions in their first full scale months. Among those who click on the icon (on .004 percent of ads served), about 3 percent of users opt-out of one or more provider. *See* Smith, S. (2011, March 11). MediaPost Publications Browsing Privacy's Next Steps 03/11/2011 from *http:// www.mediapost.com/publications/?fa=Articles.showArticle&art_aid*.

[23] Similar to sports and shopping habits, a user's browsing habits could allow an observer to make inferences about a users race, sex, sexual orientation, health status, financial health, and political affiliation, even though these categories are typically excluded from online preference managers.

nology firm has identified 600 companies involved in collecting or using tracking data about customers on their sample of 7 million domains.[24] Another lists 323 tracking companies publicly.[25] Given the value of this marketplace and the speed with which new entrants emerge, I suspect the actual number of companies engaged in tracking may be actually be even larger. Even still, identifying 600 hidden trackers and obtaining an opt-out is daunting task for even the most sophisticated privacy-conscious consumer.

Seeking to ease the process of obtaining opt-out cookies, industry self-regulatory groups such as the Network Advertising Initiative (NAI) have created one-stop websites where consumers can obtain opt-out cookies for multiple firms. However, these opt-out sites do not comprehensively cover all online tracking since only a fraction of approximate 600 companies discussed are covered.[26] This problem exists in the mobile space as well. Currently, nine of the 16 mobile ad companies do not offer an opt-out,[27] and data collected on mobile phones may be particularly sensitive, since it is often accompanied by hardware identifiers that users cannot change or geographic location information.

Most importantly, even when opt-outs are available, many firms only allow the user to opt-out of the receipt of targeted advertising, not the online tracking itself. *Advertisers continue to collect and retain data in order to build a profile on the user*, even in the presence of an opt-out cookie.

Finally, cookie-based opt-out mechanisms are *inherently brittle*. Users are frequently taught to delete their browser cookies on a periodic basis to better protect their online privacy. But, when the user clears her browser cookies, she will also inadvertently clear her *opt-out* cookies, which will—counter-intuitively—opt the user back *in* to tracking.

C. Do Not Track Proposals

Last July, this Committee held a hearing on the topic of online privacy during which the idea of "Do Not Track" was discussed. Ever since, there has been a significant amount of public discussion and debate regarding the possibility of a Do Not Track mechanism. While the name—Do Not Track—sounds much like the highly successful Do Not Call list,[28] the only substantive similarity is that they both give consumers a single point of control to express their privacy preferences. While consumers can register their phone number in a FTC registry for Do Not Call, the single point of control for Do Not Track is likely to be a preference setting in the consumer's Web browser or mobile platform.

Two primary technical approaches to Do Not Track have been proposed and implemented by major Web browser vendors. The first method is called the *header* approach, and the second is called the *blocking* approach. Two browser vendors have already taken steps to include these mechanisms in upcoming releases of their products.[29]

1. The Header Approach

In the *header* approach, the consumer can toggle a Do Not Track setting in his Web browser privacy preferences. When this setting is enabled, the browser transmits a special signal to each remote server that the consumer has expressed his preference to not be tracked.[30] The idea is to give users the ability to send a clear, persistent and technology-neutral signal to websites regarding their tracking pref-

---

[24] Steel, E. (2011, March 4). Council of Better Business Bureaus to Enforce Online Tracking Principles ≥ Digits. WSJ Blogs—WSJ from *http://blogs.wsj.com/digits/2011/03/04/council-to-enforce-online-tracking-principles/*.

[25] PrivacyChoice Tracker Index (Mar 14 2011) from *http://www.privacychoice.org/companies/all*.

[26] At the time of this writing, the NAI opt-out (*http://www.networkadvertising.org/managing/optout.asp*) currently allows consumers to opt-out of behavioral advertising by 68 member companies. AboutAds opt-out applies to 61 companies (*http://www.aboutads.info/choices/*) and even the most comprehensive list of trackers, offered by the independent group PrivacyChoice only allows opt-out of 160 (*http:// www.privacychoice.org/privacymark*).

[27] Brock, J. (2011, March 16). Mobile Tracking Privacy: Three thoughts. PrivacyChoice Blog. from *http://blog.privacychoice.org/?p=2882*.

[28] The Do Not Call list is an FTC enforced initiative based on legislation that creates a centralized registry of numbers that telemarketers may not call, under monetary penalty.

[29] Mozilla's Firefox 4.0 and Microsoft's Internet Explorer 9 (MSIE9) have announced support for the header mechanism. MSIE9 also supports the blocking method as well via their Tracker Protection Lists product.

[30] Current proposals involve sending a Do Not Track signal using a browser header within the HTTP protocol.

erence. Of course, in order this mechanism to be effective, it will depend upon a clear set of rules defining what websites should do when they receive this signal.

Under this approach, the onus is on the server to agree to respect the consumer's preference. It is possible that the server could ignore the user's request and continue to engage in tracking anyway, even once best practices are established. Thus, consumers will need a method to verify that servers are complying with the header, so they can keep firms honest about their commitment to respect user tracking preferences. Publisher sites and U.S. brands that advertise could choose to favor ad services that respect the header preference.

2. The Blocking Approach

In the *blocking* approach, the consumer maintains (perhaps with the help of a trusted third party) a list of servers that are known to engage, or are suspected of engaging, in unwanted tracking behavior. Once a user has enabled this feature, his Web browser will automatically block all connections to the servers on the list which could also result in the blocking the display of advertisement.

As opposed to the header approach, the responsibility to prevent tracking is solely on the consumer, that is, to obtain an up-to-date list of suspected tracking servers and to block them. Servers are under no express obligation to abstain from tracking, so if one is not blocked by a consumer's browser, it is free to continue tracking as usual.

One concern with this approach is that it is sometimes difficult for consumers-at-large to determine whether a domain is engaging in tracking behavior and whether to add that domain to the block list. Additionally, there are many technical mechanisms that exist today that could be used to circumvent such blocking measures.[31]

3. Other Considerations

For any consumer choice mechanism to work, we need to clearing define what "tracking" means and what obligations are placed on tracking companies when consumers elect to opt-out of tracking. Consumer groups and privacy researchers have published proposals that attempt to define "tracking,"[32] but the online advertising industry has not yet committed to respect the header nor follow any of the proposed definitions. For example, some in the industry have suggested that, like the current opt-out system, third parties be allowed permitted to continue to collect information. Others have proposed that third party services should refrain from collecting and retaining any information about consumers if they elect to not be tracked. This latter approach, while more privacy-preserving, may impact advertisers' abilities to deliver even non-targeted advertisements and includes numerous exceptions to tracking which may defeat the spirit of a privacy mechanism.

A potential way forward may be to agree upon a definition of "tracking" that balances these conflicting priorities. One of the key components that enables tracking today is the use of unique identifiers. As such, it may be wise to consider a definition of tracking that focuses on these identifiers, in which third party services make a good faith effort to strip any unique identifiers associated with the user, browser or client device making the Web request once the request has been processed and the service delivered. By focusing on the identifiers, these companies would then be free to retain the remaining data associated with the user's request, providing that it cannot be re-identified (following current best practices in the space). This approach will likely be good for both business and consumers, since it allows businesses to observe how their websites are being used and secure their servers, while preventing the creation of individual profiles.

Finally, it is important to consider whether creating more effective choice mechanisms for consumers may have perverse effects and ultimately drive websites to predicate access to content based on whether or not a consumer has consented to tracking. Websites could require that consumers allow tracking by third parties the website is affiliated with in order to gain access to it's content. In our original example, WebMD could require that their affiliates, such as DoubleClick, be allowed to track consumers in order to gain access to useful health information on the website. This trend could potentially favor large first parties over smaller, independent sites or allow companies to engage in even more invasive tracking upon receiving affirma-

---

[31] In particular, domains can "spoof" the first party transactions that are whitelisted in browsers, or effectively act as first parties. This means that they are bypassing any third party-specific controls used in the browser. See Krishnamurthy *et. al.,* (previously cited).

[32] What Does 'Do Not Track' Mean? "A Scoping Proposal" by the Center for Democracy & Technology (2011, Jan 31) from *http://cdt.org/files/pdfs/CDT-DNT-Report.pdf.*

tive consent. This is not a reason to abandon efforts to improve consumer choice, but certainly a reason for Congress to consider the issue carefully.

D. Conclusion

My research has shown that online tracking is pervasive. It is likely to be much more extensive than users might reasonably expect as they casually browse the Web. Many of these third party tracking activities are carefully tucked away from the view of the average user, and even in cases where the user realizes he is being tracked, the privacy tools he has available are often ineffective at stopping the most advanced forms of tracking.

Consumers need more transparency into who is tracking them online, what data is being collected, and how this data is being used, shared or sold. Today's technical defenses to online tracking are not able to stop the leading tracking technologies, and consumers often do not have meaningful ways to control them. To be effective, privacy protections for consumers online will likely require both a technical and policy component, working in tandem, and I believe these discussions here today are a great step in making that union a reality.

Internet-related debate involves issues that are deeply technical in nature and I am grateful that this Congressional committee has allowed technologists to participate. Thank you for inviting me to testify here today, and I look forward to helping the committee understand the technical issues that make online tracking such an interesting, yet complex, issue. I will be happy to answer any further questions.

Senator KERRY [presiding]. Thanks. Who's next?

Ms. Lawler?

STATEMENT OF BARBARA LAWLER, CHIEF PRIVACY OFFICER, INTUIT INC.

Ms. LAWLER. Good morning. And thank you to the members of the Committee for the opportunity to comment on the state of online privacy. My name is Barbara Lawler and I'm the Chief Privacy Officer at Intuit. I ask that my full statement be put into the record due to time constraints.

Senator KERRY. Without objection it will be.

Ms. LAWLER. Intuit's mission is to improve people's financial lives so profoundly they cannot imagine going back to the old way of doing things. It is through this mission that we approach the current privacy debate. Intuit is a unique corporation adhering to various regulatory data privacy regimes in the U.S. including financial and health care privacy and the privacy of tax return information.

Additionally, we touch over 50 million people through our products. These people can trust us with their most sensitive data, their Federal and state income tax return information, their individual purchase transactions, bill payments and health information, their business accounts including employee payroll, accounts receivable, vendor lists, inventory and other business data. As more technology solutions move to the cloud, customers place more trust in us as we handle their sensitive data.

At Intuit, we developed data stewardship principles that express how we think about how we use data, and offer guardrails to guide our judgment. The central concept of data stewardship is simple. It's our customer's data, not ours. We are and will be held accountable for the information entrusted to us.

As you think about privacy legislation we encourage you to consider four things.

One, a principles-based approach.

Two, a focus on customers.

Three, data-driven innovation.

And four, global uniformity.

First, we see the value in comprehensive, principles-based privacy legislation. Because we adhere to various privacy regimes, this idea could work in tandem with self-regulatory approaches, codes of conduct and best practices. A principles-based approach is not prescriptive but enables flexibility to offer data driven solutions within existing sector specific privacy laws. A principles-based approach could fill the gaps that exist between different sector approaches while at the same time blending with them.

It's also more likely to be received and effectively adapted by all businesses of all sizes. It is more likely to be understood by the public it seeks to protect. And a principles-based approach is more likely to achieve consensus over time in the international context which will be essential to global competitiveness in the emerging digital economy.

Such an approach could set forth a minimum set of requirements for business and provide a fundamental core level of consistency for businesses and consumers. Codes of conduct based on context, industry sector, technology platform and other data use drivers would build on top of a privacy baseline. Codes of conduct can serve as the framework and support for co-regulatory safe harbor programs.

Second, any relevant data regime must be focused on the customer. At Intuit, customers are the heart of everything we do. What we learn through extensive customer research is that it's not about what we think is best for business or what we think should be done. It's about keeping what's important to the customer at the heart of the principles.

Third, responsible data use can foster innovation. Consumers' expectations have changed as people are increasingly conducting their lives online. The volume and complexity of data in this new connected world presents boundless opportunities to unlock a tremendous amount of data to create better experiences and products for customers. Intuit's approach to data-driven innovation is to responsibly use data entrusted to us by our customers to improve their financial lives and the products and services we provide them.

Last but not least, legislation must take into account the need for uniformity among various privacy regimes. In developing privacy principles there needs to be a uniform approach. While so many laws and regulations are based on essentially the same principles, multi-state and multinational companies are challenged by the differences among them.

The essence of data stewardship cannot rely on just one element of our principles. It must be comprised of all of them combined: uniform principles-based legislation, customer driven innovation coupled with responsible, innovative and compelling data uses.

Thank you again for giving Intuit the opportunity to express its thoughts on this important subject. We look forward to working with you as you evaluate privacy legislation and to answering any questions you may have.

[The prepared statement of Ms. Lawler follows:]

PREPARED STATEMENT OF BARBARA LAWLER, CHIEF PRIVACY OFFICER, INTUIT INC.

Good morning and thank you Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee for providing Intuit the opportunity to share our point of view on the best way to protect consumer privacy in the technology-driven, Internet era. We applaud the Committee for its attention to this important issue.

Today, I'm here to talk to you about how Intuit views online consumer privacy. Intuit is in a unique position to comment on the current privacy debate. Not only do we have a unique perspective given the nature of our comprehensive business portfolio and compliance with privacy regimes, but fifty million people trust us with their most sensitive data. I will be talking today about the creation of Intuit's Data Stewardship Principles, the process of how we developed these principles, and what we learned from this process, as well as the principles themselves.

As you think about comprehensive privacy legislation, we encourage you to focus on four things:

1. principles-based privacy
2. customers
3. data driven innovation
4. global uniformity

About Intuit

Intuit was founded in Silicon Valley nearly thirty years ago. Our mission is to improve people's financial lives so profoundly, they cannot imagine going back to the old way of doing things.

We started small with Quicken personal finance software, simplifying the common household dilemma of balancing the family checkbook. Today, we are one of the Nation's leading providers of tax, financial management and online banking solutions for consumers and small businesses, and the accountants, financial institutions and healthcare providers that serve them. We employ nearly 8,000 people, our revenues top $3.5 billion and we're recognized by *Fortune Magazine* as one of America's most-admired software companies and one of the country's best places to work.

We have always believed that with our success comes the responsibility to give back. Part of delivering on our mission is serving as an advocate and resource for economic empowerment among lower income individuals and entrepreneurs. We have a track record of more than a decade of philanthropy that enables eligible lower income, disadvantaged and underserved individuals and small businesses to benefit from our tools and resources for free.

Through it all we remain committed to creating new and easier ways for consumers and businesses to tackle life's financial chores with the help of technology. We help our customers make and save money, comply with laws and regulations, and give them more time to live their lives and grow their businesses.

Our flagship products and services, including QuickBooks, Quicken, Mint.com and TurboTax, simplify small business management, payment and payroll processing, personal finance, and tax preparation and filing. We serve half of the accounting firms in the country, helping them be more productive with tax preparation software. And we help community banks and credit unions grow by providing on-demand solutions and services that make it easier for consumers and businesses to manage their money.

The innovation and customer driven focus that inspired these breakthroughs leads us to uncover other unmet needs and large problems to solve. For example, we are working to simplify the way millions of Americans manage their health and medical expenses. Today, doctor's offices are paper-based, inefficient and need a way to reduce costs and delight their patients who are increasingly demanding online solutions. Our Intuit Health Patient Portal offering is a secure, online way for doctors and their patients to communicate and complete key tasks. Patients can request appointments and prescription refills, pay bills, complete forms, receive lab results, and exchange messages with their doctor. As a result, doctors are able to reduce costs, delight patients, and qualify for Meaningful Use stimulus funding.

With all of these offerings, we help improve the lives of fifty million people, worldwide.

We're able to do this because our customers entrust us with their most sensitive data—fifty million people trust us with their Federal and state income tax return information; their individual purchase transactions, bill payments, and health information; and their business accounts, including employee payroll, accounts receivable, vendor lists, inventory and other business data.

We are widely recognized and respected for our strong privacy and security practices. Maintaining our customers' trust is critical to maintaining our business and

competitive advantage. We do not view customer privacy and security as an exercise in compliance but as part of our value proposition.

Intuit products span a range of sector-specific regulatory data privacy regimes in the US, including Gramm Leach Bliley Act, Fair Credit Reporting Act/Fair and Accurate Credit Transactions Act, IRC 7216—the privacy of individuals' personal tax information, Health Insurance Portability and Accountability Act; and self-regulatory regimes including PCI Data Security Standards, the U.S.-E.U. Safe Harbor Program and the TRUSTe Privacy Seal Program.

Given the nature of our comprehensive business, providing solutions for a range of tax, accounting, personal finance and health care needs, Intuit is in a unique position to comment and shape the online privacy debate.

Intuit's Data Stewardship Philosophy

As more solutions move to the cloud, customers place trust in us as we handle their most sensitive data. Data Stewardship expresses how we think about the use of data, and offers guardrails to guide our judgment. Just as we talk with our customers about product development, we also talk about their expectations around privacy. They've told us explicitly that they expect us to be stewards of their data, using it responsibly and with integrity, for their benefit, while keeping it private and secure.

The central concept of Data Stewardship is that it is the customers' data, not ours. Because we hold their most sensitive data, customers place a deep trust in us. Our customers have told us this directly through our extensive, consumer research. They care deeply how their data is used, they want clear and open explanations and to have contextual, relevant choices about those uses. They expect us to be accountable to keep our promises. Ethical data stewardship increases customers' confidence and trust.

To ensure that our nearly 8,000 employees are clear about how we manage and respect information entrusted to us, we have created a set of company-wide data stewardship principles.[1] These principles, derived directly from Intuit's core operating values—especially Integrity without Compromise—are intended to guide our mindset and behavior in all that we do. They reflect and reinforce that we're an organization that is accountable for its actions.

Intuit's Data Stewardship Principles

When we apply our Data Stewardship Principles to leveraging data, they enable us to support Intuit's growth strategies while meeting and exceeding our customers' expectations about how we use their data to benefit them and run our business to provide the products and services that serve them.

We are and will be accountable for the information entrusted to us. By design, our Data Stewardship Principles align closely with globally recognized fair information practices, including those for online privacy developed in the late 1990s and to their originating concepts, the Organization for Economic Cooperation and Development (OECD) privacy principles. As we have learned, we believe these Principles carry the most weight and meaning to actual consumers, based on an extensive research process we will describe below.

As you think about comprehensive privacy legislation, we encourage you to focus on four things:

1. principles-based privacy
2. customers
3. data driven innovation
4. global uniformity

First, we see the value in comprehensive principles-based privacy legislation. We believe there is value in the idea of baseline, principle-based privacy legislation that could work in tandem with self-regulatory approaches and codes of conduct. The Intuit Data Stewardship Principles represent our own internal code of conduct for data. A principles-based approach is not prescriptive but enables flexibility to offer data driven solutions within existing sector-specific privacy laws and, most importantly, is technology-neutral.

A principle-based approach could fill the gaps and crevices that exist between the differing sector approaches, while at the same time blending with them. It is also more likely to be received and effectively adapted by businesses of all sizes, including small businesses not actively engaged in the privacy landscape. It is more likely to be understood by the public it seeks to protect. And a principle-based approach

[1] See Appendix A for a list of our Data Stewardship Principles.

is more likely to achieve consensus over time in the international context, which will be essential to global competitiveness in the emerging digital economy. Such an approach could set forth a minimum set of requirements for business, and provide a fundamental, core level of consistency for businesses and consumers. Codes of conduct, based on context, industry/sector, technology platform or other data use drivers would build on top of a privacy baseline. Codes of conduct can serve as the framework and support for co-regulatory safe harbor programs.

Second, any relevant data regime must be focused on the customer. As we enter this important discussion, it is necessary to further emphasize the importance of both respect for the consumer participation and control of information and the value and benefit of continued innovation, in particular where the future of economic growth is going—data driven innovation. The key to our success and to ensuring balance among these interests is earning the customers' trust.

At Intuit, customers are at the heart of everything we do. We were founded on the idea of customer driven innovation, a mindset and methodology to uncover important, unsolved problems. Many companies talk about customer focus, customer innovation, but the level of commitment to this, and the rigor we put behind it, differentiates us.

For nearly thirty years, our passion for inventing products to solve important problems and perfecting those products to delight our customers, through direct customer feedback and observation, has made Intuit the first choice in financial software for consumers and small businesses. We have an instituted practice within our Corporation called "follow me homes" in which representatives from the Corporation spend a few hours with our customers to not only receive feedback on our products but to also identify key customer needs to amend our product. The Corporation commits to over 10,000 employee hours of "follow me homes" per year—with our CEO committing to approximately sixty hours per year himself. We supplement "follow-me-homes" with direct customer research, and by bringing customers into special "labs" or focus groups to evaluate and give feedback on the customer experience and usability of our products and services. Our respect for the customer is reflected in the policies and practices that have driven our business. Trusted data stewardship is central to that commitment and to our success.

The development of our Data Stewardship Principles is kept customers as our central focus: as our established practices suggest, we took our customers along with us on the journey to define our principles about the use of data in a way that reflects the needs, concerns and values of those customers. We took draft Data Stewardship Principles directly to our customers and asked them for their feedback, on both the concepts and words, on intent and practice, with real-world customer experience and expectations. Over the period of the last year alone, we conducted two rounds of quantitative, statistically valid surveys that cut across multiple customer bases and product lines to get feedback and learn if Data Stewardship and Privacy mattered to them, which principles and how much. We conducted four rounds of qualitative customer focus group sessions to dive deeper into the subtleties of transparency, choice, data use cases and security.

Staying true to customer driven innovation, we iterated and refined the Data Stewardship Principles over the course of the customer research process. After several rounds of input and iteration, the Principles have been extremely well received. Let me share some of the insights from the more than 100 consumers and small businesses we talked to in focus groups:

- Customers may not read privacy policies but care deeply about how their data is used.
- Consumers are smarter than some give them credit for—they are aware of a wide range of data uses, to benefit them directly and for necessary internal business operations.
- While a majority of our customers already have a positive impression of Intuit, the Data Stewardship Principles further build trust.
- Across all research studies, the principle around not selling or sharing personal data is the most important.
- The more transparent (meaning open, simple and clear) the company is, the more customer trust increases and the customers' need for detailed and frequent or repetitive choice mechanisms appears to decrease.
- Training employees to uphold these principles is also important to customers and adds an incremental level of trust that we will deliver against our promises.

Here are a few illustrative verbatim statements from our customers that show what Intuit's Data Stewardship Principles mean to them:

- *"This is what makes customers trust them. I like that privacy is paramount & do believe they're committed to this."*—Mike, consumer in San Diego
- *"Customer focused, protecting my data and interests, holding themselves accountable." "I like that these principles are very specific. There is no doubt, or any way to not understand exactly how Intuit intends to treat my information. I like that."*—Jackie, small business owner in Oakland
- *"Because of these principles, I will continue to use their products."*—Darryl, consumer in Denver
- *"A little safer in an unsafe world."*—Erica, consumer in Atlanta

When customers participate directly in the shaping of Data Stewardship Principles, it brings to life the Fair Information Practice concepts of Transparency and Individual Participation in profound ways.

Specifically, we have learned through this process what is substantive and meaningful to consumers.

Third, responsible data use can foster innovation. The world is quickly shifting from a paper-based, human-produced, brick-and-mortar-bound market to one where people understand, appreciate and embrace the benefits of truly connected software, platforms and services.

Consumers' expectations have changed as people are increasingly conducting their lives online. 'Cloud computing' makes it easier to access and use online sites anytime and anywhere an individual chooses. Consumers expect to interact online in an "always on" environment and to have technology make life easier. They demand even greater simplicity, such as not having to re-enter their data when they use more than one of our products or services. Increasingly, new products and services as well as enhancements to existing ones will employ more and more sophisticated, rich, real-time interactive use of data, directed and prompted by customer actions and expectations of product functionality.

The volume and complexity of data in this new world present boundless opportunities to unlock a tremendous amount of data to create better experiences and products for customers, all while keeping our customers' data safe.

Intuit's approach to data driven innovation is to responsibly use data entrusted to us by our customers to improve their financial lives and the products and services we provide them. This data includes information about our customers—who they are, where they are and how they use our products. By compiling and interpreting this data, we can create innovative, easy-to-use products that delight customers by helping them make and save money. We're also able to provide customers with information that gives them greater insight into their financial lives and helps them to achieve their personal and business goals.

To retain consumer trust in that context, Intuit's vision is that privacy and security are central to the concept of customer "delight," and therefore serve as a competitive advantage.

For innovation to thrive, we must unlock the power of data under a Data Stewardship regime. The essence of Data Stewardship cannot rely on just one element of our principles, it must be comprised of all of them combined: customer driven innovation coupled with responsible, innovative, and compelling data uses. Moreover, as global competitiveness evolves beyond the bricks-and-mortar economies of the past, and international trade takes on an electronic character in the economy of the future, sound business practices and wise public policy are critical components of innovation, invention, and full, fair and open competition.

Last but not least, legislation must take into account the need for uniformity among various privacy regimes. While so many laws and regulations are based on essentially the same principles, multi-state and multi-national companies are challenged by the differences among them. Some regulations in breach notification, for example, require notification of some state agencies; others do not. The notification triggers and thresholds are different. And the definitions of important terms vary across the landscape.

In a domestic context, we support a uniform Federal breach notification law. Aligning practices across states would provide benefits for consumers who purchase from merchants in other states. It would also lessen the complexity for merchants, a consistent goal in improving the economy.

In an international context, baseline principles that align with the Asia-Pacific Economic Coordination (APEC) Privacy Principles and the E.U. Directive would improve multi-national commerce, allowing the freer-flow of transactions and data across borders, in a consistent trusted manner. This, in turn, would improve the U.S. economy through vibrant trade. Intuit agrees that the U.S. Government should continue to work toward increased cooperation among privacy enforcement authorities around the world and develop a framework for mutual recognition of other

countries' frameworks. Intuit agrees that the U.S. should also continue to support the APEC Privacy Principles Pathfinder Project, because it is the best framework to achieve data privacy interoperability in the 21st century.

Conclusion

Once again, Mr. Chairman, Senator Hutchison, members of the Committee, thank you again for giving Intuit the opportunity to express its thoughts on this important subject. Maintaining customers trust is the foundation to building privacy principles. It is with this trust that we will learn from the customers about what they really want and what is important to them when it comes to their data. In the 21st century, customers demand more in a connected world. We must work toward the shared goal of protecting consumers while maintaining data driven innovation to improve our customers' financial lives, in a trusted, real, and fundamental way.

We look forward to working with you and the Committee toward this goal.

APPENDIX A

Intuit Data Stewardship Principles

What we stand for:

- Our customers' privacy (and their customers' and employees') is paramount to us.
- Our customers place a deep trust in Intuit because we hold their most sensitive data . . . therefore, we are a trusted steward of their data.
- Our company values start with Integrity without Compromise, and our privacy principles require that we all be accountable.

How we run our business (what we hold ourselves accountable to):

We will not:

- Without explicit permission, sell, publish or share data entrusted to us by a customer that identifies the customer or any person.

We will:

- Use customer data to help our customers improve their financial lives. We help them make or save money, be more productive, and comply with laws and regulations.
- Use customer data to operate our business, including helping our customers improve their user experience and understand the products and services that are available to help them.
- Give customers choices about our use of data that identifies them.
- Give open and clear explanations about how we use data.
- Publish or share combined, unidentifiable customer data, but only in a way that would not allow the customer or any person to be identified.
- Train our employees about how to keep data safe and secure, and educate our customers about how to keep their and their customers' data safe and secure.

Senator KERRY. Thank you, Ms. Lawler.

Mr. Calabrese?

STATEMENT OF CHRISTOPHER R. CALABRESE, LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION, WASHINGTON LEGISLATIVE OFFICE

Mr. CALABRESE. Thank you, Chairman Kerry, members of the Committee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union. We support comprehensive protections for American's personal information including a Do Not Track mechanism.

One of the new models of Internet advertising has been to target ads at the specific individual in order to make those ads more relevant. The result has been a system where Americans are routinely tracked as they surf the Internet. Americans assume there is no

central record of what they do and where they go online. However in many instances that is no longer the case.

Behavioral marketers, social networks and other online companies are creating profiles of unprecedented depth and breadth that reveal the personal aspects of our lives including our religious and political beliefs, medical information, purchases and reading habits. These profiles can legally be shared with anyone including offline companies, employers and the government. This data collection is neither benign nor anonymous.

Individual profiles identify our mental health, sexual orientation or issues with weight. They may indicate particular vulnerabilities.

Ninety-two-year-old veteran, Richard Guthrie was bilked out of more than $100,000 by criminals who identified him from marketing lists.

Cate Reid, a recent high school graduate has been identified by advertisers as concerned about her weight. "Every time I go on the Internet," she says, she sees weight loss ads. "I'm self-conscious about my weight. I try not to think about it. Then the ads start me thinking about it."

Information that can be used for identity theft is online but beyond our control. One reporter asked a company to search out information on her armed only with her name and e-mail address. She said. "Within 30 minutes the company had my social security number. In 2 hours they knew where I lived, my body type, my hometown, my health status."

Nor are individual web surfing habits anonymous. Many companies now provide a way to directly link your name and mailing address to your web surfing habits. Companies know who you are online. All of this information is available for sale with no controls.

Of particular concern, of course to the ACLU, is government access. Many civil liberties benefits of the Internet, ability to read provocative materials, associate with non-mainstream groups, voice dissenting opinions are based on the assumptions of practical anonymity and freedom from government scrutiny. Because of this information collections these assumptions are rapidly eroding.

Law enforcement routinely purchases access to offline private data bases full of detailed profiles on each of us with no legal process. They could legally do the same with online information. In fact online and offline data bases of personal information are increasingly linked. But we have no right to access those same data bases or control how they're used.

Solutions exist. The technology may be new but the problems are not. Congress and the states have passed many laws to protect Americans reading habits and viewing habits in the offline world. More than 30 years ago the U.S. Department of Health, Education and Welfare crafted basic privacy principles. Called the Fair Information Practice Principles they have become the basis for comprehensive privacy laws in many industrialized nations as well as sector specific laws in the United States.

The Department of Commerce recently called for adoption of these principles for the Internet. We endorse the use of fair information practices as well. In addition the private sector is developing innovative solutions like a Do Not Track mechanism.

These mechanisms need to be backed by the force of law. We reject any approach that relies solely on self regulation by companies. Self regulation by itself is a failed approach. It has allowed the current data collection practices to flourish.

Consumers want change. Surveys show that 67 percent rejected the idea that advertisers should be able to match ads based on specific websites consumers visit. And 61 percent believe these practices were not justified even if they kept costs down and allowed consumers to visit websites for free.

Ultimately if this information collection is allowed to continue unchecked then capitalism could build what the government never could, a complete surveillance state online. Without government intervention we may soon find the Internet has been transformed from a library and a playground to a fish bowl. And that we have unwittingly seeded core values of privacy and autonomy.

Thank you.

[The prepared statement of Mr. Calabrese follows:]

PREPARED STATEMENT OF CHRISTOPHER R. CALABRESE, LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION, WASHINGTON LEGISLATIVE OFFICE

Good morning Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU) its more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide, about the importance of online privacy. We support comprehensive protections for Americans' personal information and specifically support a "Do Not Track" option for online consumers. These protections are crucial for preventing harm to consumers and to safeguard Americans' First and Fourth Amendment rights online.

I. Introduction

Rapid technological advances and the lack of an updated privacy law have resulted in a system where Americans are routinely tracked as they surf the Internet. The result of this tracking—often performed by online marketers—is the collection and sharing of Americans' personal information with a variety of entities including offline companies, employers and the government. As greater portions of our lives have moved online, unregulated data collection has become a growing threat to our civil liberties.

As one recent report explains, the Internet has been an engine of radical, positive changes in the way we communicate, learn, and transact commerce.[1] The Internet allows us to connect to one another and share information in ways we never before could have imagined. Many of the civil liberties benefits of the Internet—the ability to access provocative materials more readily, to associate with non-mainstream groups more easily, and to voice opinions more quickly and at lower cost—are enhanced by the assumption of practical anonymity. Similarly, consumers are largely unaware of the breadth of information collection and the various uses to which it is put.

In short, Americans assume that there is no central record of what they do and where they go online. However in many instances that is no longer the case. Behavioral marketers are creating profiles of unprecedented breadth and depth that reveal personal aspects of people's lives including their religious or political beliefs, medical information, and purchase and reading habits. Even as behavioral targeting continues to grow, its practitioners have already demonstrated a disturbing ability to track and monitor an individual's actions online.

If this collection of data is allowed to continue unchecked, then capitalism will build what the government never could—a complete surveillance state online. Without government intervention, we may soon find the Internet has been transformed from a library and playground to a fishbowl, and that we have unwittingly ceded core values of privacy and autonomy.

---

[1] Federal Trade Commission (Bureau of Consumer Protection), *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, December 1, 2010.

II. Americans have embraced technology, but they still expect privacy

Technology has moved rapidly and Americans have adopted these changes into their lives:

- Over 50 percent of American adults use the Internet on a typical day.[2]
- 62 percent of online adults watch videos on video-sharing sites,[3] including 89 percent of those aged 18–29.[4]
- Over 70 percent of online teens and young adults[5] and 35 percent of online adults have a profile on a social networking site.[6]
- 83 percent of Americans own a cell phone and 35 percent of cell phone owners have accessed the Internet via their phone.[7]

Companies continue to innovate and create new ways for Americans to merge technology with daily activities. Google has spent the last 5 years building a new online book service and sales of digital books and devices have been climbing.[8] Americans increasingly turn to online video sites to learn about everything from current news to politics to health.[9] Location-based services[10] are also a burgeoning market.[11]

However this rapid adoption of new technology has not eliminated Americans' expectations of privacy. To the contrary, Americans still expect and desire that their online activities will remain private, and express a desire for laws that will protect that privacy:

- 69 percent of Internet users want the legal right to know everything that a Website knows about them.[12]
- 92 percent want the right to require websites to delete information about them.[13]

And consumers oppose online tracking:

- 67 percent rejected the idea that advertisers should be able to match ads based on specific websites consumers visit;[14] and

---

[2] Common daily activities include sending or receiving e-mail (40+ percent of all American adults do so on a typical day), using a search engine (35+ percent), reading news (25+ percent), using a social networking site (10+ percent), banking online (15+ percent), and watching a video (10+ percent). Pew Internet & American Life Project, *Daily Internet Activities, 2000–2009, http://www.pewinternet.org/Trend-Data/Daily-Internet-Activities-20002009.aspx*.

[3] A "video-sharing site" or "video hosting site" is a website that allow users to upload videos for other users to view (and, often, comment on or recommend to others). Wikipedia, *Video Hosting Service, http://en.wikipedia.org/wiki/Video_sharing* (as of January 21, 2011). YouTube is the most common video-sharing site today.

[4] Pew Internet & American Life Project, *Your Other Tube: Audience for Video-Sharing Sites Soars*, July 29, 2009, *http://pewresearch.org/pubs/1294/online-video-sharing-sites-use*.

[5] Pew Internet & American Life Project, Social Media & Young Adults, Feb. 3, 2010, *http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx*.

[6] "Social networking sites" allow users to construct a "semi-public" profile, connect with other users of the service, and navigate these connections to view and interact with the profiles of other users. Danah M. Boyd & Nicole B. Ellison, *Social Networking Sites: Definition, History, and Scholarship*, 13 J. of Comp.-Mediated Comm. 1 (2007); Pew Internet & American Life Project, *Adults & Social Network Sites*, Jan. 14, 2009, *http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx*.

[7] Pew Internet & American Life Project, *Internet, Broadband, and Cell Phone Statistics*, Jan. 5, 2010, *http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx*.

[8] *See generally* ACLU of Northern California, *Digital Books: A New Chapter for Reader Privacy*, Mar. 2010, *available at http://www.dotrights.org/digital-books-new-chapter-reader-privacy*.

[9] "More Americans are watching online video each and every month than watch the Super Bowl once a year.." Greg Jarboe, "125.5 Million Americans Watched 10.3 Billion YouTube Videos in September," *SearchEngineWatch.com*, Oct. 31, 2009, *http://blog.searchenginewatch.com/091031–110343*.

[10] "Location-based services" is an information service utilizing the user's physical location (which may be automatically generated or manually defined by the user) to provide services. Wikipedia, *Location-Based Service, http://en.wikipedia.org/wiki/Location-based_service* (as of January 21, 2011).

[11] Recent location-based service Foursquare built a base of 500,000 users in its first year of operation. Ben Parr, "The Rise of Foursquare in Numbers [STATS]," *Mashable*, Mar. 12, 2010, *http://mashable.com/2010/03/12/foursquare-stats/*.

[12] Joseph Turow, *et al., Americans Reject Tailored Advertising* 4 (2009), available at *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214*.

[13] *Id.*

[14] Lymari Morale, "U.S. Internet Users Ready to Limit Online Tracking for Ads," *USA TODAY*, December 21, 2010.

- 61 percent believed these practices were not justified even if they kept costs down and allowed consumers to visit websites for free.[15]

In sum, while Americans make great use of the Internet, they are very concerned about their privacy and specifically troubled by the practice of behavioral targeting.

III. The data collected by behavioral marketers forms a personal profile of unprecedented breadth and depth

Behavioral targeting contravenes many American's expectation of privacy and how they should be treated online. Online advertising is one of the fastest growing businesses on the Internet and it is based on collecting a staggering amount of information about people's online activities. Advertising has always been prevalent online, but instead of targeting websites—such as advertising shoes on a shoe store site—advertisers now use personal information to target individuals directly.

They do this using different surveillance tools. The simplest tools are cookies. A cookie is a file that a website can put on a user's computer when the user visits it so that when the user returns, or visits another affiliated site, it remembers certain information about the user. Cookies were initially used to help websites remember user passwords or contents in shopping bags, but as online marketing grew more sophisticated, cookies did too. Advertisers and aggregators modified cookies to track people's web page visits, searches, online purchases, videos watched, posts on social networking, and so on.

Another popular and even more invasive tool for tracking is the flash cookie. Flash cookies are often used by data aggregators to re-install a regular cookie that a user had detected and deleted. The newest and most aggressive form of tracking is the beacon. Beacons, also known as web bugs, are often used by sites that hire third party services to monitor user actions. These devices can track a user's movements extremely closely; to the point that they can monitor keystrokes on a page or movements by a user's mouse. The result of these practices is the collection and sale of a wealth of consumer data without any legal limits or protections for individuals.

As targeted ads become increasingly profitable, behavioral marketers are growing more ambitious and seeking to form an even more complete picture of unsuspecting citizens. The *Wall Street Journal* recently conducted a comprehensive study on the effects of online marketing on individual privacy and the results were alarming. The study found that the Nation's 50 top websites installed an average of 64 pieces of tracking technology on user's computers, usually with no warning. A dozen sites installed over a hundred. For example, the study found that Microsoft's popular website, MSN.com, attached a tracking device that identified and stored user's detailed personal information. According to the tracking company that created the file, it could predict a user's age, zip code, and gender, as well as an estimate of a user's income, marital status, family status and home ownership status.[16] These new technologies allow marketers to combine a vast amount of information gleaned from different websites over time in order to paint an extremely detailed profile of potential consumers. Any particular website may have little information and this may not alarm some, but when a large number of these data points are aggregated, an extremely detailed picture results.

In addition, the *Wall Street Journal* found that tracking technology has become so advanced and covert that the website owner is often not even aware of its presence. Microsoft, one of the largest developers of computer software in the world, said it did not know about the tracking devices on its site until informed by the *Journal*.[17] If these technologies have become as surreptitious as to slip past sophisticated website owners, it is completely unreasonable to believe that the average user would be able to avoid their spying.

IV. Identifying individuals and the merger of online and offline identity

Online and offline data companies are combining forces to get an even more detailed profile of consumers and further erode privacy. For example, Comscore, a leading provider of website analytic tools, boasts that "online behavioral data can . . . be combined with attitudinal research or linked with offline databases in order to diagnose cross-channel behavior and streamline the media planning process."[18]

In another example, the data firm Aperture has made the connection between online and offline identities by collecting data from offline data companies like

---

[15] *Id.*

[16] Angin Win, "The Web's New Gold Mine: Your Secrets," *Wall Street Journal*, July 30, 2010.

[17] *Id.*

[18] Why Comscore?, *http://comscore.com/About__comScore/Why__comScore* (last visited January 21, 2011).

Experian or Nielsen's Claritas and then combining it with a huge database of e-mail addresses maintained by its parent company, Datran Media.[19] According to media reports, many major companies are working with Aperture.[20] "The line between merging online and offline data isn't no-man's land anymore; it's becoming more of a common practice," said Mike Zaneis, Washington lobbyist for the Interactive Advertising Bureau."[21] A variety of services offer to merge names and postal addresses with collected IP and e-mail addresses.[22]

To be clear: *such a merger of data is only possible when consumers are specifically identified.* As described above, markets are using personal identifiers like e-mail addresses to connect online browsing habits to offline information from other databases. One venture capitalistic described it to the *Wall Street Journal:* "They're trying to find better slices of data on individuals," says Nick Sturiale, a general partner at Jafco Ventures, which has largely avoided the sector. "Advertisers want to buy individuals. They don't want to buy [Web] pages."[23] You can only "buy individuals" when you know who they are.

V. Regulation of behavioral targeting does not threaten the "Free Internet"

The ACLU believes the Internet is the most advanced marketplace of ideas and one of the greatest tools ever created for advancing American's First Amendment rights. We would never endorse any regulation that endangered the robustness and variety of this medium. Laws protecting personal information and those that would create a "Do Not Track" mechanism would not harm the Internet or end the provision of free products or services.

Behavioral targeting is different than "contextual advertising," another type of online ad service which shows ads to users based on the content of the web page they are currently viewing or the web search they have just performed. When this pairing of ads to users' interests is based only on a match between the content of an ad and a single page or search term, a website or advertising network requires no personal information about a user beyond an IP address. The practice does not raise significant privacy concerns.

Nor would commonsense regulations necessarily foreclose the use of consumer data as part of advertising and services. For example, a consumer may want to allow significant data collection by websites with whom they already have a relationship. Companies like Google and Amazon gather information that has demonstrable benefit to the consumer—by providing book recommendations or easy-to-use maps. Consumers may welcome targeted ads when they feel in control of their own information or may consider it a fair tradeoff for other goods or services.

Content has been supported for years (and in many cases for decades and even centuries) through advertising without the need for detailed targeting and tracking of consumers. But studies have demonstrated that the vast majority of the revenue from tracking consumers online goes not to content providers but rather to the behavioral targeters themselves. Industry sources say that 80 percent of the revenue from targeting—4 in 5 dollars—went to create and enhance the targeting system, not to publishers.[24] Major publishers like the *New York Times* have endorsed a "Do Not Track" mechanism—clearly they are not concerned that such a mechanism will harm their ad revenue.[25]

VI. Access to extensive personal profiles threatens personal privacy and the First and Fourth Amendment

It is no exaggeration to say that data profiles—which may combine records of a person's entire online activity and extensive databases of real-world, personally identifiable information—draw a personal portrait unprecedented in scope and detail. Because the Internet has become intertwined with so many personal facets of our lives, the same technology that has provided such tremendous advances also creates the possibility of tremendous intrusion by companies and the government.

---

[19] Michael Learmonth, "Holy Grail of Targeting is Fuel for Privacy Battle," *Advertising Age*, March 22, 2010.

[20] *Id.*

[21] *Id.*

[22] *See: http://biz.freshaddress.com/RealTimePostalAppend.aspx.* For a long list of their clients please *see: http://biz.freshaddress.com/ClientsByName.aspx*.

[23] Scott Thrum, "Online Trackers Rake in Funding," *Wall Street Journal,* February 25, 2011 at: *http://online.wsj.com/article/SB10001424052748704657704576150191661959856.html#ixzz1FYWLkEWm*.

[24] The Jordan Edmiston Group, *M&A Overview and Outlook*, Slide 13, can be found at: *http://www.jegi.com/files/docs/IABMIXX.pdf*.

[25] "Protecting Online Privacy," *New York Times*, December 4, 2010.

i. Non-governmental actors

The harms caused by excessive and invasive data collection are real and pressing. They begin with straightforward invasions of privacy. Should anyone have the right to know and sell to others the fact that you are overweight, or depressed, or gay?[26] These are all commonplace occurrences with marketers and social networking sites routinely making and selling these determinations. They have significant consequences for consumers who have no say in the collection and use of their own information. As the *Wall Street Journal* explains:

> Yahoo's network knows many things about recent high-school graduate Cate Reid. One is that she is a 13- to 18-year-old female interested in weight loss. Ms. Reid was able to determine this when a reporter showed her a little-known feature on Yahoo's website, the Ad Interest Manager, that displays some of the information Yahoo had collected about her.
>
> Yahoo's take on Ms. Reid, who was 17 years old at the time, hit the mark: She was, in fact, worried that she may be 15 pounds too heavy for her 5-foot, 6-inch frame. She says she often does online research about weight loss.
>
> "Every time I go on the Internet," she says, she sees weight-loss ads. "I'm self-conscious about my weight," says Ms. Reid, whose father asked that her hometown not be given. "I try not to think about it. . . . Then [the ads] make me start thinking about it."[27]

This tracking is ubiquitous around the Internet with tracking technology on 80 percent of 1,000 popular sites, up from 40 percent of those sites in 2005.[28]

In the information age knowledge is power and personal information can be used for many other purposes. A data-mining firm called Rapleaf has said it can make determinations about creditworthiness and whether someone will be a good customer.[29] A defense attorney attempted to access the social networking pages of two teens in order to prove they were appropriately denied health care.[30] One employer demanded access to its employee's private Facebook account as part of a background check.[31]

When information escapes a consumer's control, it gives power to others to make decisions about them that have real consequences for their lives. In addition, the lack of control and transparency surrounding consumer personal information harms not just consumers but the Internet as a whole. Uncertainty over the use or misuse of information by third parties retards the adoption of new technologies and makes consumers more anxious about revealing personal information.

Personal information can also reveal weaknesses that unscrupulous actors can exploit. Ninety-two year old veteran Richard Guthrie was bilked out of more than $100,000 by criminals who identified him from marketing lists.[32] InfoUSA routinely advertised lists of:

> "Elderly Opportunity Seekers," 3.3 million older people "looking for ways to make money," and "Suffering Seniors," 4.7 million people with cancer or Alzheimer's disease. "Oldies but Goodies" contained 500,000 gamblers over 55 years old, for 8.5 cents apiece. One list said: "These people are gullible. They want to believe that their luck can change."[33]

---

[26] *See* Testimony of Pam Dixon *The Modern Permanent Record and Consumer Impacts from the Offline and Online Collection of Consumer Information,* Before the Subcommittee on Communications, Technology, and the Internet, and the Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce November 19, 2009 at *http://www.worldprivacyforum.org/pdf/TestimonyofPamDixonfs.pdf*; Brett Michael Dykes, "Latest Facebook privacy outrage: ad data outing gay users," *The Upshot,* October 22, 2010 at: *http://news.yahoo.com/s/yblog__upshot/20101022/bs__yblog__upshot/latest-facebook-privacy-outrage-ad-data-outing-gay-users*.

[27] Win article.

[28] *Id.*

[29] Lucas Conley, "How Rapleaf Is Data-Mining Your Friend Lists to Predict Your Credit Risk," *FAST COMPANY* November 16, 2009 at *http://www.fastcompany.com/blog/lucas-conley/advertising-branding-and-marketing/company-we-keep*.

[30] Mark Stein, "Facebook Page? Or Exhibit A in Court?," *Portfolio.com,* February 5, 2008 *http://www.portfolio.com/views/blogs/daily-brief/2008/02/05/facebook-page-or-exhibit-a-in-court/*.

[31] Matt Liebowitz "Boss Demands Employee's Facebook Password," *MSNBC.com*, March 1, 2011 *http://www.msnbc.msn.com/id/41743732/ns/technology__and__science-security/*.

[32] Charles Duhigg, "Bilking the Elderly, With a Corporate Assist," *New York Times*. May 20, 2007 *http://www.nytimes.com/2007/05/20/business/20tele.html?__r=2*.

[33] *Id.*

In other cases thieves purchased access to databases of Americans' personal information and used that information to commit identity theft.[34]

Collection of personal information online turbo-charges this process. One reporter asked a company to search out information about her online. She disclosed that, armed only with her name and e-mail address, "Within 30 minutes, the company had my Social Security number; in 2 hours, they knew where I lived, my body type, my hometown, and my health status."[35]

ii. Governmental actors

As their contracts with the data aggregator industry demonstrate, government and law enforcement agencies have also found these personal data profiles irresistible. In 2006 the *Washington Post* reported that the Federal Government and states across the country have developed relationships with private companies that collect personal information about millions of Americans, including unlisted cell phone numbers, insurance claims, driver's license photographs, and credit reports through private data aggregators including Accurint, Entersect and LexisNexis. In fact, Entersect boasts that it is "the silent partner to municipal, county, state, and Federal justice agencies who access our databases every day to locate subjects, develop background information, secure information from a cellular or unlisted number, and much more."[36]

The Central Intelligence Agency (CIA), via its investment arm In-Q-Tel, has invested in a software company that specializes in monitoring blogs and social networks[37] and the Department of Defense, the CIA, and the Federal Bureau of Investigation (FBI) have all purchased use of private databases from Choicepoint, one of the largest and most sophisticated aggregators of personal data.[38] In the words of the FBI, "We have the legal authority to collect certain types of information" because ChoicePoint is "a commercial database, and we purchase a lot of different commercial databases. . . . They have collated information that we legitimately have the authority to obtain."[39]

The government has demonstrated an increasing interest in online user data in other ways as well. In 2006 the Department of Justice (DOJ) subpoenaed search records from Google, Yahoo!, and other search providers in order to defend a lawsuit.[40] In 2007, Verizon reported receiving 90,000 requests per year and in 2009, Facebook told *Newsweek* it was getting 10 to 20 requests each day. In response to increasing privacy concerns, Google started to publish the number of times law enforcement asked for its customers' information and reported over 4,200 such requests in the first half of 2010 alone. In the words of Chris Hoofnagle, a senior fellow at the Berkeley Center for Law and Technology, "These very large data bases of transactional information become honey pots for law enforcement or for litigants."[41] Given the government's demonstrated drive to access both online data and commercial data bases of personal information, it seems nearly certain that law enforcement and other government actors will purchase or otherwise access the type of detailed profiles of online behavior compiled by behavioral marketers.

Our First Amendment rights to freedom of religion, speech, press, petition, and assembly are based on the premise that open and unrestrained public debate empowers democracy by enriching the marketplace with new ideas and enabling political and social change through lawful means. The Fourth Amendment shields private conduct from unwarranted government scrutiny. Together the exercise of these rights online has allowed the Internet marketplace of ideas to expand exponentially.

---

[34] Federal Trade Commission, "ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress," January 26, 2006. *http://www.ftc.gov/opa/2006/01/choicepoint.shtm*.

[35] Jessica Bennett, "What the Internet Knows about You," *Newsweek*, October 22, 2010. *http://www.newsweek.com/2010/10/22/forget-privacy-what-the-internet-knows-about-you.html*.

[36] O'Harrow Jr Robert, Centers Tap into Personal Databases, *Washington Post*, April 2, 2008.

[37] Noah Shactman, "U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets," *Wired*, October 19, 2009 at *http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm*.

[38] Shane Harris, "FBI, Pentagon Pay For Access to Trove of Public Records," *National Journal*., Nov. 11, 2005 at *http://www.govexec.com/story—page.cfm?articleid=32802*; Robert O'Harrow Jr., "In Age of Security, Firm Mines Wealth Of Personal Data," *Washington Post*, January 20, 2005, at *http://www.washingtonpost.com/wp-dyn/articles/A22269–2005Jan19.html*.

[39] Harris, *supra* n. 16 (quoting FBI spokesman Ed Cogswell).

[40] Hiawatha Bray, "Google Subpoena Roils the Web, U.S. Effort Raises Privacy Issues," *Boston Globe*, January 21, 2006 at *http://www.boston.com/news/nation/articles/2006/01/21/google__subpoena__roils__the__web/*.

[41] Miguel Helft, "Google Told to Turn Over User Data of Youtube," *New York Times*, July 4, 2008 at *http://www.nytimes.com/2008/07/04/technology/04youtube.html*.

Courts have uniformly recognized that government requests for records of which books, films, or other expressive materials individuals have received implicate the First Amendment and trigger exacting scrutiny.[42] These cases are grounded in the principle that the First Amendment protects not only the right of individuals to speak and to express information and ideas, but also the corollary right to receive information and ideas through books, films, and other expressive materials.[43] Within this protected setting, privacy and anonymity are vitally important. Anonymity "exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular," because, among other things, it serves as a "shield from the tyranny of the majority."[44] An individual may desire anonymity when engaging in First Amendment activities—like reading, speaking, or associating with certain groups—because of "fear of economic or official retaliation, . . . concern about social ostracism, or merely . . . a desire to preserve as much of one's privacy as possible."[45]

The Supreme Court has also recognized that anonymity and privacy are essential to preserving the freedom to receive information and ideas through books, films, and other materials of one's choosing. For example, in *Lamont* v. *Postmaster General,* the Court invalidated a postal regulation that required the recipient of "communist political propaganda" to file a written request with the postmaster before such materials could be delivered.[46] The regulation violated the First Amendment because it was "almost certain to have a deterrent effect . . . Any addressee [was] likely to feel some inhibition" in sending for literature knowing that government officials were scrutinizing its content.[47] Forced disclosure of reading habits, the Court concluded, "is at war with the 'uninhibited, robust, and wide-open' debate and discussion that are contemplated by the First Amendment."[48]

These words ring equally true today in the Information Age, with the prevalence of the Internet and other new technologies. Although these technological advances provide valuable tools for creating and disseminating information, the unprecedented potential for government and companies to store vast amounts of personal information for an indefinite time poses a new threat to the right to personal privacy and free speech. In *In re Grand Jury Subpoena to Amazon.com,* the district court recognized this reality in holding that a grand jury subpoena to Amazon requesting the identities of buyers of a certain seller's books raised significant First Amendment concerns.[49] The court explained its concern over the chilling effect that would flow from enforcing such a subpoena in the age of the Internet, despite its confidence in the government's good-faith motives:

> [I]f word were to spread over the Net—and it would—that [the government] had demanded and received Amazon's list of customers and their personal purchases, the chilling effect on expressive e-commerce would frost keyboards across America. Fiery rhetoric quickly would follow and the nuances of the subpoena (as actually written and served) would be lost as the cyber debate roiled itself to a furious boil. One might ask whether this court should concern itself with blogger outrage disproportionate to the government's actual demand of Amazon. The logical answer is yes, it should: well-founded or not, rumors of an Orwellian Federal criminal investigation into the reading habits of Amazon's customers could frighten countless potential customers into canceling planned online book purchases, now and perhaps forever. . . . Amazon . . . has a legitimate concern that honoring the instant subpoena would chill online purchases by Amazon customers.[50]

The Internet is, and must remain, the most open marketplace of ideas in the history of the world. In order to guarantee this, we must provide consumers with the tools they need to control their personal information and meaningful mechanisms

---

[42] *In re Grand Jury Subpoena to Kramerbooks & Afterwords Inc.*, 26 Med. L. Rptr. 1599, 1600–01 (D.D.C. 1998) (Dkt. No. 21, Ex. B) (requiring government to show compelling interest and a sufficient connection between its investigation and its request for titles of books purchased by Monica Lewinsky); *Tattered Cover, Inc.* v. *City of Thornton*, 44 P.3d 1044, 1053 (Colo. 2002) (holding that search of bookseller's customer purchase records necessarily intrudes into constitutionally protected areas).

[43] *See, e.g., Va. State Bd. of Pharmacy* v. *Va. Citizens Consumer Council*, 425 U.S. 748, 757 (1976) (right to receive advertisements); *Stanley* v. *Georgia*, 394 U.S. 557, 564 (1969) (films); *Bantam Books* v. *Sullivan*, 372 U.S. 58, 64 n.6 (1963) (books).

[44] *McIntyre* v. *Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995).

[45] *Id.* at 341–42.

[46] *Lamont* v. *Postmaster General*, 381 U.S. 301, 302 (1965).

[47] *Id.* at 307.

[48] *Id.* (quoting *New York Times Co.* v. *Sullivan*, 376 U.S. 254, 270 (1964)).

[49] 246 F.R.D. at 572–73

[50] *In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. at 573.

for assuring privacy and protecting the robust rights established by the Constitution.

VII. Solutions exist

Reasonable and workable solutions exist for grappling with the problems of excessive data collection. While the technology is new, the problem is not. As the preceding case law demonstrates, as a society we have always been concerned about problems like judging or attacking individuals based on their reading or viewing habits. That is why 48 states protect public library reading records by statute.[51] Congress has also recognized the privacy interests of users of expressive material and created strong protections in several other contexts. The Video Privacy Protection Act prohibits disclosure of video rental records without a warrant or court order.[52] The Cable Communications Policy Act similarly prohibits disclosure of cable records absent a court order.[53]

Moreover, more than 30 years ago the U.S. Department of Health, Education and Welfare (now the Department of Health and Human Services), crafted basic privacy principles to protect personal information.[54] Called the Fair Information Practice Principles (FIPPs), they have become the basis for comprehensive privacy laws in most of the industrialized world as well as sector specific privacy laws in the United States.[55] In 2008 the Privacy Office of the Department of Homeland Security formally adopted them in its analysis of DHS programs. And in a recent report, the Department of Commerce recommended that the FIPPs as described by DHS be adopted as the basis for Internet regulation.[56]

The FIPPs stand for eight relatively straightforward ideas:

- *Transparency:* Individuals should have clear notice about the data collection practices involving them.
- *Individual Participation:* Individuals should have the right to consent to the use of their information.
- *Purpose Specification:* Data collectors should describe why they need particular information.
- *Data Minimization:* Information should only be collected if it's needed.
- *Use Limitation:* Information collected for one purpose shouldn't be used for another.
- *Data Quality and Integrity:* Information should be accurate.
- *Security:* Information should be kept secure.
- *Accountability and Auditing:* Data collectors should know who has accessed information and how it is used.

While some adjustments will have to be made to conform to new technologies, international Internet data collection practices, as well as the data collection practices of other sectors of the U.S. economy, are already governed by the FIPPs.[57] To imply as some have done that application of these regulations in this case would cause serious harm to the Internet and e-commerce seems overstated at best.

These protections must be embodied in law, not just in industry practice. For years government agencies have called on industry to provide privacy protections for consumers. However, as a recent Federal Trade Commission report explains, self-regulatory efforts "have been too slow, and up to now have failed to provide ade-

---

[51] *See, e.g.,* N.Y. C.P.L.R. § 4509; Cal. Gov. Code §§ 6267, 6254(j). The two states that do not have library confidentiality laws are Hawaii and Kentucky. However, the Attorney Generals' Offices in each state have issued opinions in support of reader privacy. Haw. OIP Opinion Letter No. 90–30 (1990) (disclosure of library circulation records "would result in a clear unwarranted invasion of personal privacy"); Ky. OAG 82–149 (1982) ("all libraries may refuse to disclose for public inspection their circulation records. . . . [W]e believe that the privacy rights which are inherent in a democratic society should constrain all libraries to keep their circulation lists confidential.").

[52] 18 U.S.C. §§ 2710(b)(2)(C), 2710(b)(2)(F), 2710(b)(3).

[53] 47 U.S.C. § 551(h).

[54] For a brief history on the principles please *see* Robert Gellman, Fair Information Practices: A Basic History at *http://bobgellman.com/rg-docs/rg-FIPShistory.pdf*.

[55] *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, October 24, 1995; Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 *et seq.*

[56] Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, December 2010.

[57] *Id.*

quate and meaningful protection."[58] One example illustrates this fact well. In 1999 and 2000 when behavioral targeting first attracted regulatory attention, an industry group, the Network Advertising Initiative (NAI), claimed that self-regulation was a solution and that all NAI members would follow a common code of conduct.[59] As regulatory attention faded, so did participation in the NAI. By 2003 it had only two members. There is no reason to believe that things would be different now.

It is important to note that technology is already moving to help. Browser manufacturers are creating technical mechanisms so that web surfers can indicate their preference not to be tracked.[60] If given the force of law through the passage of a "Do Not Track" law, those mechanisms set a solid foundation for beginning to protect personal information online.

VIII. Conclusion

The current online data collection practices create detailed profiles on each of us. These practices are neither benign nor anonymous. They harm consumers and directly impact their fundamental rights. They are also unpopular—even when explicitly tied to the provision of free services. Good solutions exist and have been adopted in other countries and other parts of the U.S. economy. The Committee should look to these solutions like the "Do Not Track" mechanism and adopt legally enforceable rules to protect consumers and end this profiling.

Senator KERRY. Well that's a pretty far reach.

[Laughter.]

Senator KERRY. I mean it's a big concept. So I'm not suggesting you're reaching. It's just it's a big statement obviously about a potential downside.

It's just you, us and that's it. That's all that's left. I'm sorry.

[Laughter.]

Senator KERRY. But I want to probe a few things then we'll get you all out of here before too, too long, if I can.

So Mr. Calabrese, you've sort of drawn this potential danger picture, which is appropriate, in front of us. What's the appropriate response to that in your judgment?

Mr. CALABRESE. Well I mean we've heard a lot of great responses. I mean, I think we can begin with the Do Not Track mechanism which again, if backed by law gives people the opportunity to sort of opt-out of this state. It's not enough on its own.

Senator Kerry, the principles that you described, the ability to give consumers control over their information is vital to this as well. I think Do Not Track is a part of that. But it's also about sharing information collected by a first party. Just because I want a company to collect my information doesn't mean I want them to use it for everything. I may want to limit that. And that's——

Senator KERRY. Is there a balance here in your judgment between the obviously very important interest that you're highlighting and also the commercial, economic interest that we all have in maintaining the viability needed to save a growing enterprise?

Mr. CALABRESE. Oh, there absolutely is a balance. But we need to set—I'm sorry.

Senator KERRY. No, go ahead.

---

[58] Federal Trade Commission (Bureau of Consumer Protection), *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, December 1, 2010.

[59] World Privacy Forum, *Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation*, Fall 2007 at: *http://www.worldprivacyforum.org/pdf/WPF__NAI__report__Nov2__2007fs.pdf*.

[60] Julia Angwin, "Web Tool on Firefox to Deter Tracking," *Wall Street Journal*, January 24, 2011.

Mr. CALABRESE. There is a balance. My fear, candidly, is that right now there's no legal protection. And there's a great deal of incentive.

I mean Americans are some of the greatest businessmen and businesswomen in the world. If you give them an economic incentive and say there's an economic incentive to track people online. They will do a really good job of it.

So I think we need to put controls in place to make sure that the consumer is part of that process.

Senator KERRY. And how far do those controls have to go if the consumer has knowledge? I mean one of the problems is we've learned—I don't know if I have statistics here or not. I don't think I do.

But we have found historically that, you know, people consistently say well this is something I'm really super, super concerned about but then they tend to engage in practices on the Internet itself that sort of belie that a little bit.

Mr. CALABRESE. Sure. Well, I think part of that is they really haven't had meaningful choice up to this point. It's been sort of a take it or leave it approach. And so it's hard to expect people to invest time and energy in something——

Senator KERRY. I think that a lot of folks at the table would disagree that they don't have meaningful choice.

Mr. CALABRESE. Sure. I think they would. By all—but I mean the fact that I can't point to a law that says I control my personal information makes, you know, makes me—makes it hard for me to tell a consumer that they in fact, do have that control. I mean, a company's promises are important but not enough.

Senator KERRY. Who else? Anybody want to speak to that, sort of the balance?

Mr. ANDERSEN. I'm happy to speak to it for a moment.

Senator KERRY. Go ahead, Mr. Andersen.

Mr. ANDERSEN. Microsoft is obviously involved in online advertising. We also provide tools to consumers to help them protect themselves from activities that they may view as tracking and also spam and things like that as well. So we're sort of in a somewhat unique position of having to make sure that we're looking at both sides of the equation.

In the testimony that I submitted we did provide some statistics about the incredible growth of online advertising, and pointed out that it really is fueling a lot of the content available on the Internet today. I do think that it is important to make sure that that is kept in mind as one thinks about legislation.

At the same time consumer trust is incredibly important to our company. We know that users want to be in control of the data that is collected about them and how that data is used as well. And so we're endeavoring to make sure that they have the tools available to them to make sure that they are in control.

Senator KERRY. What does that mean, tools available to them?

Mr. ANDERSEN. What I mean by that? I'll give you an example from Internet Explorer browser. So we have this feature called Tracking Protection that we've introduced this week with Internet Explorer. It's available on the product. From the menu, you can select a feature called "tracking protection." And what that will——

Senator KERRY. Select that when you download it or do you select that every time it comes up? Is there an icon on your——

Mr. ANDERSEN. That's a good question. When you have installed the product there are menu items that are available to you to choose from.

Senator KERRY. Is that in the initial installation because I know sometimes when you download something you get a whole menu of initial installation, you know, some signs that shows up more than it does than other times. It can be more bold faced than other times. You can miss them sometimes.

I mean, how does it show up?

Mr. ANDERSEN. That's correct. It would not be part of your installation process. You wouldn't be asked to choose among different settings at the beginning of your installation process.

What you would do is after you've installed the product you would choose from the menu of different controls that you have to place.

Senator KERRY. Do you have to choose to go to the menu or does the menu show up automatically?

Mr. ANDERSEN. You'd have to choose the menu.

Senator KERRY. So you'd have to go to the menu.

Mr. ANDERSEN. Yes, you would.

Senator KERRY. It wouldn't be like a privacy warning, the original warnings where you have to sign up and say, I agree in order to proceed forward. There wouldn't be a stop, you can't proceed forward until you've answered it.

Mr. ANDERSEN. That's correct.

Senator KERRY. So a lot of people say, well, that's not really an in your face choice.

Mr. ANDERSEN. We understand that perspective, obviously. I think——

Senator KERRY. I mean I'm sure that when you really want to get somebody's attention you guys know how to do it.

[Laughter.]

Mr. ANDERSEN. We've been pretty successful at doing that, yes.

Senator KERRY. So, does this rise to that level or does it not?

Mr. ANDERSEN. Well, it's a good question. I think that what we found is that, you know, people want to experience the full Internet when they use a browser product. And they want to receive the personalization that they're able to get by using the full Internet. At the same time there's many people who want to have a choice and want to have tools available to them that are easy to access to the product to be able to——

Senator KERRY. No one is denying the choice. It's just a question of how boldly it's there. I mean, you know, as you said, you know how to get people's attention. Everybody does in the business. And things keep popping up and popping up and you've got to figure out how the hell to get them away sometimes.

And then there are things that don't pop up. And you can't find or they're harder to find. I think that's really at the center of this to some degree. There's got to be some sense of, you know, fair play and transparency and accountability in that.

Mr. ANDERSEN. Absolutely. It's absolutely a big part of the discussion is that at what point along the user experience should you be affirmatively giving users a choice to make a decision.

Senator KERRY. Let me ask a blunt question. And maybe Mr. Montgomery this is in your area and someone else at the table perhaps into it, I'm not sure. In fact before I ask that question let me come back to Intuit, if I can.

Intuit, you were commenting, Ms. Lawler, about the four principles that you apply. And they're admirable. They're terrific. And you talk about income tax, health, vendor links, all these things that you manage.

But isn't that a very different kind of relationship and business than some other businesses. Which therefore makes it easier for you to frame this kind of a wow, we're able, you know, we're going to protect you because in fact your whole thing is the protection of the relationship with the customer. A lot of other people may not have that kind of a stake, you know.

People can come and go as long as the traffic is sufficient if they're able to track enough of what they're doing. There may be, as Senator Isakson said, a sort of a commodity value to the information they have that's sufficient to encourage them. There may be better economics on that side of the ledger than on the other which encourages them therefore to chase that information rather than to be as protective as you are.

Does that make sense the distinction I'm drawing?

Ms. LAWLER. Yes, Senator, it does. Our customers' trust is really critical to us. And you talked about the nature of the sensitive information that we have and the relationship that we have with our customers is that they're using our services and products to manage their personal life, their personal finances, to manage their businesses online.

So we have actually gone directly to our customers and asked them what's important to them. And understanding that while there is that sensitive information there are other aspects of their interaction with us that might not be, if it was another company treated in the same, more sophisticated way——

Senator KERRY. So might you agree therefore that if you go to a retail outlet of some kind, perhaps, they have a different interest? And are there different stakes as a result? Would there be a different value level of protection as a result of the difference in the activity?

Ms. LAWLER. I think this is why we are talking about a principles-based approach based on industry sector type of data use. So clearly is data more sensitive in a retail environment? Maybe somewhat less so, but one of the things that was very clear from our customers is that in all contexts whether it is more shopping related data or whether it's related to their personal finances is that, while they may not read privacy policies, they really care about how their data is used. They want to understand that through clear, open, transparent explanations. And actually the more clear and open you are about that, the less they want to be fed with choices on a constant basis. What actually mattered to them was something that was very contextual and relevant that related to their experience.

So when we think about that and think about our principles-based approach we would look at something that was flexible that worked with our environment but also could be adapted to different industries, businesses and sectors of all sizes.

Senator KERRY. Well I appreciate—I certainly have enormous respect for the concept, the data stewardship concept, that you've articulated. I think that putting that kind of statement out front it's the customers, not ours, is a high standard. And we have to sort of figure out, you know, where that applies.

Mr. Montgomery, you may have a different feeling about that a little bit.

Mr. MONTGOMERY. Not a different feeling at all, sir. I think—I think an important question that you asked a little earlier which was about very clear notice that information has been collected so nothing that is hidden under, you know, under a menu. And I think that the self regulation program of which Microsoft, by the way, is an important part, has an icon on every single advertisement that collects information.

So the billions of advertisements that go out every week that collect information will have an icon on them which will allow consumers to click on the icon. It will tell them exactly who is collecting information about them.

Senator KERRY. Is that the icon?

Mr. MONTGOMERY. That's the icon in a somewhat expanded version.

Senator KERRY. What's the chart underneath it?

Mr. MONTGOMERY. That's an example of an ad that's actually running at the moment. And if you see in the top right hand corner. That's a pervasive ad choices icon that consumers would click on.

Once they click on the icon they'll be told a little about behavioral advertising, who is collecting information. And with one click be able to opt-out. So it's——

Senator KERRY. Does Verizon get a piece of the action today?

[Laughter.]

Mr. MONTGOMERY. No, they do not, sir.

Senator KERRY. OK.

Mr. MONTGOMERY. So I think it's an important point that you raise that it needs to be out there. And we think this is going to become like the recycling logo. It's going to build consumer trust and at the end——

Senator KERRY. How does that find its way to there now? Is that a one to one relationship with Verizon or how does it work?

Mr. MONTGOMERY. So we're busy rolling out the program to our client base. I think that there are more than 100 major clients that already subscribe. And clients just simply have to give us permission to go ahead. And most of our clients agree with it.

Then there's an underpinning technology that we employ that allows us to figure out exactly who is tracking so that we can apply a compliance mechanism to the process. So if an advertiser doesn't comply we contact them. Then we call them out publicly. And ultimately, you know, that information is made public and that——

Senator KERRY. Does that presume our, kind of, consumer awareness about that or would there be some sort of a campaign that makes people aware? How would you get the word out, so to speak?

Mr. MONTGOMERY. Yes. No, it's a great question. In my testimony earlier I talked about a campaign that we've developed with the Internet Advertising Bureau called "Privacy Matters." And that is already enjoyed over 600 million impressions against consumers.

And we're going to extend that campaign so we can teach consumers about what information is collected, the importance of behavioral advertising and also the importance of having access to free content on the Internet which is fueled by advertising.

Senator KERRY. So do you still accept the notion that—incidentally, I think it's a terrific step forward and I congratulate you for it—but do you still believe that you need a baseline law where there's a safe harbor from preemptive prescriptive regulation?

Mr. MONTGOMERY. Sir, what we feel is very, very important in this process is that self regulation is given an opportunity to work in this process. And if it needs to work with a baseline law we will be very happy to cooperate with you in any way to refine and ensure compliance around that as long as the self regulation can operate within it.

Senator KERRY. But suppose, I mean, if the FTC were to certify that program or similar program like that and it's compliant with the fair treatment of people's information given the way the net works and the modern technology that's available and the low cost of collection and so forth, couldn't collectors of information outside of your program wind up doing a lot of damage broadly in ways that would be inconsistent with what you've said consumers ought to have?

Mr. MONTGOMERY. Just to clarify, you mean, data trackers——

Senator KERRY. Yes.

Mr. MONTGOMERY. Who are outside the program?

Senator KERRY. Precisely.

Mr. MONTGOMERY. I think that there are bad actors out there. And one of the—and we would absolutely support any way that we could uncover those bad actors and who are doing anything to harm consumers.

Senator KERRY. Well, since our approach is principles-based, basically, doesn't that give you the latitude within which to be able to move?

Mr. MONTGOMERY. I think what's important is right now we have over 5,000 companies subscribing to the self regulatory process. And in that way we've got 5,000 policemen out there watching for the bad actors. And we, in fact, interestingly last week we discovered some fraudulent practice on the Internet and handed it over to the FBI for further investigation.

We hear this all the time amongst our, you know, our member base where, you know, they're looking out for that all the time. So in summary, we absolutely would work with you in any way we could to ensure consumer privacy and continued innovation.

Senator KERRY. Mr. Andersen, we've shared with you, with the company, you, the drafts, current drafts, as with several of you. And I wonder if you might just share with us your sense of sort of where we are in that process now, the direction.

Mr. ANDERSEN. From our perspective the process is going very well. We absolutely appreciate the opportunity to be involved in the process. We see the drafting process going in the direction we had hoped for which is to establish baseline principles in the law that we think are reasonable and we think that industry can and should be able to sign up for it. So we're very encouraged by it.

Senator KERRY. Appreciate that.

Ms. Lawler, what about you?

Ms. LAWLER. We also, excuse me, we also like the direction that the proposal is going. We are generally supportive. We like the principles-based approach. We like the consideration around codes of conduct and safe harbor.

We look forward to working with you on refining the proposal as it moves along.

Senator KERRY. Do you have a major—is there a major hurdle in your judgment?

Ms. LAWLER. I would say that there aren't any major hurdles. I think where we would like to work with you would be on the level of prescriptiveness of certain areas around notice and contacting.

Senator KERRY. OK. Well we look forward, obviously, to working that through with you. And all of, you know, certainly.

Ms. LAWLER. Yes.

Senator KERRY. Certainly.

Ms. LAWLER. There's very much that we do like in the bill, in the proposal.

Senator KERRY. Good.

Ms. LAWLER. So we think there's a lot there to work with.

Senator KERRY. Good.

Ms. LAWLER. And in particular, you know, we've talked a lot today about concern about bad actors. And you have companies represented in this room that are high achievers, you know, set very high standards. And I think what a principle based approach that is outlined in the proposal currently will also help us is really aim at the large mass of businesses, organizations in the middle, that may not have the same level of resources or expertise in privacy issues that you see at this table.

And so, principles-based approach, using safe harbors as described in the proposal, I think is a real positive mechanism to bring the large masses into a higher level of privacy protection.

Senator KERRY. Well, we'll work with you on that. I've just been noticed that they need me back in the office. So I've got to run and do that in a moment.

I think Colonel Khadafi doesn't believe in privacy or something so I've got to go deal with it.

[Laughter.]

Senator KERRY. Quick question if I can, Mr. Soltani. I want to get—you've talked thoughtfully about the first party entity and the website that you are directly interacting with and the third party is some entity that the first party allows to interact with you and so forth. It makes sense, very logical and we get it.

But we've been struggling a little bit with the cases where you have a first party such as Facebook. And then Facebook tracks behavior in another site, et cetera. And given that the consumer had a first party relationship with Facebook as long as notice is pro-

vided and choices provided for Facebook to acquire the information is that a point somewhere in between the first and third party? How do we—we've been struggling with this a little bit.

Mr. SOLTANI. It's a great question. I believe in that context Facebook is a first party and a third party. In the context when you go and enter Facebook.com into your URL bar of your browser, that's a first party interaction.

However, in the context where you are on say, the *Washington Post* and there are Facebook widgets, buttons, objects on the page, I believe that constitutes a third-party widget. The loading of a third-party widget that then results in passive data collection I still believe would fall under third-party data collection.

It's a little nuanced since users can also interact with that widget. And in the case where users knowingly interact with a widget perhaps we can frame it as a first party interaction.

Senator KERRY. So where would the notice have to be? Would the notice have to be the first time when you first sign up? This can happen? Or does the notice have to occur each time, each face page? How does it work?

Mr. SOLTANI. Since often these things are tied to identifiers I believe perhaps upon the setting of the identifier in the first party context the notice could happen. So, your "cookie" could then be later used to tie that activity to the third-party context.

We also want to be careful here around forced third party interactions, *i.e.,* when you go to a website and a video starts playing or an ad pops up that you're forced to dismiss, since you can actually compel users to require them to interact in a third party context.

I think we still want to frame it around meaningful interactions with third party objects that consumers are aware of, and we might consider that okay. All other passive data collection we would consider third party data collection.

Senator KERRY. OK. We've got to work that through obviously. And see how we can come out of it. But there's obviously some, you know, some of this is, you know, does get into that nuance.

Mr. SOLTANI. Absolutely.

Senator KERRY. Whatever you want to call it, area. It gets tricky. I think the principle that we want to have guide us is also to do no harm even as we are protecting people. And I think, you know, we're going to try to balance that very, very carefully here.

So we will continue a thoughtful process here of engagement with all of you to try. And Danny Sepulveda has been doing a superb job, I think, of reaching out and sitting with everybody.

I also want to thank as a slight nepotism here going on. But my brother over at the Commerce Department, as General Counsel has been involved in this without my instruction or engagement at all. They've done this on their own. But I thank them for their input which has been helpful in this process, enormously helpful.

And obviously we need to work with the Administration in order to figure out where we're going here.

I hope we can get a product where everybody is standing up and saying this is good. This is something we can live with. We can work with. And the consumer is really given a set of choices and opportunities here that they don't have today to make an intel-

ligent guided selection as to where they're heading and what's happening to their information.

And I think we can come out of there without upsetting the obvious commercial interests that we all want to encourage and that are important to us. So on that note we'll adjourn here today. And look forward to trying to get this thing into shape where we can get it introduced.

I'm working, as you know, with Senator McCain, very closely. And he's got some interest in this as we go. But I hope that we'll get to a point where we can introduce this in short order.

I think we need to do it. I think we need to do it soon. I think everybody will benefit by doing this. And I look forward to getting this accomplished. So thank you all very, very much for being here today.

We stand adjourned.

[Whereupon, at 12:09 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. MARK BEGICH,
U.S. SENATOR FROM ALASKA

Thank you to Chairman Rockefeller and Senators Kerry and Pryor for their work on this vital issue for Americans. Alaskans value their privacy so much there is a right to privacy spelled out in the Alaska State Constitution. We don't want the government or private businesses invading our privacy.

Online privacy is one of the most important issues facing consumers today. I frequently hear from constituents regarding the privacy practices of companies or the impact of the Internet on their lives. The Unites States Constitution clearly protects Americans from unreasonable searches of their private information without a compelling reason, and there's no reason to believe Americans are any more apt to tolerate someone pulling private information for financial benefit through their actions on the Internet.

I am particularly concerned about the pervasive nature of tracking on children's websites. I have an 8-year-old son who regularly uses the Internet and is extremely proficient on computers. My wife and I regularly monitor his Internet usage, but I cannot find out what companies target him, who has access to that information and to which third parties this information is sold. Additionally, what protections are in place to ensure he is not unknowingly downloading inappropriate or dangerous software? What sort of "e-dossier" is already being created by my son's Internet usage? Unfortunately, I believe there are few if any protections in place for this most vulnerable population.

We must find a solution that will protect people's online experience while enabling the Internet to continue to grow and thrive. We cannot accept the "wild west" status quo any longer. I look forward to working toward a solution in the 112th Congress.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK PRYOR TO
HON. JON D. LEIBOWITZ

General Privacy Questions

Question 1. Based on the FTC's December staff report, could you please highlight for the Committee where you see the most harm posed to consumers due to a need for better online privacy protections? Where do you think are the greatest risks to consumer privacy?

Answer. The Commission staff continues to be concerned about harms that can result from unauthorized disclosure of consumers' information, including financial harm such as identity theft; physical harm such as stalking; unwarranted intrusions into consumers' time, such as unwanted telemarketing calls and spam; and harms that result from the denial of employment, insurance, and other goods and services.

In addition, consumers suffer harm simply from having their information used without their informed consent. Consumers that provide information believing it is private will lose trust in a company if the company makes that information public without the consumer's consent. Consumers believing they are simply searching for information about a health condition online will lose trust in a company that sells information about them without their knowledge. More broadly, consumer trust in online services generally is damaged if companies collect and use data in ways that consumers do not expect. The loss of consumer trust in online services would harm both consumers and business by chilling consumers' willingness to participate in online activities and electronic commerce.

The preliminary staff report asked for comment on several recommendations to address these harms. For example, to address the problem of data falling into the wrong hands—such as identity thieves and stalkers, the report recommends that companies not collect unnecessary data, maintain better data security for the data they maintain, and dispose of the data when they no longer have a legitimate business need for it. To avoid collection and use of consumers' data without their in-

formed consent, the report makes recommendations on how companies can improve transparency and obtain more informed choices.

Question 2. How can consumers be better educated about privacy risks and steps they can take to protect themselves? Do consumers have the tools necessary to adequately protect themselves in today's world?

Answer. The Commission runs educational campaigns to teach consumers how to protect their valuable personal information and make thoughtful decisions about when it is shared and used. For example, the Commission manages the interagency *OnGuardOnline.gov* campaign, which helps computers users avoid fraud, protect their privacy and stay safe online. The *OnGuardOnline.gov* site has information to help parents talk to their kids about the value of their personal information and how to make responsible choices about where and how to share it. The Commission's identity theft information for consumers (*FTC.gov/idtheft*) also provides tips and advice about how to protect sensitive information online and off. A wide variety of consumer educational materials, including many in Spanish, help consumers deter, detect, and defend against identity theft. For example, the FTC publishes a victim recovery guide—Take Charge: Fighting Back Against Identity Theft—that explains the immediate steps identity theft victims should take to address the crime.

However, the Staff Report noted that companies' privacy practices—including the collection, use, and transfer of consumer information—are often not transparent to consumers; therefore collection or use of consumer information may occur without their knowledge or consent. In such situations, consumer education is not adequate to protect consumer privacy, which is why the Preliminary Staff Privacy Report highlights the need for some of the burden surrounding privacy protection to shift from the consumer to businesses. Thus, the Report asked whether industry can do more to help consumers better understand how their information is collected and used. As outlined in the Report, industry could incorporate privacy protections such as data security, sound retention practices, and data accuracy into products and services; offer simplified consumer choice; and inject greater transparency about data collection and use into business practices.

Question 3. What do you think FTC oversight would provide that self-regulation by the industry could not?

Answer. As an initial matter, the staff report does not take a position on whether its recommendations should be implemented through legislation or self-regulation. It is intended to provide guidance to industry, Congress, and policymakers as they develop rules of the road in this area.

That said, whether or not legislation gets enacted, self-regulation will always play an important role in protecting consumer privacy. The Commission staff has supported self-regulation in the past and continues to believe that self-regulation can be an effective tool, as long as it is comprehensive, robust, effective and enforceable. And under Section 5 of the Federal Trade Commission Act, the Commission can take enforcement action against companies that break their promises to abide by self-regulatory codes of conduct. This is an important component of ensuring accountability for self-regulatory programs.

Question 4. What steps should the industry take to assist citizens with knowing what their digital life is like?

Answer. The Preliminary Staff Privacy Report contained a number of recommendations for industry to help people understand how their personal information is collected and used. In particular, the Report recommended simplifying choices for consumers and increasing transparency.

Recognizing that the current model of lengthy privacy policies was ineffective in informing consumers about information practices, the Staff Report recommended that businesses simplify choices provided to consumers. For example, the staff report indicated that companies do not need to provide choice before collecting and using consumers' data for commonly accepted practices, such as product fulfillment. For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. This will allow the consumer to focus on the choices that matter and make more informed decisions.

The Staff Report also recommended that companies increase the transparency of their data practices, by, for example, making privacy notices clearer, shorter, and more standardized, to enable better comprehension and comparison of privacy practices. The Report also recommended that companies consider providing reasonable access to the consumer data they maintain, proportionate to the sensitivity of the data and the nature of its use.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KAY BAILEY HUTCHISON TO HON. JON D. LIEBOWITZ

Question 1. Chairman Leibowitz, in his concurring statement to the FTC report, Commissioner Kovacic expresses the concern that a Do Not Track mechanism on the Internet could inherently reduce the quality of content provided, by lowering the revenue currently derived from advertising and possibly even forcing some online content providers to deny free access to those who opt out of tracking.

- Has the Commission examined what the ramifications of do not track could be on the quality of content provided online, particularly of content that is currently provided for free?
- Will you commit to ensuring that this type of analysis will be part of the Commission's analysis before the final report comes out?

Answer. The Commission recognizes the need for an appropriate balance between consumer choice about online tracking and ensuring continued innovation in this area. As the Preliminary Staff Privacy Report noted, online advertising helps to support much of the content available to consumers on the Internet. Although the Commission is continuing to evaluate the comments received on its staff report, evidence suggests a Do Not Track mechanism for exercising choice about behavioral advertising would have minimal impact on the free content available on the Internet and on innovation. First, the Preliminary Staff Privacy Report noted that certain advertising, such as first party marketing and contextual advertising, would not be affected by a Do Not Track mechanism. Thus, this type of advertising would continue to serve as a source of revenue for content providers.

Second, recent research from an organization working with the advertising industry suggests that if companies provide adequate transparency and consumer choice, consumers will choose not to opt out in great numbers, because they have a greater degree of trust in companies' stewardship of their information. See Evidon (formerly Better Advertising), Research: consumers feel better about brands that give them transparency and control over ads, *http://blog.evidon.com/2010/11/10/research-consumers-feel-better-about-brands-that-give-them-transparency-and-control-over-ads/* (Nov. 10, 2010).

Finally, key industry stakeholders have responded very positively to the request for development of a simple, easy to use Do Not Track system. Leading browser companies have offered changes to their browsers to implement Do Not Track. Mozilla, for example, has implemented a Do Not Track header for use by consumers when they browse the web, and Microsoft has rolled out a Tracking Protection List feature that allows consumers to block the collection of information by specified third parties. Apple has announced a do not track tool in a test version of its browser. The advertising industry itself also appears to recognize the value of offering simplified choice to consumers and has ramped up its effort to provide clearer disclosures and choice mechanisms after release of our preliminary staff report. Indeed, most recently, several of the leading advertising industry trade associations have agreed to work closely with Mozilla to determine how to incorporate Mozilla's Do Not Track feature into its industry self-regulatory effort. I believe these efforts demonstrate that improved consumer choice can be consistent with innovation.

As these developments take place, the Commission is continuing to analyze the comments received on the Preliminary Staff Privacy Report, including those regarding the potential effects of a Do Not Track mechanism on innovation and the availability of free Internet content. The Commission also will continue to evaluate information about the costs and benefits of any such mechanism.

Question 2. The Commission's report calls for a "privacy by design" model that includes the recommendation for companies to only collect information needed for a specific business purpose. Some comments submitted on the report expressed concern that implementing such a restriction could become so specific that it limits innovation on new and potentially beneficial uses of data. How do you envision such a restriction being implemented in a way that will allow for the continued innovation of new products and services necessary to keep American companies as leaders in the global online world?

Answer. The goal of privacy by design is to guide and motivate businesses to develop best practices for incorporating privacy into their products and services during the early stages of their development. Best practices that ensure that privacy solutions are compatible with business needs should not restrict innovation and will likely be more flexible than government rules. To be clear, the principle of privacy by design contemplates that businesses can and should collect information for their legitimate business purposes; however, as discussed in the Preliminary Staff Privacy Report, the concept of privacy by design also means the amount of data collected

and duration for which such data is retained should be limited by those legitimate business needs. This reflects concerns that collected data may be retained by companies indefinitely, increasing the risk that the data may be compromised through a security vulnerability or put to use in ways that consumers never would have expected and to which they would object. Staff's recommendation that companies implement a privacy by design approach is designed to encourage businesses simply to think through the privacy and security risks associated with collecting more information than is currently needed from consumers and retaining it for longer than necessary. The Commission has recognized these concerns in its enforcement program. For example, we have brought data security cases against companies that kept shoppers' credit card information, long after they had a business need to do so. *See e.g., In the Matter of BJ's Wholesale Club, Inc.,* Docket No. C–4148 (Sept. 23, 2005) (final consent order). In these cases, the credit card information was obtained by hackers. Had the companies taken more care in disposing of information they no longer needed, consumer harm could have been avoided. Similarly, last year Google collected personal information through its Street View cars—the company claims to have inadvertently collected that information without any intention of using it. Under the Privacy by Design approach recommended in our staff report, Google would have tested its systems to ensure that it did not collect data it did not need.

As these examples demonstrate, companies should assess privacy and security risks as part of the innovation process and work to address them appropriately. For example, although they may determine that continued collection of personal data is necessary, they could try to anonymize such data to reduce privacy and security risks.

We have received many comments on the concept of collecting and retaining data for a "specific business purpose," which we plan to address in the final report in a way that furthers consumer privacy interests without impeding innovation.

Question 3. Chairman Leibowitz, FTC Commissioner Rosch has expressed "serious reservations" about the new privacy proposal advanced in the FTC's staff report. He claims that the current "harm" model of FTC enforcement has served the Commission well. If the FTC is correctly enforcing its statutory responsibilities to ensure disclosure of "material" privacy policies and to hold companies accountable for those policies, consumers already have information to make informed decisions about their online privacy.

- If that's the case, why is it necessary to adopt a new, broader regulatory framework for online privacy?
- If privacy policies are too opaque for consumers to understand and if the FTC is concerned that consumers may be misled, why wouldn't rigorous enforcement of the FTC's Section 5 deceptive trade practices authority improve the clarity of privacy policies by companies seeking to avoid enforcement actions?

Answer. First, I note that the report does not propose a new regulatory framework—it simply provides a framework for industry best practices and potentially, for legislation, if Congress chooses to enact it.

Second, I agree with you that robust enforcement of Section 5 is critical. We have recently brought cases against companies like Google, Twitter, and Chitika, an online advertising network, alleging that their practices were deceptive. We have additional cases in the pipeline.

Third, Section 5 does not generally require companies to disclose their information practices. If they choose to make statements about privacy, and those statements are deceptive, the Commission may take action under Section 5. However, not every long or opaque disclosure will be deceptive under Commission precedent. Regardless of the threshold for Commission law enforcement actions, we believe that stakeholders should work together to improve transparency. Indeed, many companies recognize that providing clear disclosures to their consumers about their information practices helps them maintain a positive relationship with their customers. Companies have an interest in promoting that relationship regardless of the prospect of enforcement action by the FTC. The Preliminary Staff Privacy Report provides businesses with proposals for ways to simplify and improve disclosures, and we think those steps would work well in this area while we continue to take action against plainly deceptive practices.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK PRYOR TO LAWRENCE E. STRICKLING

Question 1. From your perspective, what were the two most important privacy issues you'd like to highlight in the Department's Commerce privacy green paper?

Answer. The Green Paper examines how the United States can strengthen its consumer data privacy framework while ensuring that this framework continues to encourage innovation in the digital economy. Instead of identifying specific consumer data privacy issues that companies and policymakers should address, the Green Paper focuses on recommendations that would help to create a policy framework that better addresses increasingly intensive uses of personal data in the digital economy. Two main issues emerged from this analysis.

First, consumers and businesses would benefit from the adoption of baseline, comprehensive Fair Information Practice Principles (FIPPs) in the commercial context. Much of the personal data traversing the Internet falls into the gaps between existing Federal privacy statutes. There is also evidence that consumers who use the Internet misunderstand the legal rules that apply to personal information collection and use in the commercial context. These gaps in legal protection for personal data leave consumers insecure and uneasy about how data about their activities and transactions are collected, stored, and used. Widely adopted, comprehensive FIPPs would help to fill these gaps and thereby increase consumer trust in the Internet.

Businesses would also benefit from comprehensive baseline FIPPs. Businesses generally recognize that their sustainability depends on maintaining consumer trust but find that the rules of the road are hard to discern. Applying a set of general principles to commercial activities that are not covered by an existing Federal data privacy statute would provide businesses with guidance as to what consumers and enforcement agencies expect of them.

Second, fostering innovation within a consumer data privacy policy framework requires a flexible approach to implementing privacy protections. The Green Paper proposes a framework in which the Department of Commerce would convene multi-stakeholder groups—composed of representatives from industry, civil society, academia, and other government agencies—to define codes of conduct that are enforceable by the Federal Trade Commission under its current authority or through any additional authority granted through baseline consumer privacy legislation. These codes would provide guidance about how to apply FIPPs in specific contexts. The multi-stakeholder process envisioned in the Green Paper would help to ensure that these codes set forth practices that reflect evolving consumer expectations.

Question 2. What role does consumer trust play in the way users exchange information, goods and services over the Internet?

Answer. Protecting consumer trust in the Internet is a top policy imperative of NTIA and the Department of Commerce. Consumer trust is essential to nurturing the Internet's growth, and protecting privacy is an important part of maintaining consumer trust. When consumers entrust personal information to a company that does business on the Internet, they expect that the company will handle it in ways that are consistent with this relationship. If companies use information in ways that are contrary to consumers' expectations, then consumers may be reluctant to adopt new Internet services and applications. Finally, consumer trust depends on more than privacy. Issues of security, safety, and reliability also come into play. Whether making purchases online, communicating with family members, or conducting business, consumers must know that they have control over their personal information. As innovative new applications and services are developed, it is important that consumers know that their information is safe and that providers have clear rules about how to respect individual privacy.

Indeed, the Department, in partnership with other Federal agencies and the private sector, is leading the implementation of an Administration effort to improve consumer trust online: The National Strategy for Trusted Identities in Cyberspace (NSTIC). The NSTIC envisions enhancing online privacy and security through services that provide credentials that improve upon the user name and password schemes that are common online. The NSTIC proposes using technologies that would provide individuals the option of obtaining a strong credential to use in sensitive online transactions. The NSTIC calls for the participants in this digital identity marketplace to implement privacy protections that are based on comprehensive FIPPs. Developing enforceable codes of conduct through multi-stakeholder processes is one way that the Department can work with the private sector to implement these protections.

Question 3. What do you envision the Department's role will be with respect to privacy in the future?

Answer. We propose in the Green Paper an important role for the Department of Commerce in convening stakeholders to develop enforceable codes of conduct that implement comprehensive Fair Information Practice Principles (FIPPs) that the Obama Administration supports as the foundation of Federal legislation in this area. The Green Paper outlines a multi-stakeholder process in which the Department would convene companies, civil society groups, academics, and the FTC and other government agencies to produce enforceable codes of conduct. An open development process that includes industry and consumers can help align these codes and consumer expectations.

Another important role for the Department of Commerce is to work toward greater interoperability between the U.S. consumer data privacy framework and those of our allies and trading partners. Companies would benefit from the potential reduction in multiple compliance burdens, and U.S. consumers would benefit from more consistent cross-border consumer data privacy protections. Both objectives are important to the Department of Commerce, and the Department and the Administration are committed to working with Congress to develop an appropriate legislative approach.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARK BEGICH TO LAWRENCE E. STRICKLING

Question. What steps should the industry take to assist Citizens with knowing what their digital life is like?

Answer. Enhancing transparency is one important step that companies can take to help consumers understand the role of personal data collection and use in the digital economy. As the Department of Commerce's Green Paper on consumer data privacy explains, enhanced, effective transparency requires providing consumers with information that is accessible, clear, salient, and comprehensible. Current practices surrounding disclosures of privacy practices generally fall short of this standard; the privacy policies that are the primary mechanism for explaining what information companies collect and how they use are often lengthy, dense, and difficult to comprehend. Providing simpler statements of these practices, and providing them at times when consumers can act on this information, are ways that companies can provide consumers with greater insight into, and control over, their digital lives. Online tools or interfaces that allow consumers to understand and manage the collection of personal information can also provide a link between enhanced transparency and enhanced user control.

The Department of Commerce has also recommended that companies regard enhanced transparency as part of a more comprehensive approach to handling personal information. To this end, the Green Paper encourages the broad adoption of comprehensive Fair Information Practice Principles (FIPPs).

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KAY BAILEY HUTCHISON TO JOHN MONTGOMERY

Question 1. Mr. Montgomery, you mention at the beginning of your testimony the importance of behavioral advertising to the Internet. Do you believe the enactment of baseline privacy principles in the form of Federal legislation would have an effect on targeted advertising? If so, what would it be? And, in turn, what impact might that have on the larger online ecosystem?

Answer. GroupM supports efforts to promote transparency and choice in the marketplace and believes industry self-regulation is the appropriate approach for addressing concerns with online advertising while ensuring the ad-supported web continues to provide consumers benefit and fuel the Internet economy. A major benefit of self-regulation is its ability to respond quickly to changes in the technology, business practices, and consumer preferences. It is this adaptive nature of self-regulation that makes it so well suited for the complex Internet ecosystem.

Our business is built on the belief that both consumers and companies benefit when advertising provides timely and relevant information to those consumers who are most likely to be interested. While not deliberate, a law could reduce the relevancy and effectiveness of advertising. There is already strong evidence that privacy regulations in the European Union have resulted in an average 65 percent re-

duction in the effectiveness of online ads.[1] We have concerns that a U.S. law could similarly hinder innovation in the advertising and marketing industry, undermining economic support for valuable content and services and possibly encouraging higher fees to consumers. Inhibiting innovation would restrict growth in one of the healthiest industries in a troubled U.S. economy. These conditions would discourage venture capital funding for new entries, and in so doing, stall job growth in the industry.

Question 2. Mr. Montgomery, there has been a lot of discussion about whether industry best practices and self-regulatory efforts are effective. Many believe that market forces will push companies toward such industry-led efforts and that the FTC has the existing legal authority to hold companies accountable as good stewards of consumer information. Which do you believe is best for consumers: having the Federal Government act as a legal backstop to industry-led self-regulation or having the government set top-down prescriptive rules on how to collect and use consumer data? What are some of the advantages and concerns with each approach?

Answer. Industry-led self-regulation is preferred over top-down, prescriptive rules imposed by government. GroupM believes self-regulation is the most effective means for addressing concerns with online behavioral advertising. Self-regulatory codes are adaptive and may be quickly modified to address changes in consumer preference and technology. In addition, this approach helps preserve an environment that fosters online innovation, ensures advertising continues to help fuel the Internet economic engine, and supports a vibrant, ad-supported offering of products and services online that consumers now expect to receive for free or at a low cost. GroupM believes that the Digital Advertising Alliance's ("DAA") Self-Regulatory Principles of Online Behavioral Advertising ("Principles) are comprehensive yet flexible enough to respond to the complex and rapidly evolving online advertising ecosystem. The Principles set-forth consumer-friendly standards that require participants to provide enhanced transparency and consumer choice with respect to the collection and use of data for online behavioral advertising purposes.

The DAA's program has been designed for its participants to self-police, promote compliance, and, where necessary, report non-compliant companies to the appropriate government agencies. This private-public collaboration where the Federal Government acts as a legal backstop augments the self-regulatory program's credibility and reinforces the program's accountability measures.

The DAA program is backed by independent enforcement programs working in concert to monitor and enforce compliance with the Principles, as well as manage consumer complaint resolution. These accountability programs are live and being administered by the Council of Better Business Bureaus ("CBBB") and the Direct Marketing Association ("DMA"). The DMA and CBBB Accountability Programs are empowered under the Principles to provide a public report on entities that do not come into compliance and to refer such cases to the Federal Trade Commission ("FTC"). The FTC through its authority under Section 5 of the FTC Act can enforce against entities that fail to honor its commitment to adhere to the Principles. Through industry self-policing, more cops are on the beat, which reduces the burden on the FTC.

Question 3. While a large portion of the online industry is participating in the self-regulatory program, it has not reached 100 percent. What can be done to increase participation? Is it possible to do get full participation through a self-regulatory program?

Answer. It is very possible to achieve full participation in the DAA program. The leading marketing and advertising trade associations, representing more than 5,000 companies, have committed to this self-regulatory approach because they strongly believe in the program's purpose. This unprecedented collaborative effort has brought together representatives of the entire advertising ecosystem to develop and implement principles for the use and collection of data in this important area to the economy. Already, over 60 companies are participating in the DAA's Consumer Choice Page (*http://www.aboutads.info/choices/*) and billions of ad impressions have been delivered with the Advertising Option Icon—the icon appearing in or near ads or on web pages where data is collected or used for online behavioral advertising purpose. This icon is used by participants to provide notice concerning online behavioral advertising practices and link to a universal choice mechanism.

The launch of the DAA program is resulting in a change in industry practice. Companies are starting to require their partners to adhere to the Principles. This

[1] According to a study conducted by Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," available at *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259*.

is driving participation in the program. In addition, the trade associations behind this self-regulatory effort and the Accountability Programs are reaching out to companies to promote program participation. To help companies with compliance, the DAA has selected three companies as approved providers to assist companies with implementing the Principles. These approved providers' services help companies to provide enhanced notice and choice as required by the Principles.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. KAY BAILEY HUTCHISON TO ERICH D. ANDERSEN

Question. While a large portion of the online industry is participating in the self-regulatory program, it has not reached 100 percent. What can be done to increase participation? Is it possible to do get full participation through a self-regulatory program?

Answer. The online ad industry, led by the Digital Advertising Alliance (DAA) and of which Microsoft is a member, is working to increase participation in the self-regulatory program. Among the efforts to drive participation is increased outreach to companies to promote participation and providing assistance to implement the program. Through these efforts the DAA believes it is possible to achieve full participation in its program.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN ENSIGN TO ERICH D. ANDERSEN

Question 1. How would you say the self-regulatory approach is working in the marketplace to protect consumers thus far?

Answer. While still in the early stages of roll-out, the self-regulatory approach for online advertising is on a sound path. Over 60 companies, including Microsoft, are already participating in the Digital Advertising Alliance's (DAA) Consumer Choice Page resulting in an Advertising Option Icon being delivered on billions of online ad impressions. The icon not only provides notice to consumers about online behavioral advertising practices, but also provides a link to a universal choice mechanism. With the leading marketing and advertising trade associations backing the self-regulatory approach the expectation is that more companies will participate in the Consumer Choice Page.

The last few months have shown that industry can act quickly and effectively. For example, in that short period of time, the three major browser vendors have announced do not track tools that offer unprecedented privacy protection. Even the FTC has recognized and commended the progress industry has made in acting quickly and effectively to protect consumer privacy.

Question 2. Mr. Andersen, you talked about the importance of industry self-regulation and best practices. How would your ability to protect consumers be compromised if we went in the opposite direction?

Answer. Our ability to protect consumers would be compromised by the adoption of impractical proposals. Legislation becomes overregulation if it contains preferences for particular services, solutions, or mechanisms to provide notice, obtain choice, or protect consumer data, or if it mandates prescriptive rules that may be of limited effect or that burden businesses without yielding commensurate privacy benefits. Seeking input from interested stakeholders is one way to ensure the right balance is struck.

Question 3. Mr. Andersen, your testimony highlighted the need to promote continued innovation in technology and online services. Fostering and supporting innovation in the marketplace is a top priority of mine, and there is no question that innovation is crucial for creating jobs and economic growth. In your view, what is the best way to encourage innovation while still protecting consumers' online privacy?

Answer. There are a number of ways to encourage innovation while still protecting consumers' online privacy:

- Recognition of the role of self-regulation: while comprehensive privacy legislation may provide a set of baseline protections, self-regulation can build upon those protections and adapt them to specific contexts. Consumers have different privacy expectations depending on whether they are interacting with online retailers, social media services, search engines, or online ad networks. Self-regulatory principles can be tailored to these different contexts. In addition, self-regulation can address emerging technologies or business models.
- Ensure there are no technology mandates.

- Allow for "operational use" of data. This means that companies would be able to use data to provide the service the user wanted, improve services, protect against fraud, and generally operate their business.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK PRYOR TO BARBARA LAWLER

General Privacy Questions

Question 1. How does on-line information collection usually work?

Answer. Intuit does not engage in online tracking. However, as a technology, online information tracking typically works through the use of "cookies" which are random, identifiers that have no significance on their own. These "cookies" may be limited in their duration to a particular session that a customer is having with a website, or they may persist for longer periods of time. In typical "first party" online information collection, these cookies can help a company understand several things—the time spent on the site, the pages visited (and for how long), the navigation, or "path" that the visitor took, etc. This information is frequently used to improve the performance and usability of a company's website. Information may also be collected for "3rd party" use—where the kinds of information mentioned above may be shared across several different entities, typically advertisers, web-site publishers, and companies that help to match advertisers to publishers.

Question 2. How does behavioral advertising differ from contextual advertising?

Answer. Behavioral advertising typically refers to the delivery of advertising messages based on the interests inferred from a person's on-line behavior, over time. It may include the kinds of searches that he/she does; the types of websites visited, etc. The combination of these pieces of information can be used to deduce a person's interests, in which case advertisements related to those possible interests can be shown to the individual.

Contextual advertising typically involves a "single point in time" matching of advertising content to someone based on a specific action that the individual takes. The classic example is the advertisements, or 'sponsored links', which show up in the search results for a particular search query. For example, if someone were to search for information on car tires, he/she will likely see advertisements from tire manufacturers/sellers based specifically on that search request.

Question 3. What evidence is there that behavioral advertising is effective?

Answer. There have been some studies done which have shown that people are more likely to respond to advertising based on their inferred interests, than more general advertising messages unrelated to the audience receiving them.

Question 4. What does online information collection mean for our children's reputations?

Answer. Collection of information on children under 13 is regulated by the COPPA. Intuit's products and services are financial in nature and not intended to be used by children.

We recognize the proliferation of social media and the use of it by minors. We would expect that companies providing such services would do so lawfully, and in a manner respectful of all individuals using such a service.

Question 5. To what extent is geo-location tracking a problem?

Answer. Geo-location information can be very useful to provide specific, highly relevant services to individuals, such as providing directions, identifying nearest services, etc. In all cases, however, the individual should understand that his/her geo-location information is being collected. It should also be retained and used for a very limited period of time specifically to provide those relevant services to him/her. Once the services have been delivered, the geo-location data should be deleted and/or removed from the service.

Question 6. Is Federal privacy legislation needed? If so, what should be the basic elements of any privacy legislation?

Answer. We see the value in commonsense Federal privacy legislations that could set rules of the road for companies to follow and clear the field of conflicting state laws. As the digital economy has grown over the last decade, self-regulatory approaches have allowed many businesses to offer consumers many innovative products and services while incorporating meaningful privacy protections in ways that fit the company size, structure, culture and industry. High performers that are committed to capturing and retaining their customers' trust implement a range of self-regulatory approaches, from privacy seals to government sponsored codes of conduct (such as the Dept. of Commerce Safe Harbor Program). Self-regulatory approaches may fall short for new, small start-ups, naïve companies or malfeasant companies.

The same could be said for regulation as well. It's our belief that the most effective way to protect consumers and support innovation is a principles-based approach, covering Fair Information Privacy Practices creates a credible baseline that provides the rules of the road.

Question 7. Should companies be held to higher standards with respect to our children and the way their information is handled?

Answer. The Children's Online Privacy Protection Act (COPPA) sets a high standard with respect to children online. The FTC should provide rigorous enforcement of COPPA.

Question 8. Are you concerned about employer or insurance discrimination based on information collected about consumers online?

Answer. We would have to research this issue in order to comment on this question.

Other questions

Question 9. Your testimony demonstrates a strong commitment to privacy. Do you believe that Intuit's approach to privacy is generally followed by companies operating online? How would you suggest other companies integrate privacy protections into their services?

Answer. Different businesses can offer consumers various innovative products and services while incorporating meaningful privacy protections in ways that fits the company size, structure, culture and industry. High performers like Intuit that are committed to capturing and retaining their customers' trust implement a range of self-regulatory approaches, from privacy seals to government sponsored codes of conduct (such as the Dept. of Commerce Safe Harbor Program). Self-regulatory approaches may fall short for new, small start-ups, naïve companies or malfeasant companies. It's our belief that the most effective way to protect consumers and support innovation is a principles-based approach to legislation that creates a baseline that provides the rules of the road. We believe that an emphasis on education and advocacy through industry sector associations, business groups, small business associations and local chambers of commerce. This would be necessary for both regulatory and self-regulatory approaches.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARK BEGICH TO BARBARA LAWLER

Question. What steps should the industry take to assist citizens with knowing what their digital life is like?

Answer. We are committed to educating our customers about their data stewardship choices and what they can do to protect their personal information when interacting with our products. Consumers would benefit from additional direct education and communication, such as PSAs through mass media, social networks and simple and clear information company websites.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KAY BAILEY HUTCHISON TO BARBARA LAWLER

Question 1a. Ms. Lawler, your company is engaged in a variety of online businesses and is subject to several Federal and state privacy regulations. You know as well as anyone that totally unrelated companies can be impacted in different ways by the interconnected web of privacy laws. I fear that addressing a privacy issue in one area could have unexpected ramifications in a totally different area. If this Committee considers developing new online privacy legislation, what sort of pitfalls should we look out for so that we can avoid such unintended consequences?

Answer. A principles-based legislative approach will have the highest probability of success in protecting consumers while providing a flexible, level playing field for a wide range of businesses holding different types of data for different purposes. This would allow organizations to incorporate the necessary types of privacy protections for consumers while allowing flexibility on how the protections are implemented. It can be the optimal framework for a wide range of business, especially small businesses, which are the backbone of the American economy. We are specifically concerned about requirements that provide risk to innovation and customer delight, that may limit the flexibility to try new options and methods of delivering value to our customers in a rapid, iterative fashion. Examples include mandates to require the use specific technologies or specific procedural mechanics, such as very specific requirements regarding how and when notices are delivered, worded and

formatted; or rules that place too many controls on the first party use of data especially those uses that are already consistent with consumer understanding and expectations. Specific requirements can create overlapping rules for the exact same sets of data; or specific words required for contractual agreements with third parties can create confusion or inadvertent non-compliance. The Committee must also be careful to avoid prescriptive mandates that attempt to address one set of concerns with the Internet but could unintentionally limit or prevent other elements of the Internet from functioning properly—for example, the commendable effort to increase transparency and choice related to behavioral tracking and advertising, if overly proscribed, could inhibit software as a service applications' functionality. As we developed the Intuit Data Stewardship Principles, our customers told us in multiple rounds of research that they prefer the specificity of simple, plain language—Principles rather than the policy-based, business-speak language you or I might think is better.

Question 1b. Is there an approach we can take to build upon or work within existing frameworks, such as HIPPA and Gramm-Leach-Bliley, rather than writing another separate statute?

Answer. At Intuit we have experience with applying different rules to overlapping sets of data. Both HIPAA and GLB have their strengths and weaknesses; both are based on recognized privacy principles, and yet take philosophically different approaches. HIPAA is designed to limit data uses and sharing beyond the first party organization, while GLB is designed to enable data uses beyond the first party organization. And both contain elements of proscriptive requirements, notices being a prime example.

We recommend starting from a fresh perspective that is principles based and does not rely on procedural requirements.

Question 2a. Ms. Lawler, there has been a lot of discussion about whether industry best practices and self-regulatory efforts are effective. Many believe that market forces will push companies toward such industry-led efforts and that the FTC has the existing legal authority to hold companies accountable as good stewards of consumer information. Which do you believe is best for consumers: having the Federal Government act as a legal backstop to industry-led self-regulation or having the government set top-down prescriptive rules on how to collect and use consumer data?

Answer. We believe the most effective solution would be a middle ground between the two: A principles-based legislative approach will provide a wide range of businesses holding different types of data for different purposes to incorporate the necessary types of privacy protections for consumers while allowing flexibility on how the protections are implemented. It can be the optimal framework for a wide range of business, especially small businesses, which are the backbone of the American economy.

Question 2b. What are some of the advantages and concerns with each approach?

Answer. There is an argument that market forces, policy-maker scrutiny, customer expectations are heading in right direction but will not fully cover all types of organizations—high performers, edge riders and the majority that are unaware. Enforceable self-regulatory codes of conduct work for most business—high performers are provided opportunity to excel, and those who need rules of the road are still able to comply—preserving flexibility and the ability to innovate is key. As Congress considers rules of the road, take care to not be overly prescriptive—protecting online privacy while sacrificing innovation will not help consumers or the competitiveness of the American economy.

Question 3. While a large portion of the online industry is participating in the self-regulatory program, it has not reached 100 percent. What can be done to increase participation? Is it possible to do get full participation through a self-regulatory program?

Answer. We believe that a good approach is an emphasis on education and advocacy through industry sector associations, business groups, small business associations and local chambers of commerce. This would be necessary for both regulatory and self-regulatory approaches.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN ENSIGN TO BARBARA LAWLER

Question 1. How would you say the self-regulatory approach is working in the marketplace to protect consumers thus far?

Answer. As the digital economy has grown over the last decade, self-regulatory approaches have allowed many businesses to offer consumers many innovative products and services while incorporating meaningful privacy protections to protect their customers in ways that fit the company size, structure, culture and industry. High performers that are committed to capturing and retaining their customers' trust implement a range of self-regulatory approaches, from privacy seals to government sponsored codes of conduct (such as the Dept. of Commerce Safe Harbor Program). Self-regulatory approaches may fall short for new, small start-ups, naïve companies or malfeasant companies. The same could be said for regulation as well. It's our belief that the most effective way to protect consumers and support innovation is a principles-based approach to legislation that creates a baseline that provides the rules of the road.

Question 2. Ms. Lawler in your testimony you cite the value of principles-based privacy legislation working in tandem with self-regulatory approaches and codes of conduct, highlighting the importance of enabling industry flexibility.

Answer. A principles-based legislative approach will provide a wide range of businesses holding different types of data for different purposes the ability to incorporate the necessary types of privacy protections for consumers while allowing flexibility on how the protections are implemented. It can be the optimal framework for a wide range of businesses, especially small businesses, which are the backbone of the American economy.

Question 3. In your opinion, what would be the effect of over-prescriptive, one-size-fits-all regulation on your ability to protect the online privacy of consumers?

Answer. Intuit's approach is to provide our customers a high integrity, trusted end-to-end experience that ultimately results in customer delight. Proscriptive, one-size-fits-all approaches tend to emphasize form over functional value to consumers (when was the last time you read the mandatory financial institution or HIPAA privacy notice?). Such an approach would force us to focus on procedural compliance first and customer delight and innovation second. Our priority lies with providing our customers with innovative ways to solve their financial problems while making sure their data is protected.

Question 4. Can you give me specific examples of what types of industry regulation you would consider over-prescriptive?

Answer. We are specifically concerned about requirements that provide risk to innovation and ultimately hurt our ability to meet our customer' needs, and limit the flexibility to try new options and methods of delivering value to our customers in a rapid, iterative fashion. Examples include mandates requiring the use of specific technologies or specific procedural mechanics, such as very specific requirements about how and when notices are delivered, how they are worded and formatted, or specific words required for contractual agreements with third parties. As we developed the Intuit Data Stewardship Principles, our customers told us in multiple rounds of research that they prefer the specificity of simple, plain language Principles rather than the policy-based, business-speak language you or I might think is more descriptive.

Question 5. In your view, what is the best way to encourage innovation while still protecting consumers' online privacy?

Answer. We believe that the best way is through a principles-based approach that could work in tandem with self-regulatory approaches and enforceable codes of conduct, which provide consistent guidance to all types and sizes of organizations, fill the gaps between existing regulations. The principles-based approach is especially critical to allow for flexible application by small businesses.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK BEGICH TO CHRISTOPHER R. CALABRESE

Question 1. What steps should the industry take to assist citizens with knowing what their digital life is like?

Answer. While industry can take some limited steps to protect consumers, the best way to improve public knowledge about digital life is for Congress to grant consumers control over their own personal information. If consumers had enforceable rights, they would educate themselves about how to use them. In the current system, there is no advantage to consumers in learning key facts about their digital

life such as the entities that hold personal information or the tools used to monitor web tracking. No matter how educated consumers become, they can't do anything practical or beneficial with their knowledge. They can only participate online in a "take it or leave it" way. They have no power to limit data sharing, access personal profiles, or delete records. Consumers will only take the time to learn about the use of their information if it is worth their time and effort to do so. That means giving them the tools to police their own profiles and limit data sharing. My written statement elaborates in much more detail on the full range of enforceable rights the ACLU believes should be available to consumers.

Given that reality, one useful step industry could take is to work with the Federal Trade Commission (FTC) to reduce the complexity of their privacy policies. Because the FTC can only penalize companies that engage in unfair and deceptive practices, companies have incentives to avoid providing clear notice to consumers because that notice could be used to create enforceable rights against them. Instead, they largely write bloated privacy policies that describe company practices in such detail and legalistic jargon as to be incomprehensible to consumers. If companies commit to providing simplified policies with common language and definitions that can be compared between companies (like nutrition labels on food), it would be a helpful consumer education tool.

Similarly, companies could commit in simple terms to honoring any do not track preference stated by a consumer and insuring that all advertisers on their site do the same. "Do not track" should be understood to mean no tracking or storage of information at all, not simply a ban on behaviorally targeted ads. Such a mechanism would also give consumers incentive to learn about their rights.

Ultimately both of these tools are limited compared to the real explosion of consumer education and understanding that could be created if consumers were actually given enforceable control over their information through a legislative mandate.

Question 2. Mr. Calabrese, I appreciate your comments regarding the invasion of privacy currently occurring on the Internet. Besides your recommendation for a "Do Not Track" method for browsers what else could we do to improve the experience of Internet users?

Answer. The best way to improve the experience of Internet users is to increase their trust in the system. As Internet use is increasing so is consumer awareness and fear of expanding information collection. Many new web applications use and share a great deal of personal information. Social networking sites, location based services, online retail services, and a variety of other sites all rely on a willingness of consumers to share personal information. These websites and applications can only reach their full potential if consumers can share this information secure in the knowledge that they retain control over it.

There is evidence that these fears are affecting consumers. According the Federal Communications Commission's National Broadband Plan, 22 percent of people don't use the Internet because of discomfort with computers and concern "about all the bad things that can happen if [they] use the Internet." According to Gallup polling conducted for USA Today, 61 percent of consumers opposed web tracking even if they kept costs down and allowed consumers to visit websites for free.

Efforts to protect consumer privacy must be backed by the government, not simply created by industry. For years, government agencies have called on industry to provide privacy protections for consumers. However, as the FTC report explains in its recent report on privacy, self-regulatory efforts "have been too slow, and up to now have failed to provide adequate and meaningful protection." Though industry has taken some steps, there is still no widespread adoption of provisions allowing consumer control and only a limited legally enforceable basis for relying on them.

Question 2a. Are there different recommendations for those websites targeting children?

Answer. We believe Congress should work toward providing a high level of protection to everyone's privacy online—adult and child alike. Strong protections that allow consumer control over sharing of personal information would benefit both children and adults. Within this framework, it might be necessary to provide heightened protection for children. For example, many advocates have called for special protections for sensitive information such as information related to a person's financial accounts, medical records or sexual orientation. Information on children could be placed in that category as well to assure that it receives the highest level of protection possible.

Question 2b. What about applications on phones?

Answer. Internet use on mobile phones raises two additional issues—location tracking and device identification. Mobile devices constantly record and track an individual's physical movements and the devices themselves often contain unique

identifying numbers that cannot be easily changed. This allows more robust and persistent tracking both in the physical and Internet space. This information can be gathered both by cell phone providers and applications running on those phones.

As of December 2009, more than 90 percent of the overall population of the United States subscribed to cell phone service—an estimated 285.6 million people. While cell phones are best known as devices used to make voice calls and send text messages, they are also capable of being used as tracking devices. As a result, cell phone technology has given many parties including the government, marketers, and employers an unprecedented new surveillance tool. The technical capacity now exists to track any one of the Nation's hundreds of millions of cell phone owners, for 24 hours a day, for as long as it likes. Whether it is a visit to a therapist or liquor store, church or gun range, many individuals' locations will be available either in real time or months later. Because of the sensitivity and invasiveness of location records, many advocates, including the ACLU argue for high standards for access to this information including a warrant based on probable cause for law enforcement access.

An example of the pervasiveness of this location tracking was recently described by the *New York Times.* According to the article a German lawmaker, Malte Spitz, gained access from his cell phone provider to all the location information associated with him (such access is required under German law). Using that information he was able to map his movements for 6 months. In another example, New York City attempted to fire an employee using cell phone records as evidence he was leaving work early.

Consumers are concerned about this intrusion. In a recent poll, 49 percent of respondents said they would be more comfortable with location-based services if they could more easily and clearly manage who sees their location information; 84 percent were concerned about the sharing of their location data without their consent; 84 percent were concerned about identity or data theft; and 83 percent were concerned about loss of privacy.

COMMENTS ON "THE STATE OF ONLINE PRIVACY," March 16, 2011

Adam Thierer, Senior Research Fellow, U.S. Senate, Committee on Commerce, Science, and Transportation

Published by the Mercatus Center, George Mason University and also available at *http://mercatus.org/sites/default/files/publication/comments-senate-hearing-state-online-privacy.pdf.*

As the Commerce Committee continues its exploration of online privacy issues, it is important that it ask some hard questions about the wisdom of imposing a comprehensive new regulatory regime on the Internet, which the Obama Administration appears to now favor. The Federal Trade Commission (FTC)[1] and Department of Commerce (DoC)[2] both released new privacy "frameworks" late last year and seem determined to move America toward a more "European-ized" conception of privacy regulation.[3]

Here are a few questions that should be put to the FTC and DoC officials, or those who support the direction they are taking us:

- Before implying that we are experiencing "market failure," why hasn't either the FTC or DoC conducted a thorough review of online privacy policies to evaluate how well organizational actions match up with promises made in those policies?
- To the extent *any* sort of internal cost-benefit analysis was done internally before the release of these reports, has an effort been made to quantify the potential size of the hidden "privacy tax" that new regulations like "Do Not Track" could impose on the market?
- Has the impact of new regulations on small competitors or new entrants in the field been considered? Has any attempt been made to quantify how much less entry/innovation would occur as a result of such regulation?

---

[1] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (December 2010), *http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.*

[2] U.S. Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,* U.S. Department of Commerce Internet Policy Task Force (December 2010).

[3] Adam Thierer, "Obama Admin's 'Let's-Be-Europe' Approach to Privacy Will Undermine U.S. Competitiveness," *Technology Liberation Front*, January 5, 2011, *http://techliberation.com/2011/01/05/obama-admins-lets-beeurope-approach-to-privacy-will-undermine-u-s-competitiveness/.*

- Were any economists from the FTC's Economics Bureau consulted before the new framework was released? Did the DoC consult any economists?
- Why do FTC and DoC officials believe that citing unscientific public opinions polls from regulatory advocacy organizations serves as a surrogate for serious cost-benefit analysis or an investigation into how well privacy policies actual work in the marketplace?
- If they refuse to conduct more comprehensive internal research, have the agencies considered contracting with external economists to build a body of research looking into these issues (as the Federal Communications Commission did in a decade ago in its media ownership proceeding)?
- Has either agency attempted to determine consumer's "willingness to pay" for increased privacy regulation?
- Has either agency explored the potential free speech issues that are at stake here since increased privacy regulation could potentially infringe legitimate First Amendment rights?
- More generally, where is the "harm"[4] and aren't there plenty of *voluntary* privacy-enhancing tools out there that privacy-sensitive users can tap to shield their digital footsteps, if they feel so inclined?

These are just some of the many of these questions explored in my recent filing to the Federal Trade Commission in its proceeding on *Protecting Consumer Privacy in an Era of Rapid Change*.[5] Because of the unique focus on the so-called "Do Not Track" mechanism as a potential silver-bullet solution to online privacy concerns, I am attaching the portion of my filing discussing the potential costs of such a mandated solution.

How a Mandatory "Do Not Track" Regime Creates Potential Risks to Consumers, Culture, Competition, and Global Competitiveness

More tailored forms of online advertising and the "tracking" technologies which make them possible are coming under increasing scrutiny today. Some of this can be attributed to a general unfamiliarity with how online advertising works and the role personal information and data collection play in the process.[6] Although, as noted above, no clear case of harm has been established, some privacy fundamentalists who oppose virtually *any* form data collection have elevated this concern to near "techno-panic" levels and are now demanding regulation.[7] As noted below, a variety of tools—such as, browser cookie controls or third-party plug-ins—already exist that can help consumers block targeted ads or limit data collection. But the Commission, likely inspired by regulatory advocates' claims of the complexity of those voluntary systems, is now pushing for additional steps to simplify or speed up the process. Hence, a "Do Not Track" mechanism has become the preferred universal fix, and one that the Commission is now pushing upon the marketplace. Do Not Track would demand that websites honor a machine-readable header indicating that the user did not want to be "tracked." In theory, this will allow privacy-sensitive web surfers to signal to websites that they would like to opt-out of any targeted advertising or not

---

[4] Berin Szoka and Adam Thierer, "Targeted Online Advertising: What's the Harm & Where Are We Heading? *Progress on Point* 16.2, (Washington, D.C.: The Progress & Freedom Foundation, February 13, 2009), *http://www.pff.org/issues-pubs/pops/2009/pop16.2targetonlinead.pdf*.

[5] Adam Thierer, Public Interest Comment on Protecting Consumer Privacy in an Era of Rapid Change86 (Arlington, VA: Mercatus Center at George Mason University), February 18, 2011, *http://mercatus.org/publication/public-interest-comment-protecting-consumer-privacy-era-rapid-change*. Also see, see Adam Thierer, "Unappreciated Benefits of Advertising and Commercial Speech," *Mercatus on Policy* 86 (Arlington, VA: Mercatus Center at George Mason University), January 2011, *http://mercatus.org/publication/unappreciatedbenefits-advertising-and-commercial-speech*.

[6] "Exaggerated fears are particular common regarding new technologies."." Kent Walker, "The Costs of Privacy," 25 *Harvard Journal of Law & Public Policy*, no 87, (Fall 2001), 126. A recent report by the U.K. government noted that "New media are often met by public concern about their impact on society and anxiety and polarisation of the debate can lead to emotive calls for action." *Safer Children in a Digital World*, Byron Review on Children and New Technology, Department for Children, Schools and Families, [U.K.] task force report, March 2008, 3, *http://www.dfes.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf*.

[7] "The privacy problem has morphed . . . into the latest terror of the digital ago, surpassing earlier shibboleths," argues Larry Downes. . . ." Larry Downes, "A Market Approach to Privacy Policy," in Berin Szoka and Adam Marcus, eds., *The Next Digital Decade: Essays on the Future of the Internet* (Washington, D.C.: TechFreedom, 2011), 510. Also see generally Adam Thierer, "Parents, Kids & Policymakers in the Digital Age: Safeguarding Against 'Techno-Panics,'" *Inside ALEC,* July 2009, 16–17, *http://www.alec.org/am/pdf/Inside_July09.pdf*.

have any information about them collected when visiting sites. The potential costs of such a regime will be explored in this section.

1. Potential Direct Cost to Consumers

The Commission poses a variety of questions regarding how a Do Not Track regime may be implemented and what its potential impact might be.[8] How many consumers would opt-out? How many would be willing to pay site subscriptions? How would it impact online publishers and advertisers? And so on. The truth is, nobody knows the answers to these questions, and the Commission has made no attempt to conduct a serious cost-benefit analysis of such a regime. Importantly, opinion polls cannot predict with accuracy how things will turn out once such a regime takes effect because consumer and marketplace reactions to real-world developments are more complex and nuanced than artificial surveys or experiments.[9]

What we do know is that online advertising today allows consumers to enjoy a veritable cornucopia of innovative, and mostly free, sites and services. Government regulation could "break" the implicit online *quid pro quo* currently governing online sites and services—that consumers enjoy a bevy of free content and services in exchange for tolerating ads and data collection—by creating what appears to be a cost-free choice option for consumers. That choice, however, will be anything but costless.

Lauren Weinstein, co-founder of People For Internet Responsibility (PFIR), worries that the "ability [of Do Not Track concepts] to cause major collateral damage to the Internet ecosystem of free Web services is being unwisely ignored or minimized by many Do Not Track proponents."[10] Weinstein is correct. There is no free lunch. While well-intentioned, government regulation that attempts to create a cost-free opt-out for data collection and targeted online advertising will likely have damaging unintended consequences. In terms of direct costs to consumers, Do Not Track could result in higher prices for service as paywalls go up or, at a minimum, advertising will become less relevant to consumers and, therefore, more "intrusive" in other ways.

Why might less relevant advertising represent a cost to consumers? It comes down to the value of their time and the benefits of relevant advertising to them. Ben Kunz, director of strategic planning at Mediassociates, a media planning and Internet strategy firm, argues that Do Not Track "won't stop online ads" but will instead simply lead to "tons of banners and videos everywhere online. They'll simply be less relevant."[11] *The Wall Street Journal* agrees, noting: "While many supporters of Do Not Track imagine that the opt-out would reduce the ads they see, the opposite would more likely occur, causing advertisers to blanket more media and use more intrusive techniques to reach the same number of potential customers."[12] When Google recently announced it would be offering a "Keep My Opt-Outs" extension to its Chrome web browser to come into line with the FTC's desire for more Do Not Track mechanisms, the company also noted that "once you install the Keep My Opt-Outs extension, your experience of online ads may change: You may see the same ads repeatedly on particular websites, or see ads that are less relevant to you."[13] Thus, Do Not Track "will stop marketers from serving up ads for products you may actually want," Kunz notes.[14] This represents a direct cost to consumers in terms of the hassle of unwanted, intrusive (or "spammy") advertising.

But it is the potential for prices to rise for online content and services that is the most important direct cost to consumers. If paywalls go up and subscriptions are required as a result of the new Do Not Track regime, Corey Kronengold of *Digiday* suggests the response of users could take one of two forms:[15]

---

[8] Federal Trade Commission, *Protecting Consumer Privacy*, A–4.

[9] *See, e.g.,* Berin Szoka, "Privacy Polls v. Real-World Trade-Offs," 5 *Progress Snapshot* 10 (Washington, D.C.: The Progress & Freedom Foundation, October 8, 2009), *http://www.pff.org/issues-pubs/ps/2009/ps5.10-privacy-pollstradeoffs.html*; Downes, "A Market Approach to Privacy Policy," 514.

[10] Lauren Weinstein, "Risks in Mozilla's Proposed Firefox 'Do Not Track' Header Thingy," Lauren Weinstein blog, January 24, 2010, *http://lauren.vortex.com/archive/000803.html*.

[11] Ben Kunz, "The $8 Billion Do Not Track Prize," *Bloomberg Businessweek*, December 22, 2010, *http://www.businessweek.com/technology/content/dec2010/tc20101222_392883.htm*.

[12] "The Internet Browsing Cops," January 21, 2011, *http://online.wsj.com/article/SB10001424052748704723104576061900000013690.html*.

[13] Sean Harvey and Rajas Moonka, "Keeping Your Opt-Outs," *Google Public Policy Blog*, January 24, 2010, *http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html*.

[14] Kunz, "The $8 Billion Do Not Track Prize."

[15] Corey Kronengold, "Taking Issue: The Value of Privacy," *Digiday*, December 16, 2010, *http://www.digidaydaily.com/stories/taking-issue-the-value-of-privacy*.

1. Users (especially those who are highly privacy sensitive) might gladly accept the trade-off and pay something more for those sites and services instead of having data collected or ads served; or,

2. Users might revolt against the resulting paywalls, subscriptions, micropayment schemes, tiered services, etc, and demand government intervention in the name of "fairness." We might even hear talk of "gouging" and calls for price regulation, even though developers would have no choice but to raise prices to cover costs in the absence of advertising support.

Some mix of the two could be the end result, but the latter scenario seems far more likely. "If we move too far one way, the people supplying the free content *will* get together and say we aren't going to supply the content for free," says Dilip DaSilva, chief executive of Exponential Interactive, owner of the Tribal Fusion online advertising network. "It's not like the publishers will offer free content to people who visit their site but don't want ads tracking them."[16]

Of course, there is nothing wrong with online sites and service providers charging for what they offer consumers, but, as Kronegold suggests, if regulation moves the marketplace in that direction unnaturally, many consumers will likely have a problem with it since they have grown accustomed to an abundance of "free" online services. It is impossible to determine what prices online providers might seek to charge for their services, but anything more than the $0.00 they currently charge will likely come as a shock to many consumers. As discussed in the following section, it will also have profound repercussions on the broader availability of much content and many of the services consumers take for granted. In this sense, Do Not Track becomes a "privacy tax" on consumers, requiring them to pay for things they previous received inexpensively, or for free.[17]

There are other costs associated with the process of creating paywalls and setting prices that will be borne by online content providers and consumers, as Commissioner William Kovacic noted in his statement on the Commission's privacy report:

> Setting prices is costly; if willingness to pay to avoid tracking varies substantially, the informational requirements to set access prices will be large. For a number of content providers, a price-for-content model is likely to provide less revenue than monetization via advertising; that most websites choose an ad-driven model rather than a direct fee model suggests that the former is a more efficient means than the latter to monetize content in most circumstances. At the margin—which may be large—forcing firms away from their revealed-preferred method of monetization may reduce revenue and hence degrade quality. In discussing whether website content might be degraded by consumers choosing not to be tracked, how, if at all, should such risks impact the Commission's analysis?[18]

How much content will go behind paywalls? Dan Castro of the Information Technology & Innovation Foundation fears much will:

> If a Do Not Track list ever became widely implemented companies could respond by simply blocking access to those sites for users who opt out, just as some sites today block users who use ad-blocking software or do not register on a site. Users who currently opt out of targeted advertising but continue to use the content or service which the advertising pays for are essentially free riders. They are the minority of users who are benefiting from the willingness of the majority to divulge some personal information in exchange for free or reduced-price content. It is this exchange that enables the U.S. Internet ecosystem to be so robust and largely free of charge to the average user. Privacy advocates rarely acknowledge the harm to advertising revenues that would result from a large number of consumers signing up for Do Not Track.[19]

Another alternative short of paywalls would be interstitial pop-ups warning consumers they must first disable Do Not Track before they are allowed to use portions

---

[16] Quoted in Tanzina Vega and Verne Kopytoff, "In Online Privacy Plan."

[17] "We might better think of a privacy tax—we pay the regular price unless we want to keep information about our food, alcohol, and pharmaceutical purchases from the market; to keep our habits to ourselves, we pay extra." Hal Abelson, Ken Ledeen, and Harry Lewis, *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion* (Upper Saddle River, NJ: Addison-Wesley, 2008), 11.

[18] Concurring Statement of Commissioner Kovacic, in Federal Trade Commission, *Protecting Consumer Privacy*, D–4.

[19] Daniel Castro, "Policymakers Should Opt Out of 'Do Not Track'," Information Technology & Innovation Foundation, November 2010, 3, *www.itif.org/files/2010-do-not-track.pdf*.

of the site, or perhaps any of it.[20] In other words, sites may seek to formalize the previously unwritten *quid pro quo* of information as currency. Some Do Not Track regulatory advocates try to assuage such concerns by pointing to the existence of widespread online website registration or site "login" procedures today, which do not generally require user to disable settings (such as cookie-blocking or ad-blocking) or pay anything before using site content/services. For example, Arvind Narayanan of Stanford University argues:

> I do not believe that disabling DNT as a requirement for service will become anywhere near as prevalent as logging in as a requirement for service. I bring up login only to make the comforting observation there seems to be a healthy equilibrium between sites that require login always, some of the time, or never.[21]

Ultimately, however, this observation provides little comfort since it ignores the fact that Do Not Track could be preemptively breaking business models on an unprecedented scale, thus forcing vast numbers of online publishers to make uncomfortable trade-offs going forward if they wish to provide the current level of service or expanded options. Narayanan may end up being correct and a highly tiered, permission-based Internet may not be erected. But, as the next section notes, that is a risky bet and one that could have profound consequences for the future online content and the richness of its culture.

2. Potential Indirect Costs/Impact on Content & Culture

Direct monetary cost to consumers is not the only issue here. The indirect impact of regulation on content and culture must also be considered.

While targeted online advertising only accounted for $1.1 billion in 2010, it has been growing at healthy 20 percent clip, estimates eMarketer.[22] "Factor in the use of data to determine marketing efficiencies and that figure could be as high as $7 billion to $8 billion of the $25 billion online ad spend," says Katy Bachman of *AdWeek*.[23] Larry Ponemon, Chairman of the Ponemon Institute, which studies privacy and security issues, told the *New York Times* that "Privacy fears are definitely having an economic impact" on the market, especially the uncertain legal and regulatory environment and the threat of regulation.[24] A May 2010 Ponemon Institute survey of senior marketing executives with 90 diverse organizations that were actively engaged in online marketing found that:

> 63 percent of those we surveyed said behavioral advertising generated their *greatest return on investment*. Yet 98 percent told us that, because of consumers' privacy fears, their companies are curtailing investments in online behavioral targeting. These companies are willing to sacrifice the revenue they believe they can generate through an online campaign rather than risk the potential hit to brand reputation for being as aggressive as they would like to be. Overall that curtailment has kept more than $600 million out of the behavioral targeting industry.[25]

This matters because it represents foregone investment in new forms of content, culture, and services. Media economists and industry experts have long realized that advertising is the great sustainer of media.[26] Advertising benefits society by subsidizing the creation of news, information, and entertainment. "Advertisers are critical to the success of commercial media because they provide the primary revenue stream that keeps most of them viable," argues Robert G. Picard, author of *The Eco-*

---

[20] Ironically, depending on how such permission systems are structured, this may actually end up forcing consumers to reveal more information about themselves to many sites as a condition of access content or services on those sites.

[21] Arvind Narayanan, "'Do Not Track' Explained," *33 Bits of Entropy*, September 30, 2010, *http://33bits.org/2010/09/20/do-not-track-explained.*

[22] David Hallerman, "Audience Ad Targeting: Data and Privacy Issues," eMarketer, February 2010, *http://www.emarketer.com/Reports/All/Emarketer_2000636.aspx*.

[23] Katy Bachman, "(Ad) Apocalypse Soon," *AdWeek*, December 19, 2010, *http://www.adweek.com/aw/content_display/esearch/e3i9f75082f2f627711694ca34d9b326105*.

[24] Quoted in Steve Lohr, "Privacy Concerns Limit Online Ads, Study Says," *New York Times*, April 30, 2010, *http://bits.blogs.nytimes.com/2010/04/30/privacy-concerns-limit-online-ads-study-says*.

[25] Larry Ponemon, "Fear and Loathing in Online Advertising," Ponemon Institute blog, May 3, 2010, *http://www.ponemon.org/blog/post/fear-and-loathing-in-online-advertising*.

[26] For a summary, see Adam Thierer, "Unappreciated Benefits of Advertising and Commercial Speech," *Mercatus on Point* 86 (Arlington, VA: Mercatus Center at George Mason University), January 2011, *http://mercatus.org/publication/unappreciated-benefits-advertising-and-commercial-speech*.

nomics and Financing of Media Companies.[27] Mary Alice Shaver of the University of Central Florida puts this support in context: "Advertising revenues pay for virtually all broadcast media, 70 percent to 80 percent of support for newspapers and an equally high percentage for magazines."[28]

Importantly, advertising is proving increasingly to be the only business model with any real staying power for many media and information-producing sectors. Pay-per-view mechanisms, micropayments, and even subscription-based business models are all languishing.[29] Consequently, the overall health of modern media marketplace and the digital economy—and the aggregate amount of information and speech that can be produced or supported by those sectors—is fundamentally tied up with the question of whether policymakers allow the advertising marketplace to evolve in an efficient, dynamic fashion.[30] In this sense, it is not hyperbole to say that an attack on advertising is tantamount to an attack on media itself.[31]

A March 2010 study on "The Value of Behavioral Targeting," conducted by Howard Beales on behalf of the Network Advertising Initiative, demonstrates how this could be the case.[32] Beales, the former Director of the Bureau of Consumer Protection at the FTC, found that advertising rates are significantly higher for behaviorally targeted ads, with the average return on behaviorally targeted advertising being just over twice that of other advertising. The reason that greater return on investment is important, Beales notes, is because:

> Advertising using behavioral targeting is more successful than standard run of network advertising, creating greater utility for consumers from more relevant advertisements and clear appeal for advertisers from increased ad conversion. Finally, a majority of network advertising revenue is spent acquiring inventory from publishers, making behavioral targeting an important source of revenue for online content and services providers as well as third party ad networks.[33]

This illustrates how more effective advertising can cross-subsidize and sustain online content and culture. More and better advertising means more and better content and services will be made available to consumers. Beales concluded his study by noting: "Increasingly, advertising is the financing mechanism that makes online content and services possible as well. As content traditionally provided offline (such as newspapers) continues to move to the Internet, the link between online advertising and content is likely to become increasingly vital to the provision of information and services that we have long taken for granted."[34]

With these insights in mind, it is peculiar that the Commission ignores the connection between this proceeding and another FTC proceeding which poses the question, "How Will Journalism Survive the Internet Age?"[35] That is a fair question for the FTC to ask, and one that the Federal Communications Commission has also

---

[27] Robert G. Picard, *The Economics and Financing of Media Companies* (Bronx, NY: Fordham University Press, 2002), 122.

[28] Mary Alice Shaver, "The Economics of the Advertising Industry," in Alison Alexander, *et. al., Media Economics: Theory and Practice* (Mahwah, NJ: Lawrence Erlbaum Associates, Third Edition, 2004), 250.

[29] To some extent, these are all just variations of a fee-for-service business model. "Micropayments," for example, would require a small payment for each media unit accessed or downloaded, such as $1 per news article or song.

[30] Much of the valuable information content available on the Internet, and so many of the useful services we use every day, is free," explains Larry Downes, "not because of some utopian dream of inventors or even because of the remarkably low transactions costs of the digital economy. The content is free because the costs of the services—blogs, stock quotes, even home movies posted on YouTube—are underwritten by advertisers. If we don't read and respond to ads, we'll have to pay for these services some other way," he notes. Downes, *The Laws of Disruption*, 83–4.

[31] See Adam Thierer, Berin Szoka, and W. Kenneth Ferree, *Comments of the Progress & Freedom Foundation in the Matter of the Federal Communications Commission's Examination of the Future of Media and Information Needs of Communities In a Digital Age*, The Progress & Freedom Foundation, May 5, 2010, 28–38, *http://www.pff.org/issues-pubs/testimony/2010/2010-05-05-Comments_in_FCC_Future_of_Media_proceeding.pdf*.

[32] Howard Beales, "The Value of Behavioral Targeting," Network Advertising Initiative, March 2010, *www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf*.

[33] *Ibid.*, 1.

[34] *Ibid.*, 18.

[35] Federal Trade Commission, "How Will Journalism Survive the Internet Age?" Workshop Series, 2010, *http://www.ftc.gov/opp/workshops/news/index.shtml*. All filing made to the Commission in the proceeding are located here: *http://www.ftc.gov/os/comments/newsmediaworkshop/index.shtm*.

been pondering in a series of workshops on "The Future of Media."[36] What the Commission proposes in this proceeding certainly will not help matters any and it begs the question: If not advertising, then what will sustain online media, digital age culture, and social networking services going forward?[37]

John Battelle is blunter in his assessment of how damaging this move could be to online culture:

> don't come crying to me when you realize that in opting out of our marketing-driven world, you've also opted out of, well, a pretty important part of our ongoing cultural conversation, one that, to my mind, is getting more authentic and transparent thanks to digital platforms. And, to my mind, you've also opted out of being a thinking person capable of filtering this stuff on your own, using that big ol' bean which God, or whoever you believe in, gave you in the first place. Life is a conversation, and part of it is commercial. We need to buy stuff, folks. And we need to sell stuff too.[38]

This is a simplified explanation of the value exchange that drives the Internet, but Battelle is correct that if heavy-handed regulation replaces common sense or the current online quid pro quo of information-forservices, then something must give. While the idea of a cost-free opt-out model for the all online data collection/advertising may sound seductive to some, it is vital to take into account the opportunity costs of such regulation. The real world is full of trade-offs and there is no such thing as a free lunch.

3. Competition & Market Structure

The Commission does not need to be reminded that it was created in large part to safeguard competition. This proceeding, however, threatens to tip the balance in favor of existing technologies or market players over future ones.[39] *AdWeek*'s Katy Bachman argues that:

> Heavy-handed privacy legislation could actually curb competition by crippling ad networks that serve ads to niche Websites dependent on advertising to fund content. Websites would have to resort to pay models in a medium where free content is the norm. No doubt the big brands would still draw contextual advertising, but that would come at the expense of new, emerging brands, thus squelching competition in a space that has thrived on it.[40]

Similarly, Tanzina Vega and Verne Kopytoff of *The New York Times* have noted that:

> The Federal Trade Commission's proposed privacy mechanism could cause a major shift in the online advertising industry, as companies that have relied on consumers' browsing history try to make up for what could be billions in lost revenue.
>
> If the vast majority of online users chose not to have their Internet activity tracked, the proposed "do not track" system could have a severe effect on the industry, some experts say. It would cause major harm to the companies like online advertising networks, small and midsize publishers and technology companies like Yahoo that earn a large percentage of their revenue from advertising that is tailored to users based on the sites they have visited.
>
> Under a situation where many users opt out of being tracked, other companies, like Google, may take a much smaller hit because the vast majority of its revenue comes through search ads that would not be affected by a do-not-track mechanism. Microsoft, which also sells display advertising through its ad net-

---

[36] Federal Communications Commission, "Future of Media," *http://reboot.fcc.gov/futureofmedia*.

[37] Castro goes even further, arguing that "If the goal of the initiative is to restrict targeted advertising, it would be better for Congress to just ban Internet advertising outright and develop a 'Corporation for Public Internet' to fund Internet content and applications." Castro, "Policymakers Should Opt Out of 'Do Not Track'," 4.

[38] John Battelle, "Thurs. Signal: Go On, Opt Out. Just Don't Come Cryin' To Me . . ." *Federated Media Publishing,* December 1, 2010, *http://www.federatedmedia.net/blog/2010/12/thurs-signal-go-on-opt-out-just-don't-come-cryinto-me*.

[39] "Regulation that disfavors one technology or business model would also deter entry, thwart innovation, and limit competition and choice in the sale of online advertising." Joan Gillman, *Testimony before the House Energy & Commerce Committee, Hearing on Do Not Track Legislation: Is Now the Right Time?* December 2, 2010, 5, *http://energycommerce.house.gov/hearings/Testimony.aspx?TID=4184*.

[40] Katy Bachman, "(Ad) Apocalypse Soon," *AdWeek*, December 19, 2010, *http://www.adweek.com/aw/content__display/esearch/e3i9f75082f2f627711694ca34d9b326105*.

> work, could also survive a hit to user data collection since it earns revenue from sources other than advertising, including software and gaming, experts say.[41]

"In a setting where first-party advertising is allowable but third-party marketing is not, substantial advantages may be created for large incumbent firms," argue Avi Goldfarb and Catherine Tucker.[42] "For example, if a large website or online service were able to use its data to market and target advertising, it will be able to continue to improve and hone its advertising, while new entrants will find it difficult to challenge the incumbent's predominance by compiling other data or collecting their own data," they conclude.[43]

And Kunz fears that "the 'Long Tail' of niche content is going to get crushed" since "thousands of small websites may disappear as dollars flow to consolidated publishing centers." "Do Not Track will send billions of dollars to the big online publishers, hurting the little sites you might find most interesting. The second point is painful. It could really harm you, too, dear consumer, if you read things online other than *The New York Times*, Bloomberg, or iVillage.com."[44] This should hardly be surprising since economists have long recognized that "advertising typically benefits new entrants and small firms more than it does large, established firms,"[45] and that is likely to be the case for targeted online advertising since it would be the easiest way for niche sites to find interested consumers and advertisers.

Thus, the risk exists that a Do Not Track mandate could steer markets in unnatural, inefficient directions by erecting new barriers to entry or directly picking technological winners and losers.[46] If so, the Commission will have failed in its mission to safeguard competition and improve consumer welfare.

4. International Competitiveness

Some advocates of intervention on this front do not hide their desire to move the United States in a direction the European Union has followed with "data directives" and more stringent forms of privacy regulation. But America's refusal thus far to walk down that more regulatory path offers scholars the chance to evaluate Europe's more-restrictive approach and study whether America's lead in the global digital marketplace might be tied to its more "hands-off" approach to online regulation. A recent study by Goldfarb and Tucker found that "after the [European Union's] Privacy Directive was passed [in 2002], advertising effectiveness decreased on average by around 65 percent in Europe relative to the rest of the world."[47] They argue that because regulation decreases ad effectiveness, "this may change the number and types of businesses sustained by the advertising-supporting Internet." Regulation of advertising and data collection for privacy purposes, it seems, can affect the global competitiveness of online firms.

This is what makes talk of "harmonization" among privacy regimes so dangerous. It threatens to undermine America's competitive advantage in the global digital arena. It is hard to find many European counterparts that rival Google, Amazon, Apple, Facebook, eBay, Microsoft, or other market leaders. Why is it that the information technology sector has thrived in America and that U.S. companies are leaders in many of their respective sectors across the globe? Might it be precisely because the U.S. did *not* follow others down the path of "data directives" and heavy

---

[41] Tanzina Vega and Verne Kopytoff, "In Online Privacy Plan, the Opt-Out Question Looms," *New York Times,* December 5, 2010, *http://www.nytimes.com/2010/12/06/business/media/06privacy.html*.

[42] Avi Goldfarb and Catherine Tucker, "Comments on 'Information Privacy and Innovation in the Internet Economy,'" Comments to the U.S. Department of Commerce, January 24, 2011, 4, *http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/NTIA__comments__2011__01__24.pdf*.

[43] *Ibid.*

[44] Kunz, "The $8 Billion Do Not Track Prize."

[45] Thomas M. Lenard and Paul H. Rubin, *Privacy and the Commercial Use of Personal Information* (Washington, D.C.: The Progress & Freedom Foundation, 2002), xxii.

[46] As the National Cable and Telecommunications Association (NCTA) noted in comments to the Department of Commerce: "In a nascent and highly dynamic market characterized by rapid technological change such as online advertising, any regulation that favors or disfavors one technology or business model over another could seriously thwart innovation and the development of new business models that could benefit consumers, content providers, and advertisers, by prematurely locking market participants into one sanctioned approach. Moreover, limiting online advertising to specified designated permissible techniques would deter new entry, and limit competition." National Cable and Telecommunications Association, *Reply Comments to the U.S. Department of Commerce,* January 28, 2011, 10–11. *http://www.ntia.doc.gov/comments/101214614–0614–01/comment.cfm?e=17AF54FD-5201-474A-8EB8-E8B6071AEDEC*.

[47] Avi Goldfarb and Catherine Tucker, "Privacy Regulation and Online Advertising," 57 *Management Science* 1, (January 2011), 57–71, *http://papers.ssrn.com/sol3/papers.cfm?abstract__id=1600259*.

handed, top-down regulation of the Internet more generally? "If applied to American companies, these European laws would restrict the breakneck innovation of the commercial web," argues the NetChoice Coalition.[48] And Yahoo! correctly summarizes:

> It is no coincidence that the U.S. is the birthplace of most of the widely used global websites and online services. Our legal frameworks encourage innovation through reasonable liability regimes, controls on harmful uses of information, promotion of a diversity of online voices, security requirements based on the sensitivity of the data, and a light regulatory hand that favors and recognizes complementary roles for industry self-regulation.[49]

The Department of Commerce's recent privacy green paper says America should look to "prevent conflicting policy regimes from serving as a trade barrier."[50] But should the U.S. impose burdensome new regulations on American companies to achieve that goal? Would we really be better off if all U.S. firms and policy more closely resembled the E.U. in this regard?

Some privacy advocates posit the need for greater "interoperability" or harmonization of privacy policies internationally to facilitate smoother online commercial interactions or data flows. Yet, the Commerce Department's recent privacy green paper notes that "a considerable amount of global commerce takes place on the Internet [and] global online transactions currently total an estimated $10 trillion annually" and is growing. Still, it continues on to claim that "the lack of cross-border interoperability in privacy principles and regulations creates barriers to cross-border data flow and significant compliance costs for companies,"[51] and repeats the argument for harmonization.

There are three problems with that theory. First, it assumes that the benefits of regulatory harmonization—*which, to be perfectly clear, would arrive in the form of increased regulation on U.S. operators*—would outweigh the cost of complying with those new rules.

Second, there is no reason that harmonization could not work in the opposite direction. If the Commerce Department, the FTC and other U.S. lawmakers want to promote U.S. trade, exports, commerce, and global competitiveness, the proper way to "leveling the playing field" in this context should be the same as it is in relation to speech policy or trade law: the rest of the world should follow America's lead; the U.S. should absolutely not regulate up to achieve parity with theirs.

Which raises a final problem with the argument for harmonization of privacy regimes through increased regulation on U.S. businesses: it sets a horrible precedent. At least thus far this has not been the approach the U.S. Government has taken in most other Internet policy contexts, and with good reason. Consider this in the context of speech controls. When policymakers in Europe and other regions or countries stifle free speech and expression online, America's response has not been to mimic them but, rather, to lead by example. That is, when confronted with conflicting regulatory regimes abroad, our response has usually been to proudly boast to the world that we have the more sensible approach to Internet regulation, which is to say, it should be tightly limited so as not to stifle speech or commerce. Some critics might label this "American exceptionalism," but it is really just common sense if we hope to promote the international competitiveness of U.S. online businesses and remain a global leader in this arena.

5. "Silver-Bullet" Solutions Rarely Adapt or Scale Well

Finally, there is the more general normative problem of the Commission seeking a simple solution to a complex "problem" such as online privacy protection. Do Not Track fits into a long line of proposed silver-bullet solutions that would mandate a "universal" solution to a complicated economic or social issue.

When it comes to such information control efforts, there aren't many good examples of simple fixes or silver-bullet solutions that have worked, at least not very long. Consider the illusive search for a solution to online pornography. The PICS/ICRA experience is instructive in this regard. PICS and ICRA refer to the W3C's Platform for Internet Content Selection[52] and Internet Content Rating Associa-

---

[48] Steve DelBianco and Braden Cox, NetChoice Reply Comments on Department of Commerce Green Paper, January 28, 2011, 7, *http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=1EA98542–23A4-4822-BECD-143CD23BB5E9.*

[49] Anne Toth, Comment of Yahoo! on *Commercial Data Privacy and Innovation in the Internet Economy*, January 28, 2011, 2, *http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=F6A50C0B-00CC-44A6-B475-FE218170CA02.*

[50] Department of Commerce, *Commercial Data Privacy and Innovation*, 20.

[51] *Ibid.*

[52] *http://www.w3.org/PICS.*

tion.[53] For a time, there was hope that voluntary metadata tagging and content labeling could be used to screen objectionable content on the Internet. But the sheer volume of material to be dealt with made that task almost impossible. The effort has been abandoned now.[54] Of course, it is true that effort did not have a government mandate behind it to encourage more widespread adoption, but even if it would have, it is hard to believe that all pornography or other objectionable content would have been labeled and screened properly.

In a similar way, The CAN–SPAM Act aimed to curtail the flow of unsolicited e-mail across digital systems and, yet, failed to do so. Private filtering efforts have helped stem the flow to some extent, but have not eliminated the problem altogether. Royal Pingdom estimates that in 2010 89.1 percent of all e-mails were spam.[55] "Spam pages," are also a growing concern. In January 2011, Blekko, a new search engine provider, created a "Spam Clock" to track new spam pages and found 1 million new spam pages were being created *every hour*.[56]

Similar problems await information control efforts in the privacy realm, even if a mandated Do Not Track mechanism required the re-engineering of web browser architecture and/or standards. "It's a single response to an overly-simplifies set of choices we encounter on the web," notes the NetChoice Coalition, which represents e-commerce companies.[57] Also, Do Not Track "does not address mobile or app data, nor any data created outside a traditional web browser," notes Michael Fertik, CEO of Reputation.com.[58] "At the same time, the growth in technology and understanding can render current solutions inadequate. A privacy rule to limit behavioral advertising today might not work in the future when more data is available and there are more powerful algorithms to process it," he says. "There is no reliable way of ensuring this technology is being used, however," says Sidney Hill of *Tech News World*. "Ensuring compliance with antitracking rules will become even *more* difficult as more users turn to mobile devices as their primary means of connecting to the Web."[59]

Importantly, Do Not Track would not slow the "arms race" in this arena as some seem to hope or suggest.[60] If anything, as noted in more detail below, a Do Not Track mandate will speed up that arms race and have many other unintended consequences.[61] Complex definitional questions also remain unanswered, such as how define and then limit "tracking" in various contexts, as well as how to enforce such a regime. Lauren Weinstein summarizes some of the most obvious issues:

> Sending out a new "Do Not Track" header—even beyond basic associated technical requirements at the client and server ends—and even if there's agreement on how that header is defined—tells you nothing about what actually happens to that header after being sent by the client browser. How does the user who sends such a header actually confirm that they're "not being tracked" as a result? And how do they know that continued tracking isn't caused by a technical

---

[53] *http://www.fosi.org/icra.*

[54] *http://www.icra.org.*

[55] Royal Pingdom, "Internet 2010 in Numbers," January 12, 2011, *http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers*.

[56] *http://www.spamclock.com.* Also see, Danny Sullivan, "Blekko Launches Spam Clock To Keep Pressure On Google," *Search Engine Land*, January 7, 2011, *http://searchengineland.com/blekko-launches-spam-clock-tokeep-pressure-on-google-60634*.

[57] Steve DelBianco and Braden Cox, *NetChoice Reply Comments on Department of Commerce Green Paper*, January 28, 2011, 14, *http://www.ntia.doc.gov/comments/101214614–0614–01/comment.cfm?e=1EA98542-23A4-4822-BECD-143CD23BB5E9*.

[58] Michael Fertik, *Comments of Reputation.com, Inc. to the U.S. Department of Commerce*, January 28, 2011, 12, *http://www.reputation.com/blog/2011/01/31/reputation-com-comments-commerce-department-privacy-greenpaper.*

[59] Sidney Hill, "Internet Tracking May Not Be Worth the Headaches," *Tech News World,* December 29, 2010, *http://www.technewsworld.com/story/Internet-Tracking-May-Not-Be-Worth-the-Headaches-71543.html*.

[60] Some examples: "The header-based Do Not Track system appeals because it calls for an armistice in the arms race of online tracking." Rainey Reitman, "Mozilla Leads the Way on Do Not Track," *Deeplinks*, Electronic Frontier Foundation, January 24, 2011, *https://www.eff.org/deeplinks/2011/01/mozilla-leads-the-way-on-do-not-track.* Similarly, Chris Soghoian argues that "opt out mechanisms . . . [could] finally free us from this cycle of arms races, in which advertising networks innovate around the latest browser privacy control." Christopher Soghoian, "What the U.S. Government Can Do To Encourage Do Not Track," *Slight Paranoia*, January 27, 2011, *http://paranoia.dubfire.net/2011/01/what-us-government-can-do-to-encourage.html.* Finally, Arvind Narayanan of Stanford University argues that Do Not Track, "is a way to move past the arms race between tracking technologies and defense mechanisms, focusing on the actions of the trackers rather than their tools." Arvind Narayanan, "'Do Not Track' Explained," *33 Bits of Entropy*, September 30, 2010, *http://33bits.org/2010/09/20/do-not-track-explained.*

[61] "Too often, well-intentioned efforts to regulate technology are far worse than the imagined evils they were intended to prevent." Abelson, Ledeen, and Lewis, *Blown to Bits*, 159.

> issue that prevented the header from ever being received and processed by the destination server?
>
> Perhaps the header line was "eaten" by an intermediate proxy server (it's quite common for proxies not to pass along all headers). Or maybe the header reached a server that simply hadn't been modified to recognize it yet. Or did the header reach a server in some jurisdiction (say, outside of the U.S.) that wouldn't even be "required" to know about that new header? And so on.
>
> You can't just send a Do Not Track header and expect meaningful results. In practice, you end up having to build an entire confirmation apparatus of some sort—and even then it's likely to be a mess. Without confirmation, you can send out whatever headers you wish, but when you don't get the results you expect, what does that mean? Who knows? This all gets very complicated, very quickly.[62]

Moreover, in light of the global nature of online commerce and speech, Do Not Track will not scale as well as advocates hope.[63] Castro says:

> Another problem with Do Not Track is that it does not scale well on the global Internet. As described above, to be effective, the proposal would require a Federal mandate calling for substantive modifications to networking protocols, web browsers, software applications and other Internet devices. Besides raising costs for consumers, it is unclear how effective such a mandate would be outside of the U.S. borders or how well the proposal would be received by international standard bodies.[64]

Again, as noted previously, the regulatory experience with spam, objectionable content, and copyrighted content suggest serious challenges lie ahead because of the borderless nature of online activity /commerce.

6. Implications of This New Regime in Other Contexts

A final danger with the FTC's proposed Do Not Track information control regime is that it could also establish a precedent for other forms of Internet regulation. If, in the context of privacy policy, "opt-in" becomes the new default norm or mechanisms such as Do Not Track become the preferred top-down mandate, similar regulatory norms might be expected in other contexts. Why not mandatory "opt-in" for other types of speech or content? For example, should the presence of potentially objectionable content across digital networks be used as an excuse for greater regulation of the Internet?

That is not the way things currently work, of course. At least in the United States, we demand that personal and parental responsibility be the first and primary line of defense against unwanted communications or content. Why should it be any different when it comes to "privacy" concerns?[65]

Consider how things work in the context of speech and content regulation, American jurisprudence has become a fairly settled matter: people (or parents) are expected to take responsibility for unwanted information flows in their lives (or the lives of their children). Under current law, it is assumed that the many user empowerment tools on the market (filters, monitoring software, other parental control technologies) constitute a so-called "less-restrictive means" of controlling content when compared to government regulation.

Many privacy advocates—such as ACLU, the Center for Democracy & Technology, and the Electronic Frontier Foundation—vociferously endorse this "less-restrictive means" test or "educate and empower" paradigm in the free speech context. Generally speaking, when it comes to speech regulation, they rightly argue "household standards" (user-level controls) should trump "community standards" (government regulation). And in Court they repeatedly employ the "less-restrictive means" test to counter government efforts to regulate information flows.

---

[62] Lauren Weinstein, "Risks in Mozilla's Proposed Firefox "Do Not Track" Header Thingy," Lauren Weinstein blog, January 24, 2010, *http://lauren.vortex.com/archive/000803.html*.

[63] "Many behavioral targeting companies are based outside the US—making legislation ineffective," says Doug Wolfgram, CEO of IntelliProtect, an online privacy management company. Quoted in Tony Bradley, "Why Browser 'Do Not Track' Features Will Not Work," *Computerworld*, February 10, 2011, *http://news.idg.no/cw/art.cfm?id=ACE91A0E-1A64-6A71-CE2572C981C0204A*.

[64] Castro, "Policymakers Should Opt Out of 'Do Not Track'," 3.

[65] The Cato Institute's Jim Harper argues: "Privacy is not a gift from politicians or an entitlement that can be demanded from government. Privacy is a product of personal responsibility. Like moral living, privacy is the product of careful consideration and concerted effort by individuals. To be sure, protecting privacy can be hard. It involves knowledge, vigilance, and constant trade-offs." Harper, "Understanding Privacy," 5.

When it comes to privacy, however, many of them abandon this vision. For some reason, when the topic of debate shifts from concerns about potentially objectionable content to the free movement of personal information, personal responsibility and self-regulation become the *last* option, not the first. What is most troubling about this is that those advocates could be unwittingly undermining the power of the "less restrictive means" test more generally, which is a vitally important barrier to greatly enhanced government control of cyberspace. That is, when privacy advocates ignore, downplay, or denigrate user empowerment tools, they are essentially saying self-help is the right answer in one context, but not the other.

That is a shame because, as discussed below, self-help tool work well in both contexts. And the same arguments used against private parental empowerment technologies are often trotted out in opposition to privacy controls. Can privacy tools be confusing at times or difficult to set up? Yes, they can, but no more so that parental control tools. Are privacy tools as effective as parental control tools? In some ways privacy tools are actually more effective because in the case of parental controls, the person you are attempting to "protect" (namely, kids) often have a stronger incentive to evade/defeat those tools. Moreover, privacy-enhancing controls can be very effective—perhaps even *too effective*—at shutting down unwanted information flows. Whether it is ad-blocking tools, cookie controls, or encryption techniques, these tools can actually be far more effective blocks on information flows than, say, Internet filters meant to block porn or hate speech, which is also more subjective by nature.

Of course, no technological empowerment tool or solution is perfect. But as the Supreme Court held in *United States* v. *Playboy,* empowerment tools need not be perfect to be preferable to government regulation. "Government cannot ban speech if targeted blocking is a feasible and effective means of furthering its compelling interests," the Court held.[66] Moreover, "It is no response that voluntary blocking requires a consumer to take action, or may be inconvenient, or may not go perfectly every time. A court should not assume a plausible, less restrictive alternative would be ineffective; and a court should not presume parents, given full information, will fail to act."[67]

Again, the exact same principle should hold for privacy regulation[68] Why not expect those especially privacy-sensitive users who object to targeted online advertising to do something about it? To the extent effective self-help privacy tools exist, they provide a means of solving policy problems that is not only "less restrictive" than government regulation but generally more *effective* and customizable as well. Why settle for one-size-fits-all solutions of incomplete effectiveness when users can quite easily and effectively manage their own privacy? Indeed, those who advocate personal responsibility and industry self-regulatory approaches to free speech and child protection issues should be advancing the same position with regards to privacy.

○

[66] *United States* v. *Playboy Entertainment Group,* 529 U.S. 803, 815 (2000).

[67] *Ibid.*, 824.

[68] Chapman University Law Professor Tom Bell has argued the same principle should hold in both contexts. Tom W. Bell, "Internet Privacy and Self-Regulation: Lessons from the Porn Wars," *Briefing Paper* 65 (Washington, D.C.: Cato Institute, August 9, 2001), *http://www.cato.org/pub_display.php?pub_id=1504.*