

DO-NOT-TRACK LEGISLATION: IS NOW THE RIGHT TIME?

HEARING
BEFORE THE
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION
OF THE
COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES
ONE HUNDRED ELEVENTH CONGRESS
SECOND SESSION
DECEMBER 2, 2010
Serial No. 111-161



Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

78-138

WASHINGTON : 2013

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

COMMITTEE ON ENERGY AND COMMERCE

HENRY A. WAXMAN, California, *Chairman*

JOHN D. DINGELL, Michigan

Chairman Emeritus

EDWARD J. MARKEY, Massachusetts

RICK BOUCHER, Virginia

FRANK PALLONE, Jr., New Jersey

BART GORDON, Tennessee

BOBBY L. RUSH, Illinois

ANNA G. ESHOO, California

BART STUPAK, Michigan

ELIOT L. ENGEL, New York

GENE GREEN, Texas

DIANA DeGETTE, Colorado

Vice Chairman

LOIS CAPPS, California

MICHAEL F. DOYLE, Pennsylvania

JANE HARMAN, California

TOM ALLEN, Maine

JANICE D. SCHAKOWSKY, Illinois

CHARLES A. GONZALEZ, Texas

JAY INSLEE, Washington

TAMMY BALDWIN, Wisconsin

MIKE ROSS, Arkansas

ANTHONY D. WEINER, New York

JIM MATHESON, Utah

G.K. BUTTERFIELD, North Carolina

CHARLIE MELANCON, Louisiana

JOHN BARROW, Georgia

BARON P. HILL, Indiana

DORIS O. MATSUI, California

DONNA M. CHRISTENSEN, Virgin Islands

KATHY CASTOR, Florida

JOHN P. SARBANES, Maryland

CHRISTOPHER S. MURPHY, Connecticut

ZACHARY T. SPACE, Ohio

JERRY McNERNEY, California

BETTY SUTTON, Ohio

BRUCE L. BRALEY, Iowa

PETER WELCH, Vermont

JOE BARTON, Texas

Ranking Member

RALPH M. HALL, Texas

FRED UPTON, Michigan

CLIFF STEARNS, Florida

NATHAN DEAL, Georgia

ED WHITFIELD, Kentucky

JOHN SHIMKUS, Illinois

JOHN B. SHADEGG, Arizona

ROY BLUNT, Missouri

STEVE BUYER, Indiana

GEORGE RADANOVICH, California

JOSEPH R. PITTS, Pennsylvania

MARY BONO MACK, California

GREG WALDEN, Oregon

LEE TERRY, Nebraska

MIKE ROGERS, Michigan

SUE WILKINS MYRICK, North Carolina

JOHN SULLIVAN, Oklahoma

TIM MURPHY, Pennsylvania

MICHAEL C. BURGESS, Texas

MARSHA BLACKBURN, Tennessee

PHIL GINGREY, Georgia

STEVE SCALISE, Louisiana

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

BOBBY L. RUSH, Illinois
Chairman

JANICE D. SCHAKOWSKY, Illinois
Vice Chair

JOHN SARBANES, Maryland
BETTY SUTTON, Ohio
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BART STUPAK, Michigan
GENE GREEN, Texas
CHARLES A. GONZALEZ, Texas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
KATHY CASTOR, Florida
ZACHARY T. SPACE, Ohio
BRUCE L. BRALEY, Iowa
DIANA DeGETTE, Colorado
JOHN D. DINGELL, Michigan (ex officio)

CLIFF STEARNS, Florida
Ranking Member

RALPH M. HALL, Texas
ED WHITFIELD, Kentucky
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
MICHAEL C. BURGESS, Texas

CONTENTS

	Page
Hon. Bobby L. Rush, a Representative in Congress from the State of Illinois, opening statement	2
Hon. Ed Whitfield, a Representative in Congress from the Commonwealth of Kentucky, opening statement	3
Prepared statement	5
Hon. Lee Terry, a Representative in Congress from the State of Nebraska, opening statement	10
Hon. Betty Sutton, a Representative in Congress from the State of Ohio, prepared statement	11
Hon. Steve Scalise, a Representative in Congress from the State of Louisiana, opening statement	12
Hon. Henry A. Waxman, a Representative in Congress from the State of California, prepared statement	125
Hon. John D. Dingell, a Representative in Congress from the State of Michigan, prepared statement	130
Hon. Joe Barton, a Representative in Congress from the State of Texas, prepared statement	131
Hon. John Barrow, a Representative in Congress from the State of Georgia, prepared statement	135
Hon. Mary Bono Mack, a Representative in Congress from the State of California, prepared statement	136

WITNESSES

Daniel J. Weitzner, Associate Administrator for Policy, National Telecommunications and Information Administration, U.S. Department of Commerce	13
Prepared statement	16
Answers to submitted questions	138
David Vladeck, Director, Bureau of Consumer Protection, Federal Trade Commission	29
Prepared statement	31
Susan Grant, Director of Consumer Protection, Consumer Federation of America	62
Prepared statement	66
Answers to submitted questions	144
Joseph Pasqua, Vice President of Research, Symantec Corporation	72
Prepared statement	74
Joan Gillman, Executive Vice President and President, Media Sales, Time Warner Cable	85
Prepared statement	87
Eben Moglen, Legal Advisor, Diaspora, Professor of Law, Columbia University, Founding Director, Software Freedom Law Center	95
Prepared statement	97
Daniel Castro, Senior Analyst, Information Technology and Innovation Foundation	101
Prepared statement	103
Answers to submitted questions	149

DO-NOT-TRACK LEGISLATION: IS NOW THE RIGHT TIME?

THURSDAY, DECEMBER 2, 2010

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

The subcommittee met, pursuant to call, at 11:14 a.m., in Room 2123, Rayburn House Office Building, Hon. Bobby L. Rush [chairman of the subcommittee] presiding.

Present: Representatives Rush, Dingell, Schakowsky, Sutton, Green, Gonzalez, Barrow, Matsui, Space, Markey, Whitfield, Pitts, Bono Mack, Terry, Murphy, Gingrey, Latta, and Scalise.

Staff Present: Michelle Ash, Chief Counsel; Tim Robinson, Counsel; Felipe Mendoza, Counsel; Michael Ostheimer, Counsel; Will Wallace, Special Assistant; Brian McCullough, Minority Counsel; and Sam Costello, Minority Counsel.

Mr. RUSH. Good morning to all who are gathered here.

And we want to convene this hearing on the Subcommittee on Commerce, Trade, and Consumer Protection. So the hearing is now called to order. And we will begin with opening statements, with two announcements by the chair.

There are possibly five votes that are currently occurring on the floor. So, at this time, we will have the opening statements from the chair and from the ranking member. At the conclusion of those opening statements, we will recess and go vote, and we will reconvene probably close to around the noon hour. And then we will leave the—we will allow Members on both sides to continue their opening statements for a half an hour. So, upon reconvening, the Members will be given an additional half an hour for their opening statements.

And the purpose of that is to allow Members to deliver their opening statements, but also to do it within a certain specified time span so that we won't have stragglers coming in and keeping the opening statements—keeping this phase—prolonging this phase.

So that is how we will operate this morning.

Mr. BARROW. Mr. Chairman?

Mr. RUSH. Yes?

Mr. BARROW. Mr. Chairman, some of us have conflicting committee hours. Would this be an appropriate time to ask for unanimous consent that all Members of the committee might have 5 legislative days within which to submit a statement for the record?

Mr. RUSH. I would think so. If there is no objection?

Hearing no objection, so ordered.

Mr. BARROW. Thank you, Mr. Chairman.

OPENING STATEMENT OF HON. BOBBY L. RUSH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. RUSH. The chair recognizes himself for 5 minutes for the purpose of an opening statement.

Good morning. We are pleased to welcome into our midst today seven witnesses. They have graciously offered to share their views with this subcommittee about the feasibility of a legislative Do Not Track mechanism and how technological solutions to privacy perils and pitfalls could augment a comprehensive national privacy framework.

Through such a mechanism, consumers could advise would-be trackers unambiguously and persistently that they do not wish to be followed by digital snoopers and spies across Web sites and their various fixed and mobile computing devices.

More than 2 years ago, I heard testimony, as chairman of this very same subcommittee, from Ms. Lois Greisman, the FTC's associate director of Division of Marketing Practices. And Ms. Greisman spoke about the FTC's successes in routing out the excessive and abusive telemarketing acts and practices through the Do Not Call Registry.

From fiscal years 2003 through 2007, more than 145 million telephone numbers had been entered into the Do Not Call Registry. Over the same period, approximately \$80 million in fees have been collected from a base of over 18,000 unique entities who access from the registry.

As part of that opt-out and enforcement regime, the FTC stood prepared to initiate cases under its telecommunications sales rules to obtain temporary and permanent injunctions against violations, secure orders for more than half a million dollars in consumer restitution, and refer civil penalty action to the Department of Justice.

Almost a year before Associate Director Greisman's 2010 testimony and following 2 days of FTC town-hall meetings on online behavior tracking in the fall of 2007, the Consumer Federation of America and other privacy groups noted that self-regulatory initiatives devised by industry had, sadly, failed. One of those groups, the Consumer Federation of America, which happens to be represented today by Ms. Susan Grant, called upon the FTC way back then to implement a one-stop opt-out for online tracking, similar to the agency's successful Do Not Call Registry.

At the end of this second session of the 111th Congress, it would appear that we have come full circle with the FTC's endorsement of a Do Not Track mechanism that was released just yesterday as part of its preliminary staff report. The title of that draft report is "Protecting Consumer Privacy in an Era of Rapid Change."

Being the last hearing of this subcommittee that I will chair in this Congress, please allow me to reflect briefly on some of the major accomplishments and achievements of the CTCP Subcommittee over the 110th and 111th Congresses.

With the assistance of my able colleagues on both sides of the aisle, I have convened hearings, markups, and helped to guide, under the leadership of Chairman Waxman, to guide successfully

more than a dozen bills out of the full committee, including the Consumer Product Safety Improvement Act and the Wall Street Reform Act.

Our subcommittee was also very active in conducting oversight over the National Highway and Traffic Safety Administration in the wake of massive recalls of unsafe automobiles. We have also asked questions at hearings about the effects of the disastrous Macondo oil well spill on the gulf-area tourism and travel industry and the health effects of formaldehyde on persons in post-Katrina trailers.

I am especially and I am immensely proud of the collaboration that has existed between this subcommittee and the CTI, the Communications, Technology, and Internet Subcommittee, currently led by my friend, Chairman Boucher. In working closely with CTI to conduct oversight and to draft legislation, our two subcommittees held six joint hearings during the 111th Congress on a range of public safety and consumer protection topics, including texting while driving and online and offline privacy.

And I do believe that the record will show that this subcommittee was highly productive, very effective in accomplishing a lot, much, in a relatively short period of time.

With that said, I once again thank the witnesses for coming in this morning. I thank my colleagues on both sides of the aisle who are members of this subcommittee. And I yield back the balance of my time.

And I recognize now the ranking member of the subcommittee, Mr. Whitfield, for 5 minutes for the purpose of an opening statement.

OPENING STATEMENT OF HON. ED WHITFIELD, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF KENTUCKY

Mr. WHITFIELD. Thank you, Chairman Rush.

And we appreciate your holding this hearing today on the Do Not Track concept. I say that because I don't think we really have any legislation, but it is an idea. And we all recognize that consumer protection for the Internet is an important issue and one that I am glad this subcommittee continues to address.

I believe that all of us understand that the Do Not Call Registry, which was developed over many years of legislation and dialogue, has been very successful because it does provide a mechanism for consumers to stop unsolicited cold calls from telemarketers.

However, I am concerned with taking a similar model and applying it to the Internet by establishing a Do Not Track system simply because we are not really comparing apples to apples.

First, I am not sure the technology is in place to establish such a mechanism. It is my understanding that there are several competing technologies out there on how exactly to create a Do Not Track list. And so the question would be, is the government really the best entity to make that decision?

I also think we need to ask what will happen to advertisement-supported Internet content if a Do Not Track system is implemented. In order for Internet content to remain largely free to con-

sumers, it is supported by advertising. Would an advertising model be sustainable in the absence of marketers' ability to track?

In addition, I assume most consumers would rather see advertisements they are interested in rather than completely irrelevant advertising. So if a Do Not Track system was implemented, would consumers receive less-relevant ads?

While I agree that it is important for consumers to have an understanding of what information is being collected and how it is used, we need to seriously discuss the Do Not Track model to evaluate whether it accomplishes the appropriate objectives.

Some have expressed concern that a one-size-fits-all Do Not Track model could impact consumers' choices by preventing their access to the benefits of online advertising. Now, personally, I believe a better approach may be to empower consumers to have better control over their online experience. For example, why not have disclosures which let consumers know what type of information is being collected and how it is being used or allow consumers to tailor their online browsing experience so that they may promptly have the benefits of information specific to their interests?

Lastly, I think we should be mindful about the economic impact this proposal could have, particularly since we are in the middle of the holiday gift-giving season and we understand that more shoppers are buying their holiday gifts online each year—a benefit to many consumers and businesses that never would have reached each other before the Internet became mainstream. We need to be mindful not to enact legislation that would hurt a recovering economy. To that end, I am curious to find out if there have been any economic-impact studies or reports to see how implementing a Do Not Track system would impact our economy.

Once again, I appreciate Chairman Rush's interest in the issue, his strong dedication to online privacy. And I look forward to the testimony of our witnesses today.

And one other comment that I might make on an unrelated matter. I know that Chairman Genachowski and the FCC are looking at issuing some new Net neutrality rules. As we know, there have been some court decisions on that issue. And I hope that the FCC does not move in that direction right now, and give us an opportunity to further explore that issue here in the Congress.

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

[The prepared statement of Mr. Whitfield follows:]

Remarks of the Honorable Ed Whitfield

Ranking Member, Subcommittee on Commerce, Trade, and Consumer Protection

Hearing on “Do Not Track Legislation: Is Now the Right Time?”

December 2, 2010

Thank you Chairman Rush.

- I support consumer protection for the Internet, including data security protections
 - I supported the Do Not Call Act and the Do Not Call Improvement Act
 - I support greater privacy controls and protections for consumers
- Americans overwhelmingly supported the Do Not Call legislation because they were tired of having to answer unsolicited, cold calls from various marketers – particularly when they interrupted dinner.
- Telemarketers used personally identifiable information – name, phone number, address, and other publicly available information – to identify to whom they would make those unsolicited calls.

- Similarly, targeted advertising uses individual information about consumers, gleaned from their internet browsing behavior, to deliver relevant advertising.
 - Unlike telemarketers, however, online advertisers do not interrupt consumers' web activity – or their dinner.
 - Several witnesses will testify that the problems that lead us to the Do-Not-Call legislation are simply not the same as the issues around advertising in the online world. And as a result, the Do-Not-Call solution will not easily translate into a “Do Not Track” list. I am very interested to learn why and what the ramifications would be.
 - In the event these stakeholders are correct and a Do Not Track registry is not feasible, I think it would be helpful to our discussion today to try to identify exactly the harm or action we seek to prevent or address with a Do Not Track registry.
- I am not sure any of us fully understand what information is being collected and by whom when we see an online advertisement.
- That we don't know the who or the what in targeted advertising is a legitimate concern.

- If in order for internet content to remain free to consumers it must be supported by advertising, I assume most consumers would rather see advertisements they are interested in rather than completely irrelevant advertising. But the mechanism for determining what is relevant to any individual consumer is the question at hand.
 - When data used to target advertisements is not personally identifiable, most consumers probably wouldn't mind.
 - But when data used to serve ads goes beyond anonymity or inferred characteristics about a person based on aggregated data into the active targeting of ads based on known individual behavior or known individual identity, I think consumers may have a much different reaction.
 - One company promotes its services in the following manner:
 - “But why try to infer interests when (Company X) knows a consumer's interests? How people spend their hard-earned money is the most powerful and accurate indicator of their interests. Now your ads can be served to a precise audience based on the products they've purchased - online and offline. This is the next evolution of online ad targeting...”

- This is the type of profiling that raises serious concerns for many consumers.
- Many industry stakeholders recognize these concerns and have developed their own initiative to give consumers an “opt-out” from advertising networks’ behavioral advertisements. This is a good step but it leaves open the question whether advertisers will begin to migrate to the ad networks that do not participate in the IAB program.
- After all, this approach is only as good as the number of stakeholders who participate and the number of consumers who are made aware of and avail themselves of this option.
- All of that being said, I’d like to say that the timing of this hearing is what concerns me most.
 - These are legitimate issues. However, more shoppers buy their holiday gifts online every year -- a boon to many consumers and businesses that never would have reached each other before the Internet became main stream.
 - As many retailers enter the busiest shopping season of the year – the season that usually determines whether they will make a profit - consumers might misunderstand the issue we are discussing today.

- When Congress calls a hearing and media reports on the issue as if it is a new issue, consumers take notice. Our economy is still very fragile and I do not want to scare Americans into withdrawing from the Internet if there is not a legitimate threat. Are we sending a message at the onset of Christmas shopping season that there is a serious threat to consumers' personal information?
- The hearing is focused on the idea of Do Not Track, not "Do Not Shop/Buy", and I hope that our oversight into this matter does not translate into an immediate deterring of consumer purchases.
- Once again, I appreciate the Chairman's interest in the issue and I look forward to the testimony and yield back.

Mr. RUSH. I think we have 5 minutes remaining—2 minutes? Two minutes, OK.

Well, the subcommittee now stands in recess until the conclusion of this series of five votes on the floor.

[Recess.]

Mr. SPACE [presiding]. The hearing will come to order.

And we were in the middle of opening statements when we were called for a vote. And I believe the gentleman from Nebraska, Mr. Terry is next.

OPENING STATEMENT OF HON. LEE TERRY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEBRASKA

Mr. TERRY. Thank you, Mr. Space.

The issue that we are here on, targeting and creating this “do not target” list or whatever it will be called is—I think it is worthy of discussion and looking into. Of course, it is going to be an issue of how we define it and how we really help consumers here.

I was one of the eight, I think, classified the “Do Not Call Eight.” There were eight of us that voted against the Do Not Call list. And there are ways of helping consumers and not helping consumers, and we want to make sure we do it the right way.

I am actually more frustrated with the FCC than either two of you sitting here today, and the actions taken by the FCC chairman to usurp congressional power and authority in a new proposed order of regulating the Internet. Certainly, doing that on the eve of a new Congress is a message to us that they want to ram it down the public’s throats before an opportunity comes for a different majority in the House of Representatives. But the issue is very bipartisan against the FCC’s power grab.

Now, the order has been circulated amongst the Members. We don’t get to see it in Congress yet. This committee, Energy and Commerce, Telecom Subcommittee, partially this subcommittee, have authority, jurisdiction. We are cut out of the deal. AT&T has ostensibly agreed to something under duress, is my personal opinion. It was, “Either you agree to this, or we are really going to come after you.”

And I think those type of tactics of the public not knowing, that order of how to regulate the Internet, doing it under duress, making parties agree to things under threat of, “Well, it will be worse for you if you don’t,” those are the type of tactics that the public rejected on November 2nd. And so I would call on the FCC to stand down, don’t go forward with the proposed order on regulating the Internet.

I yield back.

Mr. SPACE. Thank you, Mr. Terry.

The gentlewoman from Ohio, Ms. Sutton.

Ms. SUTTON. Thank you, Mr. Chairman. I will just submit my opening statement for the record so we can move along to the testimony. Thank you.

[The prepared statement of Ms. Sutton follows:]

**Opening Statement of Congresswoman Betty Sutton
CTCP Hearing on “Do Not Track Legislation: Is Now the Right Time?”
December 2, 2010**

Thank you Chairman Rush for holding today’s hearing on “Do Not Track Legislation: Is Now the Right Time?”

This Committee has held several hearings exploring a wide range of privacy issues. What we have learned has been very eye-opening. These hearings have raised legitimate concerns about consumer privacy; about the collection and use of consumer data.

Many Americans are unaware of how much data about them is being collected, let alone how it is being used or shared. Details of their lives are being collected, analyzed, packaged and sold. This is tantamount to rifling through one’s trash or going through someone’s mail.

Information is being collected through non-transparent and complex methods. And, these methods are ever-changing making it increasingly more difficult for consumers to avoid having their online activities monitored.

Consumers deserve and expect better. We must do more to safeguard consumer privacy and ensure that there are appropriate mechanisms to protect consumers from unknown and unwanted tracking.

I look forward to hearing from today’s witnesses on the concept of developing a simple, one-stop, opt-out for online tracking.

Mr. RUSH. Thank you, Ms. Sutton.
The congressman from Louisiana, Mr. Scalise.

OPENING STATEMENT OF HON. STEVE SCALISE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF LOUISIANA

Mr. SCALISE. Thank you, Mr. Chairman.

We have learned at previous hearings that Web tracking can provide valuable information to businesses and marketers, thus enabling them to provide targeted online advertisements. And these benefits are not just limited to businesses. Consumers can enjoy a personalized Web experience and receive ads tailored to their interests without having to search or sit through a sales pitch.

And just as important, tracking and behavioral advertisements benefit the Internet itself, because it helps underwrite the cost of these sites that so many consumers enjoy and with many of these services that are provided for free.

But we also recognize the growing concern over the information that is collected on consumers, many of whom may not even know that their online activity is being tracked, and the potential for that personal information to be compromised or used illegally.

That is why we must proceed prudently and find the appropriate balance between protecting consumers and promoting a dynamic Internet environment that continues to produce the innovations and advancements that we have all come to enjoy.

Our first step should not be finding ways the government can regulate the issue. We do not need more government directives on the Internet. A surefire way to stifle innovation would be to pass more government regulations that restrict innovation in this dynamic industry without a proper approach. Constructive roles for government to play would include encouraging public-private partnerships, promoting best practices, and encouraging investment, innovation, and competition.

But I believe we must first look to self-regulation and what steps the industry will take and has already taken to protect consumers. Today we can see examples of self-regulation, including the development of built-in opt-out mechanisms on Internet browsers.

We must also further examine the concept of Do Not Track. The idea itself leads to questions that must be answered as we move forward. Will a Do Not Track mechanism adequately protect consumers in light of developing technologies? Will it be consistent across different industries and technologies? And will it restrict the exchange and use of consumer data in ways that deter innovation and growth?

As I have stated at previous hearings, the technology in the Internet industries are among the most advanced and competitive in our country, and they are also among the most beneficial, both for consumers and our economy. And they have achieved this status by advancing and growing on their own, with little interference from the Federal Government. And some would say that is one of the reasons that they have been so successful in innovating.

We must continue to allow these industries to develop and innovate, and I believe we can do this in a way that strengthens consumer privacy. Protecting consumers and protecting the Internet

economy are not mutually exclusive goals. We must ensure that government intervention does not stifle innovation.

And, finally, I will chime in and concur in what my colleague from Nebraska said. I strongly oppose the effort by the FCC to regulate the Internet through Net neutrality and especially in some dark-of-night attempt that didn't go through the proper scrutiny that it deserves.

Thank you, and I yield back.

Mr. RUSH. Thank you, Mr. Scalise.

And seeing no other Members present, at this point I would like to introduce and thank our witnesses for appearing before the committee today.

We have with us today Mr. Daniel Weitzner, associate administrator for policy at the National Telecommunications and Information Administration and U.S. Department of Commerce; also Mr. David Vladeck, director of the Bureau of Consumer Protection with the FTC.

Welcome, gentlemen. It is the practice of the subcommittee to swear in witnesses, so I would ask that you stand and raise your right hand.

[Witnesses sworn.]

Mr. SPACE. Please let the record reflect that the witnesses have answered in the affirmative.

And, with that, I would introduce again Mr. Weitzner for his 5-minute opening statement.

TESTIMONY OF DANIEL J. WEITZNER, ASSOCIATE ADMINISTRATOR FOR POLICY, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE; DAVID VLADECK, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

TESTIMONY OF DANIEL J. WEITZNER

Mr. WEITZNER. Thank you, Congressman Space and Ranking Member Whitfield and members of the subcommittee. I thank you for the opportunity to testify on behalf of the United States Department of Commerce and the National Telecommunications and Information Administration. NTIA appreciates your leadership on commercial privacy policy and thanks you for the opportunity to engage on the question of how best to protect consumer privacy in the rapidly evolving Internet age.

And I am especially pleased to be here with my colleague, David Vladeck. And I hope you will allow me to congratulate the FTC on the important privacy report that they released yesterday. Their expert insight on privacy matters will certainly inform the administration's thinking on the issue going forward. I know it is a lot of work to get those out, so thank you.

I would like to highlight three points from my written remarks, if I could: first, the Commerce Department's approach to privacy as part of our overall efforts to develop innovation-sustaining Internet policy principles; second, the urgency for the United States to reassert global leadership on privacy policy; and, third, our view of how to approach the goals behind the Do Not Track concepts.

We are all well-aware of the transformations enabled by the Internet. Politics, education, scientific research, health care, and even romance have all moved online. These powerful, exciting, and innovative developments also feed a growing concern among citizens about how their data is being stored, monitored, and analyzed.

This is the policy challenge that confronts us. To harness the full potential of the digital age, we need to establish ground rules that promote innovative uses of information while building a well-founded sense of trust that consumers' legitimate expectations of privacy will be respected.

Earlier this year, in order to develop a broad policy framework that promotes innovation in the Internet environment, Commerce Secretary Gary Locke established the Department's Internet Policy Task Force. The task force, which draws from a number of bureaus in the Commerce Department, including my own, NIST, the Patent and Trademark Office, the International Trade Administration, and others, is developing policy recommendations in a range of areas, including protecting privacy, assuring cybersecurity, establishing balanced copyright protection models, and preserving the global free flow of information.

Consumer privacy is our first order of business. After consulting with a wide variety of consumer and commercial stakeholders, we have heard the unmistakable message that it is time to shore up privacy protection in the United States and abroad. So what needs to be done to enhance privacy protection while encouraging ongoing innovation?

First, we need to affirm a privacy baseline regarding the handling of consumer information. This baseline should be built on a full set of fair information practice principles. To paraphrase a comment we received in our notice of inquiry, baseline FIPS are something that consumers want, companies need, and the economy will appreciate.

Second, we realize that the government is not going to have all the answers. With or without legislation, the centerpiece of Internet privacy protection will have to be an increased sense of urgency and incentives for the development of voluntary but enforceable codes of conduct. These are what Chairman Rush's bill calls "choice programs and safe harbors." This approach recognizes that technologists and entrepreneurs, privacy and consumer advocates, business and the government have to work together to develop best practices for managing commercial data.

Best practices or a code of conduct are an indispensable mechanism by which all companies must adopt a strategy for implementing fair information practices. In order to be sure that these codes of conduct reflect the perspective of all stakeholders, all the stakeholders must be involved in the development of these codes.

The alternative, however, is to wait for lengthy and conceivably contentious agency rule-making procedures. This will neither serve consumers, who need protection in today's new services, nor businesses, which need flexibility in the application of privacy rules. The FTC, through after-the-fact enforcement, would provide critical legal assurance to consumers that the companies are actually adhering to the commitments that they make.

Finally, I want to say that there is an urgent need to renew our commitment to leadership in the global privacy policy debate. All around the world, including in the European Union, policymakers are rethinking their privacy frameworks. As leaders in the global Internet economy, it is incumbent on the United States to develop an online privacy framework that enhances trust and encourages innovation. Congressional leadership, continued FTC enforcement efforts, and administration engagement will all be important to show the world that the U.S. has a strong privacy framework and that we are committed to strengthening it further.

Turning to the question of Do Not Track, allow me to start from first principles. We believe that individual choice and control over the flow of information has always been the foundation of Internet policy. To the extent that tools provide effective protection for individual choices, government properly avoids regulations that would otherwise restrict the free flow of information.

There has been continued innovation in these tools available to users over time, but we believe that we need to see more rapid action by businesses in providing users with easy-to-understand ability to control how their personal information is used.

I just want to say in closing to all the members of the committee that I think that we have seen, across the history of Internet policymaking, strong bipartisan commitment to helping the Internet to develop, to keeping it open, and to protecting people's basic rights. We saw this with Section 230 of the Communications Decency Act that is a foundation of our Internet policy framework. We saw it with the notice and take-down provisions in the Digital Millennium Copyright Act, and even in institutions such as the Congressional Internet Caucus. They have all benefitted from leadership of support of Democratic and Republican Members of Congress alike.

Like these other issues, safeguarding consumer privacy, we hope, will remain a bipartisan priority. And we look forward to this committee's continued leadership in the next Congress.

Thanks very much.

[The prepared statement of Mr. Weitzner follows:]

Testimony of Daniel J. Weitzner

Associate Administrator for Policy Analysis and Development
National Telecommunications and Information Administration
United States Department of Commerce

Before the
Subcommittee on Commerce, Trade and Consumer Protection
Committee on Energy and Commerce
United States House of Representatives

“Do-Not-Track” Legislation: Is Now the Right Time?

December 2, 2010

I. Introduction.

Chairman Rush, Ranking Member Whitfield, and Members of the Subcommittee, thank you for your invitation to testify on behalf of the U.S. Department of Commerce. As the Associate Administrator for the Office of Policy Analysis and Development at the National Telecommunications and Information Administration (NTIA), I welcome the opportunity to testify before you to discuss how best to protect consumer privacy in the rapidly evolving Internet Age.

Establishing a strong U.S. framework for commercial data privacy is important to ensuring continued consumer trust and innovation in the Internet environment. The Commerce Department's Internet Policy Task Force has been hard at work over the last year to develop a framework for an updated approach to online privacy that will strengthen consumer protection in a manner that encourages continued innovation in the Internet marketplace. My testimony today will first focus on the overarching principles guiding the Commerce Department's review of Internet policy. I will then highlight general ideas for reform which will be discussed in more detail in a forthcoming report. I will elaborate on how we intend for our report to feed into the work of the recently-formed White House task force on "Privacy and Internet Policy." Finally, I will conclude with a discussion of "do-not-track" proposals.

I am especially pleased to be here today with my colleague David Vladeck, the Director of Consumer Protection at the Federal Trade Commission (FTC). Under the leadership of Chairman Leibowitz, the FTC has strengthened its vital role as the leading consumer data protection agency in the United States and continues to conduct itself as a consumer protection and privacy enforcement agency that is the envy of the world. Effective enforcement and leadership by the FTC needs to remain a pillar of U.S. commercial data privacy protection.

During the past fifteen years, networked information technologies – personal computers, mobile phones, and other devices – have been transforming the nation's – indeed, the world's – social, political and economic landscape. The Internet has grown into an essential platform not only for trade, but also for democracy and free speech that is celebrated in America and around the world and a vital engine of the global economy. Almost any transaction you can think of is being done online – from consumers paying their utility bills and

people buying books, movies and clothes, to major corporations paying their vendors and selling to their customers. According to the U.S. Census, domestic online transactions are currently estimated to total \$3.7 trillion annually.¹ Digital 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.

E-commerce statistics capture only one portion of the economic, social, and political change brought on by the Internet. We are experiencing not only an economic transformation, but also tremendous innovation. For example:

- A decade ago, going online meant accessing the Internet on a computer in your home. Today, it also includes iPhones, portable games, and interactive TVs.
- Numerous companies are creating “cloud computing” platforms, which offer on-demand, super-computing capacity.
- Single purpose “smart applications” – like smart air conditioners – will connect to the smart grid, enabling greater energy efficiency and conservation.

As powerful, exciting, and innovative as these developments are, they also bring with them new privacy concerns. Increased collection, analysis, and storage of personal information by private entities is becoming central to the Internet economy, making the online economy more efficient and companies more responsive to their customer needs. Yet these same practices also feed into a growing concern among consumers about how their data and transactions are being monitored and preserved.³ This is the policy challenge that confronts us today. It is one that must be approached both deliberately and with care. In a word: to harness the full power of the digital age, we need to establish ground rules that promote innovative uses of information while still respecting consumers’ legitimate privacy interests. At the same

¹ U.S. Census Bureau, “E-Stats,” 27 May 2010, <http://www.census.gov/econ/estats/2008/2008reportfinal.pdf>.

² Secretary Gary Locke, *Remarks on Cybersecurity and Innovation*, Georgetown University, Washington, DC (September 23, 2010); see also US Ambassador to the OECD Karen Kornbluh, *Remarks on Internet Intermediaries*, OECD Workshop, Paris, France (June 16, 2010).

³ According to a recent survey, 85% of adults say they are “more concerned about online privacy than they were five years ago.” Common Sense Media, *Online Privacy: What Does It Mean to Parents and Kids* (2010), <http://www.common Sense Media.org/sites/default/files/privacypoll.pdf> (last visited Nov. 26, 2010).

time, as we go about creating these privacy guidelines, we also need to be careful to avoid creating an overly complicated regulatory environment.

II. Overarching Principles Guiding the Internet Policy Task Force's Review of Commercial Data Privacy.

Over the past year, the Department of Commerce and NTIA have been focused on developing and sharing policy ideas to ensure that we continue to have an Internet environment that encourages innovation and creativity and that fosters trust with users. This effort is guided by two overarching principles:

First, preserving consumer trust is essential to the sustainability and continued growth of the digital economy. If users do not trust that their personal information is safe from misuse, they will worry about using new Internet-based services, thus threatening economic growth.

Second, commercial data privacy implicates a broad array of interests—industry, consumer, civil society, academic, and governmental—and we need a policy development process that includes input from all of these stakeholders. We can learn from the unique multi-stakeholder processes that have helped build and operate the Internet in order to arrive at best practices that can protect user privacy according to an appropriate, enforceable set of rules.

There is little question that multi-stakeholder organizations have played a major role in the design and operation of the technical aspects of the Internet and are directly responsible for its success. Indeed, many point to one specific multi-stakeholder institution known as the Internet Corporation for Assigned Names and Numbers (ICANN) as strengthening the Internet's infrastructure and thus ensuring that the Internet continues to be a significant medium for conducting research, communicating with others, and conducting business. As many of you know, ICANN was created out of an effort to bring more coordination and sustainability to the management of the Internet domain name system (DNS), as the Internet grew into a large-scale global network. Government has played a role in creating and sustaining ICANN as a multi-stakeholder model. The key role for the Commerce Department and NTIA was to convene private sector and other Internet stakeholders to discuss important DNS-related issues, bring these matters to the public's attention, and work together with interested parties to tackle

challenging problems. This multi-stakeholder process provides foundational stability and predictability, on the one hand, and agility to keep up with the Internet's dynamism, on the other.

Commercial data privacy similarly must respond to changes in networked technologies and their uses. In the years following the commercialization of the Internet in the early to mid 1990s, the government imperative was to seek unrestrained growth of the Internet as a medium. During this first phase of Internet policymaking, early online privacy engagements between the Commerce Department, the FTC, and commercial and non-commercial private sector stakeholders set out a model for addressing emerging privacy challenges such as those posed by the new and rapidly growing online advertising industry. These efforts led to progress toward voluntary, enforceable privacy disclosures, whose premise was that industry commitments would develop faster and provide more flexibility than legislation or regulation.

The Internet grew rapidly through the 2000s and supported tremendous economic growth and social innovation. Personal data available on the Internet also grew rapidly in volume and granularity, which in turn expanded the market for personal information. Congress acts on discrete challenges, such as combating spam and protecting children's personal information. Meanwhile, the over-arching "notice-and-choice" model of privacy policy – posting privacy policies on websites to inform consumers' choices about whether to use the site – remained basically unchanged. The FTC, of course, continued to enforce companies' obligations under this framework, but the previous Administration pulled back from earlier efforts to promote industry codes that addressed new privacy challenges.

Today, we are in the third decade of Internet policy-making. Government must continue to convene stakeholders to discuss critical technology issues, bring these issues to the public's attention, and work together with all interested parties to solve challenging problems. This convener role is an important way to provide leadership on these issues, while preserving the benefits of a multi-stakeholder approach. These principles have been practiced at the Commerce Department. In April of this year, Commerce Secretary Gary Locke formally announced the creation of the Department's Internet Policy Task Force. As the President's principal advisor on telecommunications and information policy, NTIA was asked to play a

leading role in the Task Force. Through its Task Force, the Department is conducting a broad review of the four key public policy and operational challenges facing the Internet: (1) enhancing commercial data privacy; (2) ensuring cybersecurity in the commercial context; (3) protecting copyrights; and (4) ensuring the global free flow of information. On the issue of protecting copyrights, we are working closely with the U.S. Intellectual Property Enforcement Coordinator and the interagency enforcement committee she chairs that Congress created to coordinate Federal efforts to combat unlawful uses of intellectual property.

Commercial data privacy has been the Internet Policy Task Force's first order of business. Our effort began by listening to everyone who was willing to talk to us: consumer groups, companies, trade associations, civil society, and academics. This past spring, these conversations helped NTIA to shape a Notice of Inquiry, which posed a number of questions about the connections between privacy, policy, and innovation in the Internet economy. NTIA held a public symposium in Washington, where experts from all sectors shared their views on topics ranging from international frameworks to specific voluntary codes of conduct. And NTIA has been working informally, but closely, with our colleagues at the FTC, which is the U.S. federal government's main commercial data privacy enforcement agency.

We have learned a great deal from this early effort. It is clear that we need to strengthen our framework. The current U.S. commercial data privacy framework is the product of diverse political and cultural forces, as well as decades of exchange with foreign and international systems. The U.S. framework has also had international influence since 1970, when Fair Information Privacy Practices -- first promulgated by the Department of Health, Education & Welfare as a response to mainframe computing -- were adopted and expanded by international bodies, such as the Organization for Economic Cooperation and Development (OECD). The U.S. framework remains robust: our privacy protections stem from common law, state law, and specific federal protections, and are bolstered by FTC enforcement and self-regulatory mechanisms. But the U.S. framework leaves some areas out and does not provide consumers, businesses, or our international partners with a clear set of rules for the handling of commercial data.

Now, it is time to shore up commercial data privacy protection in the U.S. and abroad, and to preserve the unique online environment that has allowed sustained commercial growth on a domestic and global scale.

Like so many Internet and telecommunications issues, safeguarding consumer privacy should remain a bipartisan concern. This has been the case from the very beginning of Internet policy making. Section 230 of the Communications Decency Act, and the notice-and-takedown provisions of the Digital Millennium Copyright Act (DMCA), benefitted from the leadership and support of Republican and Democratic Members of Congress. Similarly, I have been heartened to hear recent comments from both this Subcommittee's Chairman and Ranking Member that online privacy will continue to remain a priority in the next Congress. Working together, I am confident that we can achieve meaningful reform.

III. Commerce Department's Forthcoming Report on Commercial Data Privacy.

The Commerce Department will soon publish a series of policy ideas and questions through a Department of Commerce "green paper," which are intended to play a key role in our effort to close gaps in consumer protection, strengthen online trust, and bolster the Internet economy. The paper will contain both proposed recommendations for discussion and a further set of questions on topics about which we seek further input.

So what have Internet stakeholders expressed to us about what specifically needs to be done to strike a better balance between privacy and innovation? First, they feel that it is time that consumers be provided, essentially, a privacy baseline regarding the handling of their consumer information. This baseline would be based on a full set of fair information practice principles (FIPPs) – guidelines that represent widely-accepted concepts concerning how online entities collect and use personal information – and would provide transparent disclosure to consumers, businesses, and Internet stakeholders across the various commercial contexts in which recorded data is being used. To borrow from one of the responses we received to our Notice of Inquiry, baseline FIPPs are something that consumers want, companies need, and the economy will appreciate. If desired, industry, consumer groups, civil society, and the U.S. Government all have important roles to play in helping this framework take hold. We take note of the fact that many commenters in our Notice of Inquiry, including leading Internet

companies and many civil society groups, support a legislated set of privacy baselines. In assessing a range of tools to support dynamic, baseline privacy protection, our report will address the role that properly tailored legislation could play in this framework.

Second, consistent with our multi-stakeholder model, we agree with Internet stakeholders that government is not going to have all the answers. Along with government, there are vital roles for industry, consumer groups, and civil society to play in putting FIPPs into practice in the United States. A multi-stakeholder strategy for implementation will be critical to ensure that we end up with a framework that is rational, that provides businesses with clear markers about how to meet their obligations, but that is also dynamic, to keep information practices in line with consumer expectations as technologies and markets evolve.

With or without legislation, Internet stakeholders suggested that the centerpiece of Internet privacy protection may be upgrading the role of voluntary but *enforceable* codes of conduct, developed through open, inclusive processes. This approach recognizes that technologists and entrepreneurs, privacy and consumer advocates, businesses, and the government have to work together to develop best practices for managing commercial data in particular circumstances. Launching such multi-stakeholder processes is, indeed, challenging. But, given the success of using this model in other Internet contexts, such as development of standards and protocols, we are confident that it will be successful.

Voluntary but enforceable codes of conduct are an important mechanism by which all companies would adopt some strategy for implementing FIPPs. The specific means of doing so would be flexible and able to adapt to changing business models as they are introduced, as opposed to having to wait for lengthy and contentious agency rulemaking procedures. After-the-fact oversight by the FTC is an essential to provide consumers the assurance that companies adhere to the commitments made in the codes of conduct.

The Commerce Department's Internet Policy Task Force will continue to make commercial data privacy reform a top priority. Our future efforts on privacy reform have been motivated by listening to everyone willing to talk to us: companies, consumer groups, civil society, state regulators, and academics. We began our conversation with these stakeholders this past spring and we will continue to engage experts from all sectors on topics ranging from

international frameworks to voluntary codes of conduct. Our work will also complement, not supplant, the FTC, which fully maintains its independent enforcement and policy making roles as the main privacy enforcement agency. Nor would the Commerce Department change how the federal government goes about managing its own information practices through the Office of Management and Budget and individual agency Chief Privacy Officers. Instead, the key role for our new Task Force would be to bring together the many different parties that are necessary to help develop commercial data privacy practices for new circumstances.

As new online business models emerge, the Commerce Department and NTIA can help convene stakeholders to develop best practices by providing more cohesive Executive Branch leadership on commercial data privacy issues. These best practices can be developed faster than any regulatory proceeding would allow, while providing greater certainty for businesses and necessary protections for consumers. An institutional commitment to engage on information privacy issues in a dynamic, multi-stakeholder manner over the long term would do more than just help voluntary industry codes to develop; it would also be a better vehicle for us to better engage with Congress in addressing the commercial data privacy issues we are all confronting.

On the overall architecture for privacy reform there are three basic tools of government – prescriptive, before-the fact regulation; after-the-fact enforcement; and government-as-convenor, which enables cooperation and better convergence on best practices. Our overall efforts on commercial data privacy can be explained by an effort to develop an architecture that puts each of these in its proper place. As a convener, the Commerce Department’s role is much different than a regulator conducting after the fact enforcement. Rather, our role is to encourage standard setting, effective cooperation, and sharing of best practices – as well as challenging firms to attend to privacy issues.

And finally, stakeholders have requested that the Obama Administration help renew our commitment to global interoperability by redoubling our collaboration with multilateral organizations engaged in developing with global privacy standards and principles. The legal and policy framework surrounding the Internet, especially privacy, is complicated both domestically and internationally. While they understand that governments must act to protect their citizens,

they also wish to avoid fragmented sets of inconsistent and unpredictable rules that frustrate innovation and create needless barriers to the free flow of information, goods, and services on the global Internet.

In furtherance of this agenda, on October 24th, the White House announced the formation of a Privacy and Internet Policy Subcommittee to further advise the Obama Administration on commercial data privacy policy. This Subcommittee – which Commerce Department General Counsel Cameron Kerry co-chairs with Assistant Attorney General Christopher Schroeder – is working to coordinate federal agencies, while engaging public stakeholders, in an effort to promote a broad, visible, forward-looking commitment to a consistent set of Internet policy principles. These core principles include facilitating transparency, promoting cooperation, strengthening multi-stakeholder governance models, and building trust in online environments.

The idea of the Subcommittee is to consult with stakeholders to address the direction of U.S. laws and regulations on Internet privacy, with a focus on commercial data privacy. The Subcommittee will work closely with private companies and consumer groups in endeavoring to strike the appropriate balance between the privacy expectations of consumers and the needs of industry, law enforcement, and other Internet stakeholders. The Subcommittee will begin its review of Internet commercial data privacy policy with the Commerce Department's green paper and stakeholder comments responding to the recommendations and questions set forth in the green paper. We have always viewed the Commerce Department's green paper as one step in an ongoing conversation, rather than a final statement of policy views, and we are working with the Subcommittee as it begins its inter-agency consideration of this critical Internet policy issue. 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 commercial data privacy policy, regulation, and legislation.

IV. Do-Not-Track.

Turning to the question of do-not-track proposals, let me start by saying that individual choice and individual control over the flow of information to and from the user has been a foundation of Internet policy from its inception. For example, user empowerment technology

(including filtering, blocking, and monitoring tools) has provided families with the means to protect their children from viewing inappropriate material online. There have been some similar developments in the area that the “do-not-track” concept is intended to address—online behavioral advertising. As Web users became aware that cookies could be used to track their activities on a single Web site as well as across multiple sites, browser developers provided their users with the means to block and manage cookies in a variety of ways. More recently, members of the online advertising industry developed common principles about the collection and use of tracking information, and the industry is rolling out a system to help consumers manage their tracking preferences online. To the extent that these tools provide effective protection for individual choices, government properly avoids regulations that would otherwise restrict the flow of information.⁴

I am pleased that discussions of any “do-not-track” requirement similarly focus on how to maximize individual choice and individual control of access to information. The Commerce Department generally supports these types of consumer empowerment. Significant challenges face the online industry, consumer advocates, regulators and policy makers, regardless of whether Do-Not-Track features are enacted pursuant to legislation or developed through voluntary agreement. Any Do-Not-Track system would necessarily have two components: first, a technical mechanism (such as one built into Web browsers) that provides the user a way to signal his or her intent not to be tracked or profiled depending on the context; and second, an understanding between individual web users and all of the various commercial (and non-commercial) services on the Web that engage in tracking as to exactly what sort of behavior those services would avoid. The technical mechanism may take some work to implement, but is presumably manageable. The second, agreement on what is meant by the “do-not-track” sign on, say, the user’s browser, is a more complex task, requiring agreement on policy and best practices among a number of players including users, advertisers, marketers, technology companies, and other intermediaries.

Some users want to avoid tracking altogether. That is, they want to be sure that no Web site or third party service collects or stores any data about their Web browsing behavior.

⁴ See *Reno v. ACLU*, 521 U.S. 844 (1997).

That goal can largely be accomplished with existing browser settings (to block any cookies) and additional tools that enable the user to unilaterally block other Web tracking features. For these users, greater consumer education about tools already available might be all that is needed. But many users want more nuanced choices. That is, users might be happy to have certain Web sites collect and store some information about browsing habits when it serves the users' interests, but they might want to avoid other tracking or profiling that they consider intrusive or simply of no benefit to them. In the first instance, a user may want sites to remember his or her preferences, account information, or even to provide certain types of customization. However, that same user might also want to prevent the creation and use of profiles that allow marketers or advertisers to learn details about his or her buying habits. Reaching agreement on these more complex set of choices, beyond just the technology, will require careful work. So, the best approach to achieving the important goals motivating the Do-Not-Track concept is through a voluntary, multi-stakeholder process, backed up, in the end, by FTC enforcement of the privacy commitments made to consumers through such a system.

Thus, today's debate over the feasibility of "do-not-track" may actually be an illustration of a larger problem: the overarching need for a more dynamic commercial data privacy framework that can incentivize the creation of industry codes of conduct, while also being flexible enough to keep pace with innovation. The robust, dynamic commercial data privacy framework to be discussed in the Commerce Department's green paper will help us explore ways to address new applications and technologies like do-not-track. Specifically, the Commerce Department's Internet Policy Task Force will start to convene industry and consumer groups to discuss the next steps toward achieving voluntary agreements on implementation methods for a do-not-track requirement. Our Department's Task Force is also well situated to work collaboratively with the FTC and other government agencies to encourage industry to create a workable model. Once crafted and adopted by stakeholders, the FTC's enhanced enforcement authority can ensure compliance with these voluntary agreements, as appropriate.

V. Conclusion.

As we embark on these active discussions of how to enhance our commercial data privacy framework, we should keep in mind the broad recognition that privacy protections are crucial to maintaining the consumer trust that is essential to nurturing the Internet as a political, educational, cultural, social, and business medium. Our challenge is to create a framework that enlarges U.S. prosperity and democratic values while providing meaningful tools to empower individuals to make informed and intelligent choices for protecting their privacy.

Mr. Chairman, I thank you again for the opportunity to testify on this critical issue of commercial data privacy. Over the next few months, the Obama Administration will remain engaged with all of you as Congress continues its consideration of commercial data privacy legislation. Working together with Congress and the FTC, I am confident in our ability to achieve meaningful progress. I welcome any questions you have for me. Thank you.

Mr. SPACE. Thank you, Mr. Weitzner.

And, Mr. Vladeck, you have 5 minutes for your opening testimony.

TESTIMONY OF DAVID VLADECK

Mr. VLADECK. Thank you, Mr. Space, Ranking Member Whitfield, members of the subcommittee. I appreciate the opportunity to be here today to underscore the Commission's support for Do Not Track, a view shared by four of our commissioners. At this point, the Commission has not taken a position on how Do Not Track should be implemented.

But before I discuss Do Not Track specifically, let me note that it is only one aspect of a robust framework for protecting consumer privacy. Throughout its 40-year history of enforcement and policy-making experience, the Commission has tried to protect consumer privacy and build consumer trust in a fast-evolving marketplace.

Yesterday, the Commission issued a preliminary staff report on protecting consumer privacy in the marketplace. This report makes three main points: One, companies should adopt a privacy-by-design approach, baking in protections like security and accuracy throughout their business processes. Two, current practices place too heavy a burden on consumers to safeguard their own privacy. Companies should provide choices about data collection and sharing in a simpler way at a time when consumers are making decisions about their data. And consumer decisions, once made, need to be respected. And three, companies should improve transparency of their information collection and use practices.

Now, Do Not Track is an important component of the second piece of the framework because it would allow consumers to exercise choices about online tracking in a simple, universal, and persistent way. We believe that there is strong public support for a new Do Not Track mechanism, that it is technologically feasible and enforceable, and that, once implemented, it will put consumers back in control of their own data.

Now, we have heard three main objections to the Commission's proposal for a Do Not Track mechanism that I would like to discuss.

Objection number one: Do Not Track would create new privacy problems because it would require the Federal Government to create a registry or list of consumers who do not want to be tracked. Our response? We are not proposing the creation of a list, nor are we proposing a centralized system managed by the Federal Government. While the FTC must be able to ensure through enforcement that a Do Not Track mechanism effectively implements consumer choice, there is no need for a Do Not Track mechanism to be administered by the Federal Government.

Objection two: Industry already provides adequate opt-out choices to consumers. The FTC's response? Self-regulation has been too slow to afford consumers meaningful choice. Many industry representatives agree with the Federal Trade Commission that providing consumers with choices about third-party tracking is essential to build the trust necessary for the marketplace to grow. So, in that respect, there is no difference between the Federal Trade Commission and industry.

And some industry members have taken important positive steps, but existing choices are hard to find and hard to use. Many of these mechanisms also may lead consumers to believe that they are opting out of third-party tracking when, in fact, they are just opting out of receiving targeted ads.

Finally, these mechanisms may not be fully effective. Consumers may believe they have opted out of tracking if they block third-party cookies on their browser, yet they still may be tracked through flash cookies and other devices. A robust Do Not Track mechanism must be clear, easy to locate and use, and effectively implement the user's choice to opt out of third-party tracking.

Objection number three: Do Not Track is neither feasible nor enforceable. The FTC's response? We have learned from our roundtables and from the technologists we have on staff that a Do Not Track mechanism is feasible technologically. Browsers or computers could be programmed to send a Do Not Track signal as the consumers surf the Web. Servers run by ad networks and other companies that engage in tracking would be programmed to receive and honor that request.

Most importantly, this Do Not Track setting would be designed to apply to all third-party tracking methods, thereby putting an end to the current arms race in which some companies subvert consumer choice by developing and using new tracking technologies.

Compliance with tracking by companies is essential. But tracking leaves digital footprints, and the technical means exist that may identify parties that do not respect consumer choice. We believe that these tools can be effective in oversight and enforcement.

Although we are confident that Do Not Track is feasible and can be effective, we are seeking comment on the best way to implement this mechanism.

Let me conclude by saying that if Congress chooses to enact legislation, the Commission requests authority to conduct APA rulemaking and to obtain civil penalties for violations. Rulemaking is important so that the Commission can have flexibility in an area where technology evolves rapidly. And the ability to find violators would provide strong incentives for companies to comply with any legal requirements, helping to deter future violations.

Thank you. We are happy to answer any questions you may have.

[The prepared statement of Mr. Vladeck follows:]

**PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION**

on

Do Not Track

Before the

**COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION
UNITED STATES HOUSE OF REPRESENTATIVES**

Washington, D.C.

December 2, 2010

Chairman Rush, Ranking Member Whitfield, and members of the Subcommittee, I am David Vladeck, Director of the Bureau of Consumer Protection of the Federal Trade Commission (“FTC” or “Commission”). I appreciate the opportunity to present the Commission’s testimony on Do Not Track.¹

Privacy has been central to the Commission’s consumer protection mission for forty years. During this time, the Commission’s goal in the privacy arena has remained constant: to protect consumers’ personal information and ensure that consumers have the confidence to take advantage of the many benefits offered by the ever-changing marketplace. Nevertheless, from time to time, the Commission has re-examined its approach to privacy to ensure that it keeps pace with changing technologies and business practices.

The latest effort in this process is a Commission staff report, released just this week, which sets forth a proposed 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. Next, it sets forth some highlights from the Commission staff’s new report on consumer privacy. Finally, it discusses

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 testimony) is premature. My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

the concept of Do Not Track.

I. The FTC's Efforts to Protect Consumer Privacy

A. Enforcement

The Commission has an aggressive privacy enforcement agenda. In the last fifteen years, it has brought 29 data security cases; 64 cases against companies for improperly calling consumers on the Do Not Call registry; 83 cases against companies for violating the Fair Credit Reporting Act ("FCRA");² 96 spam cases; 15 spyware cases; and 15 cases against companies for violating the Children's Online Privacy Protection Act ("COPPA").³ 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 through legislative recommendations.⁵

In addition, the Commission has brought numerous cases against companies for violating the FTC Act by making deceptive claims about the privacy of the information they collect,

² 15 U.S.C. §§ 1681e-i.

³ 15 U.S.C. §§ 6501-6508.

⁴ 15 U.S.C. §§ 7701-7713.

⁵ See, e.g., Prepared Statement of the Federal Trade Commission Before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the S. Comm. on Commerce, Science, and Transportation, 111th Cong. (Sept. 22, 2010), *available at* <http://www.ftc.gov/os/testimony/100922datasecuritytestimony.pdf>; Prepared Statement of the Federal Trade Commission Before the Subcomm. on Interstate Commerce, Trade, and Tourism of the S. Comm. on Commerce, Science, and Transportation Committee, 110th Cong. (Sep. 12, 2007), *available at* <http://www.ftc.gov/os/testimony/070912reauthorizationtestimony.pdf>.

which has the effect of undermining consumer choices on privacy. Below are four recent examples.

First, the Commission just settled 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 the 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.

Second, this past September, the Commission announced a case against US 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 names still appeared in search results. The Commission's settlement requires US Search to disclose limitations on its opt-out offer, and to provide refunds to consumers who had previously opted out.⁶

Third, this summer, the Commission alleged that the social networking service Twitter deceived its customers by failing to honor their choices to designate certain "tweets" as private.⁷ On one level, Twitter is a traditional data security case – the FTC charged that serious lapses in

⁶ *US Search, Inc.*, FTC File No. 102 3131 (Sept. 22, 2010) (consent order accepted for public comment).

⁷ *Twitter, Inc.*, FTC File No. 092 3093 (June 24, 2010) (consent order accepted for public comment).

the company's data security allowed hackers to obtain unauthorized administrative control of Twitter, including access to private "tweets" and non-public user information. 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 privacy of communications, requires Twitter to maintain reasonable security, and mandates independent, comprehensive audits of Twitter's security practices.⁸

Finally, last year the Commission settled allegations that Sears violated Section 5 of the FTC Act by failing to disclose adequately the scope of consumers' personal information collected via software that Sears represented would merely track their "online browsing."⁹ The

⁸ Many of the Commission's earliest consumer privacy cases similarly held companies accountable for their privacy statements and practices. *See, e.g., GeoCities, Inc.*, 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.*, 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 auction site 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.*, 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*, Docket No. C-4071 (Jun. 28, 2003) (consent order) (same); *Gateway Learning Corp.*, 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*, Docket No. C-4135 (Apr. 19, 2005) (consent order) (alleging that a service provider disclosed customer information in violation of merchant privacy policies).

⁹ *Sears Holdings Mgmt. Corp.*, FTC Docket No. C-4264 (Aug. 31, 2009) (consent order).

FTC charged that the software, in fact, monitored consumers' online secure sessions as well – including those on third-party websites – and collected information such as the contents of shopping carts, online bank statements, email headers and subject lines, drug prescription records, and other sensitive data. In addition to requiring that Sears destroy information previously collected, the settlement provides that if Sears advertises or disseminates tracking software in the future, it must clearly and prominently disclose the types of data the software monitors, records, or transmits and whether any of the data will be used by a third party. This disclosure must be made prior to installation of the tracking software and separate from any user license agreement.

The Commission also looks for opportunities short of formal law enforcement to ensure that companies keep their privacy promises. For example, this past summer, the Commission's Bureau of Consumer Protection sent a letter to individual stakeholders in XY Corporation, which operated a now-defunct magazine and website directed to gay male youth.¹⁰ The letter expressed concern about these individuals' efforts to obtain and use old subscriber lists and other highly sensitive information – including names, street addresses, personal photos, and bank account information – from gay teens. The letter warned that selling, transferring, or using this information would be inconsistent with the privacy promises that were previously made to the subscribers, and may violate the FTC Act; thus, the letter urged that the data be destroyed. After receiving a copy of the FTC letter, the court overseeing bankruptcy proceedings involving the

¹⁰ See Letter from David C. Vladeck to Peter Larson and Martin E. Shmagin (Jul. 1, 2010), available at <http://www.ftc.gov/os/closings/100712xy.pdf>.

XY Corporation ordered the destruction of the information.¹¹

B. Consumer and Business Education

The FTC has done pioneering 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 file sharing, social networking, laptop security, and identity theft.¹²

The FTC has developed additional resources specifically for children, parents, and teachers to help kids 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.¹³ The publication includes information about how parents should talk to children about online privacy, sexting, and cyberbullying. In less than one year, the Commission already has distributed more than 6 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,

¹¹ The Commission staff has issued similar types of letters in other matters involving privacy and data security. For example, earlier this year, it sent letters to companies that had experienced breaches of their computer networks through peer-to-peer file-sharing programs, urging them to review their security practices and take steps necessary to protect their information from unauthorized access. *See, e.g.*, FTC Press Release, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), *available at* www.ftc.gov/opa/2010/02/p2palert.shtm.

¹² *See* <http://www.onguardonline.gov>. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alerta en Línea have attracted nearly 12 million unique visits.

¹³ *See* FTC Press Release, 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>.

for example, social networking and peer-to-peer file ("P2P") sharing.¹⁴

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.

C. Policy Initiatives

The Commission's privacy work also includes 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.¹⁶ Based upon the Town Hall discussions, staff released for public comment a set of proposed principles to encourage industry to improve their behavioral advertising practices.¹⁷ 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)

¹⁴ See <http://www.onguardonline.gov/topics/social-networking-sites.aspx>.

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

¹⁶ FTC Town Hall, *Behavioral Advertising: Tracking, Targeting, & Technology* (Nov. 1-2, 2007), available at <http://www.ftc.gov/bcp/workshops/behavioral/index.shtml>.

¹⁷ 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/P859900stnt.pdf>.

affirmative express consent for the use of sensitive data.¹⁸ This report was the catalyst for industry to institute a number of self-regulatory initiatives, discussed further below.

The Commission also recently conducted a series of public roundtables on consumer privacy,¹⁹ which took place in December 2009, and January and March 2010. The report issued this week 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.

At the roundtables, stakeholders 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, 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 Commission staff released its report this week, proposing a new framework to guide policymakers and industry as they

¹⁸ 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. The revisions primarily concerned the principles' scope and application to specific business models. *Id.* at 20-30.

¹⁹ See FTC Press Release, *FTC to Host Public Roundtables to Address Evolving Privacy Issues* (Sept. 15, 2009), available at <http://www.ftc.gov/opa/2009/09/privacyrt.shtm>.

consider further steps to improve consumer privacy protection. Staff is seeking comment on the proposed new framework through January 2011 and expects to issue a final report in 2011.

II. The Proposed Framework

The proposed framework contains three main concepts. First, the Commission staff proposes 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, companies that collect and use small amounts of non-sensitive 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 proposes that companies provide choices to consumers about their data practices in a simpler, more streamlined manner than has been used in the past. 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 – namely, product and service fulfillment, internal operations such as improving services offered, fraud prevention, legal compliance, and first-party marketing. Some of these practices, such as where a retailer collects 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. 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. The Commission supports such a mechanism, as discussed further below.

Third, the Commission staff proposes 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 consumer groups, regulators, and others can compare data practices and choices across companies, thus promoting competition among companies. The Commission staff also proposes 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 Commission staff believes that the extent of access should be proportional to both the sensitivity of the data and its intended use. In addition, 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 Commission staff proposes 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 facilitating competition on privacy across companies.

In addition to proposing these broad principles, the Commission staff is seeking comment from all interested parties to help guide further development and refinement of the proposed framework.

III. Do Not Track

In considering a uniform choice mechanism for online behavioral advertising, the Commission recognizes the benefits of such advertising, which helps support some of the online content and services available to consumers and allows personalized advertising that many consumers value.²⁰ At the same time, the practice continues to be largely invisible to consumers.

²⁰ See Comment of Microsoft Corporation at 1 (November 6, 2009), available at <http://www.ftc.gov/os/comments/privacyroundtable/544506-00020.pdf>.

Some surveys show that certain consumers who are aware of the practice are uncomfortable with it.²¹ 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 tracking on their sites.²² To address these concerns, the Commission, consumer groups, and leading industry participants²³ have supported the idea of improved transparency and consumer choice over the practice of tracking consumers to serve targeted advertisements.

²¹ 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 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_telecom_and_utilities/006189.html.

One laboratory study demonstrates that consumers are willing to pay more to shop at websites that have better privacy policies. Serge Egelman, Janice Tsai, Lorrie Faith Cranor and Alessandro Acquisti, *Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators*, Carnegie Mellon University, available at <http://www.guanotronic.com/~serge/papers/chi09a.pdf>. Although the study included only consumers who stated they had privacy concerns about shopping online, it showed that these consumers were willing to pay more for privacy.

²² Jessica Vascellaro, *Websites Rein in Tracking Tools*, Wall St. J., Nov. 9, 2010, available at online.wsj.com/article/SB10001424052748703957804575602730678670278.html.

²³ See Press Release, Interactive Advertising Bureau Press Release, *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.

Indeed, the FTC repeatedly has called on stakeholders to create better tools to allow consumers to control the collection and use of their online browsing data. In response, several companies have developed new tools that allow consumers to control their receipt of targeted advertisements and to see and manipulate the information companies collect about them for targeting advertisements.²⁴ An online certification company has launched a pilot program to display an icon on advertisements that links to additional information and choices about behavioral advertising.²⁵ An industry group comprised of media and marketing associations has developed self-regulatory guidelines and an opt-out mechanism for behavioral advertising.²⁶ This group has formed a coalition to develop an icon to display in or near targeted advertisements that links to more information and choices. The coalition has pledged to implement this effort industry-wide.²⁷

In addition, each of the major browser vendors offers a mechanism to limit online tracking with varying scope and ease of use. These browser vendors recognize the importance of offering consumers choices in this area.

²⁴ See, e.g., *Google's Ad Preferences Manager*, Google, <http://www.google.com/advertisements/preferences> (last visited Oct. 21, 2010); *Yahoo's Ad Interest Manager*, Yahoo http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/ (last visited Oct. 21, 2010).

²⁵ See Press Release, TRUSTe, TRUSTe Lanches TRUSTed Ads Privacy Platform (Oct. 4, 2010), available at http://www.truste.com/about_TRUSTe/press-room/news_truste_trustedads.html.

²⁶ See *supra* note 23; Tony Romm and Kim Hart, *Political Intel: FTC Chairman on Self-Regulatory Ad Effort*, POLITICO Forums (Oct. 11, 2010), available at <http://dyn.politico.com/members/forums/thread.cfm?catid=24&subcatid=78&threadid=4611665>.

²⁷ 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 *supra* note 23.

While some industry members have taken positive steps toward improving consumer control, there are several concerns about existing consumer choice mechanisms. First, industry efforts to implement choice on a widespread basis have fallen short. The FTC has been calling on industry to implement innovations such as “just-in-time” choice for behavioral advertising since 2008. Although there have been developments in this area as described above, an effective mechanism has yet to be implemented on an industry-wide basis. Second, to the extent that choice mechanisms exist, consumers often are unaware of them, and click-through rates remain low.²⁸ For example, consumers are largely unaware of their ability to limit or block online tracking through their browsers, in part because these options may be difficult to find; further, those consumers who know about these options may be confused by the lack of clarity and uniformity among the browsers in how choices are presented and implemented.

Third, existing mechanisms may not make clear the scope of the choices being offered. It may not be clear whether these mechanisms allow consumers to choose not to be tracked, or to be tracked but not delivered targeted advertising. Also, consumers may believe that opting out at one company or website will prevent tracking or will block personalized advertising – or even all advertising – everywhere. Finally, consumers are not likely to be aware of the technical limitations of existing control mechanisms. For example, they may believe they have opted out of tracking if they block third-party cookies on their browsers; yet they may still be tracked

²⁸ *Transcript of December 7, 2009, FTC Privacy Roundtable*, Remarks of Alan Davidson of Google, at 113, available at http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdf.

through Flash cookies or other mechanisms.²⁹

Given these limitations, the Commission 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. To be effective, there must be an enforceable requirement that sites honor those choices.³⁰

Such a mechanism would ensure that consumers would not have to exercise choices on a company-by-company or industry-by-industry basis, and that such choices would be persistent. It should also address some of the concerns with the existing browser mechanisms, by being

²⁹ 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, the consumer does not delete Flash cookies stored on his computer. Instead, the consumer must know that Flash cookies exist, go to the Adobe website, and follow the instructions provided there to have them removed.

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*, N.Y. Times, Oct. 10, 2010, available at <http://www.nytimes.com/2010/10/11/business/media/11privacy.html>.

³⁰ As is often true with online privacy, it may be difficult for consumers to ascertain which parties are not respecting their choices. However, technical methods exist that may reduce the ability of sites to track users, or that may identify parties that do not respect consumer choices not to be tracked for behavioral advertising. The Commission believes these tools could be effective to help monitor and enforce a uniform choice mechanism.

more clear, easy-to-locate, and effective, and by conveying directly to websites the user's choice to opt out of tracking. Such a universal mechanism could be accomplished through legislation or potentially through robust, enforceable self-regulation.

If Congress chooses to enact legislation, the Commission urges Congress to consider several issues.

First, any such mechanism should not undermine the benefits that online behavioral advertising has to offer, by funding online content and services and providing personalized advertisements that many consumers value.

Second, such a mechanism should be different from the Do Not Call program in that it should not require a "Registry" of unique identifiers. In the context of the Do Not Call program, each telephone already has a unique identifier in the form of a phone number. In contrast, there is no such persistent identifier for computers, as Internet Protocol ("IP") addresses³¹ can change frequently. Rather than creating such an identifier in this context, which would raise significant privacy issues,³² the Commission recommends a browser-based mechanism through which consumers could make persistent choices.³³

Third, some companies currently offer consumers a choice between opting out of online behavioral advertising altogether or affirmatively choosing the types of advertising they receive.

³¹ An Internet Protocol address (IP address) is a number that is assigned to any device that is connected to the Internet.

³² A new identifier would be yet another piece of personally identifiable information that companies could use to gather data about individual consumers.

³³ Although the practicalities of a proposed choice mechanism here would differ from Do Not Call, it would be similar in that it would allow consumer to express a single, persistent preference regarding advertising targeted to them.

For example, at the roundtables, one company described how it shows consumers the categories of advertising associated with them, and allows them to de-select those categories and select additional ones.³⁴ The panelist noted that, when given this option, rather than opting out of advertising entirely, consumers tend to choose to receive some types of advertising.

As this example illustrates, consumers may want more granular options. We therefore urge Congress to consider whether a uniform and comprehensive choice mechanism should include an option that enables consumers to control the types of advertising they want to receive and the types of data they are willing to have collected about them, in addition to providing the option to opt out completely.

Fourth, it is imperative that any universal choice mechanism be understandable and simple. In addition to being easy to find and use, such a mechanism should make it clear to consumers exactly what they are choosing and if there are limitations to that choice.

Finally, if Congress does choose to enact legislation, the Commission requests the authority to conduct rulemaking under the Administrative Procedure Act and to obtain civil penalties to enforce the legislation. Rulemaking authority is important so that the Commission can have flexibility in an area where technology evolves rapidly. And the ability to fine violators would provide a strong incentive for companies to comply with any legal requirements, helping to deter future violations.

³⁴ *Transcript of December 7, 2009, FTC Privacy Roundtable*, Remarks of Alan Davidson of Google, at 101-02, available at http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdf.

V. Conclusion

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

Mr. SPACE. Thank you, Mr. Vladeck.

And, at this time, the chair will entertain questions of the witnesses. And our first on the list will be our chairman emeritus, Mr. Dingell.

Mr. DINGELL. Mr. Chairman, thank you very much.

The time that you have and I have is very limited, so if you would please, gentlemen, could you give me “yes” or “no” answers to the first question here?

Do you believe the current industry efforts to regulate itself with respect to consumer data privacy are sufficient enough to address consumer concerns? Yes or no?

Mr. VLADECK. No.

Mr. DINGELL. Sir?

Mr. WEITZNER. No.

Mr. DINGELL. Now, gentlemen, again, yes or no. Do you believe that such efforts could be improved, or do you believe that the Congress should pass comprehensive online privacy legislation?

Mr. VLADECK. That is two questions.

Mr. DINGELL. Well, all right. Then to the first half, yes or no, and then to the second half, yes or no. And you are perfectly right.

Mr. VLADECK. On the first half, yes, we believe that self-regulation can improve the current system.

And with respect to the second question, the Commission has not taken a position on whether legislation is needed.

Mr. DINGELL. OK.

Sir?

Mr. WEITZNER. With respect to the first question, we are confident that the industry efforts can improve.

With respect to the second question, the administration hasn’t taken a position yet.

Mr. DINGELL. Now, gentlemen, here is a problem that I think all of us confront. Is there a single Federal agency that is capable of implementing and enforcing Do Not Track requirements? Is there a single agency?

Mr. VLADECK. We believe there is.

Mr. DINGELL. OK. Now, then—and, sir, your comment, if you please?

Mr. WEITZNER. I think there is an agency that could.

Mr. DINGELL. All right. Now, which one is it, or which one should it be—FTC, NTIA, or the FCC?

Mr. WEITZNER. You go first on that one.

Mr. VLADECK. Yes, we believe that we have both the ability and the enforcement infrastructure. Of those agencies, the Federal Trade Commission is the enforcement agency. And we think that we are up to the task.

Mr. WEITZNER. We have great confidence in the FTC as an enforcement agency. And NTIA, as you know, is not a regulatory agency.

Mr. DINGELL. And I hope you don’t take that as being an unfair question to you.

Very frankly, I would make this observation. The FTC has a rather proud record of doing these kinds of things at the behest of the Congress and doing them well.

Now, gentlemen, again, advertising plays an essential role in the support of free Web sites and Internet applications. What impact would—and this can't be a yes-or-no question—what impact would a Do Not Track proposal have on that support?

Mr. WEITZNER. I think the answer is going to depend quite a bit on what the Do Not Track mechanism is and what it means.

What we know is that there are more and more companies that are offering users some kind of opt-out and enhanced notice mechanism. I don't believe that we have seen dramatic falloff of advertising revenue as a result.

I think that there are mechanisms that could be mandated which could have a dramatic impact on advertising revenue. I think that counsels to look at the issue very carefully so that we don't disrupt the Internet economy.

Mr. DINGELL. It is a concern, then?

Mr. WEITZNER. Yes.

Mr. DINGELL. Thank you.

Now, gentlemen, should a Do Not Track mechanism involve simply no collection of information, or should it include a prohibition on the use of such information to target consumers?

Mr. VLADECK. I will take the first stab at that.

I think that what we envision is a Do Not Track mechanism that would permit consumers—first of all, we don't believe that a Do Not Track mechanism is necessarily an all-or-nothing, one-time-or-forever mechanism. We believe that the point of Do Not Track is to give consumers control over the collection of data, through tracking, that they do not want to have collected.

And so, if you look at both the testimony, our report, and the questions that the report poses for industry, we want to explore tailored Do Not Track that would enable consumers to permit certain kinds of tracking but to exclude other kinds of data collection and, therefore, data use.

Mr. DINGELL. Sir?

Mr. WEITZNER. I would say that data collection limitations are a very blunt instrument and tend to have unexpected consequences and sometimes may make false promises to users. I think that the concerns that we see, however, are split between concerns about collection and concerns about use. It is a difficult question.

Mr. DINGELL. Gentlemen—and my time is running out here—it seems that Do Not Track, as it is presently discussed, is all or nothing, meaning that either a user permits his data to be collected or he does not allow such data to be collected.

Is there a middle-of-the-road approach that could be adopted and a regulatory structure that could be constructed that would enable us to do this in a proper way, giving consideration to the concerns of everybody?

Mr. VLADECK. I think the answer to your question is “yes.” And one of the things the Federal Trade Commission is exploring is a Do Not Track mechanism that provides consumers with great choice about what information they are willing to have collected through tracking and what information they are not.

And so, our effort is to—we have solicited comment on this, but our effort is to devise a system that gives consumers very broad

and granular control over the tracking of their personal information.

Mr. DINGELL. Sir?

Mr. WEITZNER. Congressman Dingell, I think it is very important to recognize that this question doesn't arise in a vacuum. For 10 or 15 years in the evolution of the Internet advertising environment, we have had an evolution of mechanisms that give users increasing control over how their information is used and increasing awareness of how it is used.

We think it is very important to continue that trend and to encourage that to continue to happen. I think that will help to get to some of the more nuanced mechanisms that my colleague, Mr. Vladeck, is talking about.

Mr. DINGELL. Thank you, gentlemen.

Mr. Chairman, I would like to pay just a brief word of tribute to you. You have served here well and with distinction. I am proud to see you running the committee today. I am grateful to you for your excellent service in this institution. And I want to congratulate you and commend you and wish you well on behalf of John Dingell and, I think, on behalf of the rest of my colleagues on the committee.

Thank you.

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

And our next questioner is the ranking member, Mr. Whitfield of Kentucky.

Mr. WHITFIELD. Well, thank you very much.

I would like to echo Mr. Dingell's comments, Mr. Space, and tell you how much we enjoyed serving with you. And we know we will look forward to seeing you in the future as we move along.

Thank you all for your testimony very much. We appreciate it.

With the release of the privacy report yesterday, I believe Chairman Leibowitz referred to a privacy deficit, and he sort of compared that to a budget deficit. And there is no question, we have a budget deficit.

And so that raises the question, when he is talking about a privacy deficit—and I think both of you have indicated that you are not advocating Do Not Track legislation at this time—how severe do you think this privacy deficit is that Mr. Leibowitz talked about yesterday?

Mr. VLADECK. We spent a full year developing a record that underpins the report that we issued yesterday. And there are two themes that I think emerged from the roundtables that we held and from our interactions with every imaginable stakeholder.

One is the general concern that consumers are not aware that they are being tracked online and the extent of tracking and what has really happened, which is there is a commodity now in personal data. There is, you know, a data collection and use industry. And so, I think one concern is that we need to make this clear to the public, we need to educate the public. And I suspect that when Chairman Leibowitz was talking about the deficit, that was part of what he was addressing.

The other theme is that people do not feel they have adequate control over their data when they browse. And I recognize that industry has come up with some browser-based options and some

other efforts to try to respond to consumer demand for greater control. Our concern is those efforts have fallen short. And one of the reasons why we thought we needed to issue this report is to talk about the gap, the mismatch between consumer demand and expectation and what is presently being offered. And we are hoping that a report will stimulate discussions like this so we all collectively can move forward.

Mr. WHITFIELD. Thank you.

Mr. WEITZNER. Congressman Whitfield, here is what I think we know. I wouldn't necessarily say that we have a deficit because that presumes it is quantifiable in some way. But I think we have two almost disparate facts, almost contradictory facts before us. We see people using the Internet more and more and more. We had a very positive Cyber Monday, if that is what it is called. So we see people embracing this technology in so many ways, and we certainly want that to continue.

What we also know from surveys, from public comments, from the consultations that we have done at the Commerce Department with a very wide range of stakeholders is that there is increasing concern on the part of the public about how privacy is being handled. People are not sure exactly what their rights are, they are not exactly sure how to protect them, who to go to when they feel wronged.

I think that, if there is a gap, it is perhaps there, in the fact that the Internet is more and more important to us but we have increasing uncertainties. And I think it is worth working collectively to close that gap.

Mr. WHITFIELD. Thank you very much. I appreciate that.

Recognizing that the advertising model is so important to the Internet and trying to balance that versus privacy protection, do both of you feel confident that we could come to a solution on this issue somewhere down the road where you can protect both of these in an adequate manner?

Mr. WEITZNER. I think that what we have seen, as I alluded to in the previous interchange, is that Internet users have actually been given more and more control through the various services that we all use on the Internet. We haven't seen advertising revenue go down. If anything, we have seen it go up and we have seen it proliferate into a whole new variety of business models.

That is a very positive change. I think we would certainly want to watch very carefully to make sure not to take steps that would turn that in the other direction. But I think it is a mistake to assume that giving people more control means a reduction in advertising revenue.

Mr. WHITFIELD. OK.

Mr. VLADECK. Yes, we share that view. And let me make two brief points. One is, you know, no one wants to interfere with innovation and business development on the Internet. It is a very powerful engine that drives a big part of our economy. But we don't want to sacrifice consumer privacy at the same time.

And, in fairness to industry, industry recognizes this. I mean, the advertisers have banded together to give consumers opt-out rights against targeted advertising. I can't imagine that they would want to kill the golden goose that laid the golden egg. And so I don't

think—I think that, in terms of our aspirational goals, you know, we are not that far apart.

Mr. WHITFIELD. Well, thank you very much. I really appreciate your testimony.

And my time has expired, Mr. Chairman.

Mr. SPACE. Thank you, Mr. Whitfield.

Mr. Green from Texas.

Mr. GREEN. Thank you, Mr. Chairman.

I would like to ask unanimous consent that my statement be placed into the record.

[The information was unavailable at the time of printing.]

Mr. GREEN. And thank each of you for being here. This is an issue that our committee and not only this Subcommittee on Consumer Affairs but also our Telecom Subcommittee has dealt with for many years. And I have always come down on the side of, if I am using the internet, I would rather have the option of opting in to have someone track me than opting out.

And that is my first question, is, would constructing a framework that allowed the Internet users to actively opt in to tracking be a more feasible approach? Now, we know, in practicality, very few people opt in. And if you opt out, there will be more people who just won't take the time to opt out.

What are the strengths of the opt-in? And how is Do Not Track better? The two options, opt-in or opt-out.

Mr. VLADECK. Let me answer that question in two ways.

In terms of the strength of Do Not Track, our view is that it would be uniform, easy-to-use, and a durable choice by consumers, a choice they can change and a choice they can modify. But under the existing regime, in order for consumers to, for example, not receive delivered, targeted behavioral advertising, they have to go to multiple sites that are hard to use and often are confusing. So we are trying to relieve the burden on the consumer to exercise choice. And, in our view, a Do Not Track mechanism is the ideal solution to that problem.

Now, in terms of opt-in and in terms of opt-out, we have requested comments on this, because we have seen both mechanisms used by marketers in a way that are confusing to consumers. You have seen opt-ins that simply require you to click a button after reading through a long, you know, end-user licensing agreement that you don't read because no one reads them. And we have seen opt-out mechanisms that are also confusing to use.

So what we are hoping to do here is to find a simple, easy-to-use, easy-to-find tool that consumers can use to express their choice about being tracked and how much they want to be tracked, if at all. That is the goal of the Federal Trade Commission.

Mr. WEITZNER. Congressman Green, I would just echo my colleague's views here.

Historically, as you know, the privacy debate has always been framed as this kind of stark opt-in versus opt-out choice. I think our goal should be to move beyond that and to create an easy set of choices for users to have access when it makes sense for them to have access.

I think that this opt-in/opt-out model really ignores the fact that Internet technology can make choices much more easy and much more accessible.

Mr. GREEN. OK. Will implementing a Do Not Track list create a false sense of security for users? What can complement the Do Not Track system to keep users informed of the remaining potential data collections and tracking and inform them of measures they can take to limit if they choose? Because even if you opt out of the tracking, what is the security that you know that you are not being tracked?

Mr. WEITZNER. I think that that comes, in many ways, to a definitional question about just what Do Not Track or Do Not Profile or Do Not Advertise really comes to mean and the question of who is ultimately going to be accountable to answer the preferences that are expressed by users.

I would say that I think there is a growing agreement in the technical community that it is not so hard to understand how to enable a user to send out a Do Not Track signal. The question is, who is supposed to listen to that signal? And I think that is a hard question to answer.

As Mr. Vladeck noted, we want to give users a subtle set of choices so that their complex preferences can be represented, but I think we risk, if we try to draw lines too firmly, we do risk creating a false sense of security.

Mr. VLADECK. Well, can I respond briefly?

We want to provide a sense of security. And one of the design features that can be built into a Do Not Track mechanism is an end to what we now see as an arms race, that many companies are engaged in defeating consumer choice by developing tracking devices that are not easily removed.

And so, part of our concern is we do not want to get into an endless cycle where a browser is able to remove cookies, tracking cookies, but isn't able to deal with flash cookies or super cookies or the next generation of tracking devices.

Mr. GREEN. One of the concerns I have is—and we haven't dealt with this before—is there authority with the FTC and even with NTIA to do this? What is to keep it from happening in Great Britain or, you know, somewhere else, Switzerland or somewhere else? They just move those browsers there, and we lose the ability to control them in our own country.

Mr. WEITZNER. I think that the point that you are underscoring, Congressman Green, is the need to have broad agreement about just what these promises and these commitments really mean, what should a consumer really be able to expect.

We have urged, as we have talked about this issue, the need to come to broad voluntary agreements amongst industry groups that spread across the globe and consumer groups that increasingly represent different countries so that we can have what is something closer to a global set of expectations. The Internet is a global marketplace, and we are going to need that more and more.

Mr. VLADECK. Well, there is another answer, as well, Congressman, which is that, if we successfully implement a Do Not Track regime in the United States, tracking devices, for example,

launched in another country, will not be able to track the consumer unless the consumer starts visiting sites somewhere else.

And that question is a question that we have explored with our own technologists, including—and I am happy to introduce Dr. Ed Felton, who is a Princeton University computer science professor who will be joining the Federal Trade Commission as our chief technologist at the first of the year.

But, I mean, there are real disadvantages to trying to end-run a Do Not Track system simply by moving a server, you know, into another country. And we would be glad to, at another time, explain why that would not necessarily bypass a Do Not Track system.

Mr. GREEN. Well, I think, having dealt with this for many years, I think our committee on a bipartisan basis falls on the side of the privacy. And my last question is, are there any types of information that you feel shouldn't be tracked or just hardcore shouldn't be collected at all?

Mr. VLADECK. One of the reasons why we have gravitated to a Do Not Track option is because there are certainly categories of information—health information, family information, financial information, maybe information concerning not only children but teens, geo-location data, religious information, political information—that people probably do not want tracked and that data collected.

And, therefore, a Do Not Track option would empower consumers to avoid being tracked and have their data collected in those sensitive areas.

Mr. GREEN. Thank you, Mr. Chairman.

Mr. SPACE. Thank you, Mr. Green.

I do have a couple of questions of my own before we get to the next panel. First, I would be remiss if I didn't reference something that I always reference in hearings having to do with broadband and digital technology, and that is, and I know it is a little off point, but it is important to a lot of people in this country who don't have any access to the Internet. And I want to commend both NTIA and the FTC for their efforts in promoting rural broadband access universally.

That digital technology has become such a profound part of our everyday life experience, our economies, and has happened in just the last 10 or 15 years. And imagine where we will be in 10 or 15 years from now.

So I mention that just because I want to underscore the importance of making up for this rural divide that exists in this country when it comes to access.

The fact of the matter is digital communication is integrated very heavily into our economy and integrated very heavily into the everyday life of consumers in all realms, health care, education, et cetera.

One of the concerns I have on this particular issue, the privacy issue, is the lack of sophistication of the normal consumer vis—vis that of the normal carrier and telecom provider. At the same time, I am cognizant of the importance of profitability and that Do Not Track legislation may have an adverse effect on that bottom line.

I further understand that the industry itself has attempted several times to deal with the privacy concerns, and my assumption from your testimony is that you feel it has inadequately done so.

My understanding is there is a coalition in the industry with approximately 5,000 participating companies, according to the Interactive Advertising Bureau. And we checked just last week, I think there were 58 actual participating companies.

I would be interested in your impression as to the level of industry commitment to this issue and what nonlegislative means might be available to help stimulate greater interest among industry?

Mr. WEITZNER. Thank you, Congressman Space.

And, first of all, thank you for your attention and your leadership on the rural Internet access issues. It is a major priority, as you know, for NTIA, and we appreciate your support on that.

I would say that there have been ongoing industry efforts from the very beginning of the commercial Internet environment to help users understand how to use their services, how to protect themselves, for example, against content that they don't want to receive, that they don't want their children to receive. And I would say as well there have been efforts to help educate users about privacy protection. Those efforts, I believe, have to be ongoing and have to be stepped up. I think it is not fair to say that there have been no efforts, but certainly, we think the efforts ought to be increased.

In the work that we have been doing on privacy at the Department of Commerce, one of the things that we have learned is that it is really critical to develop what we have called a multi-stakeholder approach to privacy protection, to have industry groups working together with consumer advocates, together with regulators, together with State attorneys general, all of whom have a significant responsibility in this area, and we certainly hope, going forward, that it will be possible to find ways to encourage those efforts. They clearly have to be stepped up.

I think that consumer education on the Internet happens very often really through the design of services, not so much through talking to users. You think about how we have had hundreds of millions of people learn to use the Internet. It has been because services have been built so that they are easy to use, so that the tools that people want are accessible, and I think we have to apply that kind of innovation and accessibility to the privacy area.

Mr. VLADECK. Let me just add a few thoughts, if I may.

One is, on the educational side, I agree completely with Mr. Weitzner that we need to do more. One important recommendation we make in our privacy report is that we start engaging in privacy by design; we build privacy in from the start. And we need to do a better job of doing that.

On some of the smartphones, for example, now, they will let you know when your geolocation data is being shared. We need to broaden those kind of technological innovations to alert consumers about privacy issues.

Second, I think that the Federal agencies need to do a better job as well as industry in terms of public education. We take public education very seriously. We have distributed now nearly 5 million copies of a booklet designed for parents and kids to learn about Internet use, smartphone use. This is a book called "Net Cetera" that has been distributed in school districts around the country.

Finally, the second point is that with respect to your industry stepping up to the plate question, nothing in our report and noth-

ing in our testimony would preclude a robust, inclusive, enforceable, Do Not Track regime, self-administered by industry, provided that these commitments were backed up by an enforceable regime, such as the one that the Federal Trade Commission administers under Section V. We need to have a system in place in which consumers have confidence that their choices are being respected.

There is nothing that would preclude a self-regulatory regime, as long as, at the end of the day, there is a law enforcement agency that would be able to single out and to go after people who did not engage in that kind of respect.

Mr. SPACE. Thank you, gentlemen.

The gentleman from Massachusetts, Mr. Markey, is recognized.

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

As cochairman of the Bipartisan Privacy Caucus with Joe Barton and former chairman of the Telecommunications and Internet Subcommittee, I have long believed that consumers should have control over their own personal information.

When it comes to kids and their use of the Internet, it is particularly important that stringent privacy protections are applied so that children do not have their online behavior tracked or their personal information collected or disclosed.

In 1998, I was the House author of the Children's Online Privacy Protection Act, or COPPA, which was signed into law by President Clinton. COPPA places parents in control over what information is collected from their children online. My law covers children aged 13 and under, and it requires operators of commercial Web sites and online services directed to children under 13 to abide by various privacy safeguards as they collect, use, or disclose personal information about kids.

Those requirements are still on the books and are kind of the "constitution" right now for the protection of children, and those were important safeguards. But in Internet years, 1998 is so long ago. We might as well be talking about the Peloponnesian War. The 1990s was back in the BF era, Before Facebook, just another time and place.

Now is the time for new legislation to protect kids and to prevent them from being tracked online. That is why next year I plan to introduce comprehensive children's privacy legislation that will include a Do Not Track requirement so that kids do not have their online behavior tracked or their personal information collected or profiled. I look forward to working with my colleagues to move this legislation forward.

I also want to commend Commonsense Media and its CEO, Jim Steyer, for their excellent work in this area. For many kids, the Internet is like online oxygen. They can't live without it. The Internet enables kids to access incredible opportunities that were unimaginable only a few years ago. But we must also protect children from the dangers that can lurk in this online environment.

We thank the two of you for your longstanding commitment to ensuring that protection is there for children.

May I ask, Mr. Vladeck, in your testimony, you indicate the Federal Trade Commission's support for development of a Do Not Track capability so consumers can avoid having their activities monitored online. As you know, in its ongoing series on online pri-

vacy, the Wall Street Journal has reported that popular children's Web sites install more tracking technologies on personal computers than do the top Web sites aimed at adults. Now, I am extremely concerned about that trend.

Is that practice used by those Web sites covered by COPPA?

Mr. VLADECK. So, remember, we are talking—COPPA covers children 12 and under, and we believe it is—that COPPA would apply.

We have accelerated our review of COPPA in large measure because of exactly the concerns that you have outlined. That is, today, for many children, the Internet is a playground of the sort that we used to play in, except they spend a lot of time on the Internet. So we have accelerated a review of our COPPA rule.

We just held a roundtable a few months ago to explore these issues and other issues that are raised; online gaming sites where children spend a fair amount of time only, the migration of these interaction sites to smartphones. So, yes, we share your concerns about this and we look forward to working with you in crafting legislation.

Mr. MARKEY. Do you want legislation to pass that gives you the specific authority to be able to deal with these issues?

Mr. VLADECK. I am not authorized to speak for the commission on this issue. I will say that in beginning our COPPA review process, one possible end of it would be legislative recommendations. And so we may well—our interests may well coincide here because we are hoping to make our recommendations about COPPA within the next few months.

Mr. MARKEY. Well, I will be looking forward to your comments on my legislation.

In response to the question of whether or not self-regulation in fact works in this industry, your answer is that—

Mr. VLADECK. It is not—in our view, self-regulatory efforts have thus far fallen short.

Mr. MARKEY. And you agree with this as well?

Mr. WEITZNER. We think they could be a lot more urgent and robust, and we are looking at ways to encourage those efforts, particularly as to children.

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

Mr. MARKEY. I thank the gentleman for the time you have given me and thank you for your excellent service to our country as well.

Mr. SPACE. Thank you. At this point, the chair recognizes the gentlewoman from the great State of Ohio, Betty Sutton.

Ms. SUTTON. I thank the chairman.

And I, too, add my voice to those who thank you so very much for your service to our country and, of course, to the great State of Ohio. We appreciate all that you have done. You have made the lives of the people that I represent better through your service, and we will miss you on this committee and in this Congress.

Thank you, gentlemen, for your testimony. The first thing I want to talk about is, the Wall Street Journal pointed out, in a story called "Slow Going for Web Piracy Software," that it is a challenge to get people to pay for Web privacy software. Nonetheless, there are firms that are sprouting up that, for a fee, will help people protect their online privacy. And the purveyors of these companies, de-

spite the slow going, appear sort of optimistic about the future of this.

In fact, the head of one such firm has glowingly referred to the emergence of a “privacy economy” in response to a growing concern about the amount of information being collected and stored about each of us and how it could potentially be used.

This particular service, for an ongoing fee, helps people scrub their online reputations and to remove themselves from tracking networks. One of the ways it gets data collectors to remove its clients information is by paying them a fee.

This notion of a privacy economy seems to be premised more on the idea that data collectors will make their money either by selling your information to someone else or by getting you to pay to stop it from being used.

It also sounds like privacy is being transformed into a commodity available to those who can afford it.

So, gentlemen, should we be concerned that if government and industry fail to address quickly and appropriately in a more robust baseline privacy protections, that what we might have emerge instead is something like a privacy economy, where some people will be able to buy privacy and others won't?

Mr. WEITZNER. That is a complex question, Congresswoman Sutton.

I would say that, first of all, it is great news that there is innovative energy out there looking to give people more control over their information, to shape their Internet experience as they choose, and I think we can all hope that those efforts succeed.

I think that some of those—it is not clear that that is going to ever offer the whole answer to the privacy question. There is no doubt that there is money to be made, businesses to be developed in this increasingly complex economy of personal information, and we welcome that.

Some of the privacy concerns that people have, however, are not economic; they are not just about whether they get a penny or two for the use of their information. It is about how trustworthy they feel the online environment is. It is about whether they are treated fairly by those who they do business with. So I think we have to always keep in mind that there is a non-economic component to this as well, where I think a lot of the Federal Trade Commission's work over the last decade has been very important.

Mr. VLADECK. Let me add one thought, which is, we want to build confidence and trust in the Internet economy, and having to pay a fee in order to engage in a retrospective effort to claw back personal information doesn't seem to us the right way to go about this.

Ms. SUTTON. And as I indicated in my question, that is actually what currently is starting to evolve. OK.

I appreciate the work that both the FTC and the Department of Commerce have devoted thus far to developing the frameworks for protecting consumers' privacy as indicated by your answers here today, and how to best protect consumers' privacy is clearly an important and complicated issue.

But both the FTC and Commerce have devoted nearly a year to listening to and distilling stakeholders' views and recommendations

on this issue, and the idea that a more robust and effective approach must be taken to protecting consumers' privacy has been percolating for even longer than that. And while the FTC report provides a proposed framework for protecting consumers' privacy, it also raises more questions and asks for more feedback, and I understand that, and I understand the report from the Department of Commerce is going to take the same approach.

So, Mr. Weitzner, do you know when we should expect Commerce to issue its report?

Mr. WEITZNER. We are hoping it will be very soon now, Congresswoman Sutton, certainly in weeks, not months, is our expectation.

Ms. SUTTON. And will that report also raise more questions and request more feedback?

Mr. WEITZNER. It will, Congresswoman. And I will say that our goal really is to be able to contribute to the public dialogue in general and also to the administration, the broad administration deliberation on privacy policy questions, including the question of how to respond to legislative proposals that are out there now and additional ones that will come.

So we felt that we have had to take a—do a very broad consultation, and we have had a chance to do that. We are optimistic that that will contribute to the debate. We do feel a real sense of urgency about moving forward on this issue, both because of the domestic situation and also because of the global situation.

Ms. SUTTON. Thank you.

Mr. SPACE. Does the gentlewoman yield the balance of her time?

Ms. SUTTON. Do I still have time?

Mr. SPACE. Now your time has expired.

Ms. SUTTON. I would love to ask more questions.

Mr. SPACE. Thank you, gentlemen, for your testimony.

In dismissing you, I would like to again extend the committee's gratitude for the work you do and for your testimony today.

STATEMENTS OF SUSAN GRANT, DIRECTOR OF CONSUMER PROTECTION, CONSUMER FEDERATION OF AMERICA; JOSEPH PASQUA, VICE PRESIDENT OF RESEARCH, SYMANTEC CORPORATION; JOAN GILLMAN, EXECUTIVE VICE PRESIDENT AND PRESIDENT, MEDIA SALES, TIME WARNER CABLE; EBEN MOGLEN, LEGAL ADVISOR, DIASPORA, PROFESSOR OF LAW, COLUMBIA UNIVERSITY, FOUNDING DIRECTOR, SOFTWARE FREEDOM LAW CENTER; AND DANIEL CASTRO, SENIOR ANALYST, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

Mr. SPACE. I would ask that the second panel step forward to the table. While you are situating yourselves, I will introduce you and then swear you in.

We have with us Ms. Susan Grant, director of consumer protection of the Consumer Federation of America; Mr. Joseph Pasqua, vice president of research, Symantec Corporation; Ms. Joan Gillman, executive vice president and president, Media Sales, Time Warner Cable; Dr. Eben Moglen, legal advisor, professor of law, Columbia University, and founding director, Software Freedom Law Center; and Mr. Daniel Castro, senior analyst, Information Technology and Innovation Foundation.

If you could find your seat, and I would ask that you rise so I may administer the oath.

[Witnesses sworn.]

Mr. SPACE. Let the record reflect that the witnesses have all answered in the affirmative.

Ms. Grant, I will start with you. But before we begin with the testimony, I find it necessary, Mr. Moglen, to make some specific remarks in advance before, once again, I yield the floor.

We as Members of Congress are never inclined to censor testimony or to influence a witness's remarks in open congressional forums, including this hearing.

Having said that, Congress tries mightily to preserve the highest standards of decorum to foster the most constructive dialogue and debate possible on important matters like consumer privacy.

Accordingly, I would ask you to provide your oral testimony without making any comments that could be construed as a personal attack against any company or any company's employees.

I would also ask for unanimous consent that Mr. Moglen be given an opportunity to revise his written remarks and submit the same within 5 days.

Hearing no objection, it is so granted.

With that, I would introduce Ms. Susan Grant, director of consumer protection, Consumer Federation of America, for her 5 minutes of testimony.

STATEMENT OF SUSAN GRANT

Ms. GRANT. Thank you.

On behalf of Consumer Federation of America, an association of nearly 300 consumer organizations in the United States, I am pleased to provide our perspective on this important question, Is now the right time for Do Not Track legislation? And our answer is, not surprisingly, yes.

As a recent Wall Street Journal investigation series, "What They Know," so clearly detailed, consumers are being tracked on the Internet, wherever they go, whatever they do, without their knowledge or consent. Information about their online activities, what they search for, what they click on, what they purchase, what they share with others, who their friends are in social networking sites, is compiled, analyzed and used to profile them. Sometimes information is gathered about their offline activities to create even richer profiles.

This tracking is primarily used for marketing at this time, but it can also be used to make assumptions about people for employment, housing, insurance, and financial services, for purposes of lawsuits against individuals, and for government surveillance. There are no limits to what this type of information can be used for, what information can be collected, how long it can be retained, and with whom it can be shared.

As the Wall Street Journal characterized it, "one of the fastest growing businesses on the Internet is the business of spying on consumers."

If someone were following you around in the physical world, tailing you and making note of everywhere you go, what you read, who you talk to, what you eat, the music that you listen to, what you

buy, what you watch, you might find this disturbing. The argument that we don't know your name, just the make and model of your car, and we are only going to use this information for advertising, might not assuage your concerns about being stalked.

On the Internet, even if the tracker doesn't know your name, you are not anonymous. As the Federal Trade Commission and Members of Congress have recognized, your Internet protocol address and other unique persistent identifiers are essentially personally identifying information, and, as the Wall Street Journal put it, the skill of data handlers is "transforming the Internet into a place where people are becoming anonymous in name only."

The ability to cross-reference data makes it easy to make assumptions about people and treat them a certain way based on information that has been collected about their activities, even if you don't know their names. Furthermore, as news reports and scholarly articles have described, it is relatively easy to re-identify data that is supposedly anonymous.

With more and more people using the Internet as an essential tool for communications, education, managing their finances, researching health and other sensitive subjects, buying goods and services, sharing information through social networks, engaging in political and civil discourse, accessing government programs and benefits, and storing personal and workplace documents, it is crucial that they be able to exert effective control over the collection and use of what is gleaned about their online activities.

No matter what one thinks about the benefits and risks of online tracking and behavioral advertising, and there are many different views, the fact is that consumers have the basic right to privacy and that right should be respected.

While online behavioral tracking and targeting is less visible to consumers than telemarketing, surveys clearly show that people are uncomfortable with this practice. For instance, a 2009 survey by researchers at the University of Pennsylvania and the University of California found that 66 percent of respondents did not want Web sites they visit to show them tailored ads, and when the common tracking methods were explained to them, an even higher number rejected tailored advertising.

More recently, a poll commissioned by the nonprofit organization Consumer Watchdog this past July revealed that 90 percent of Americans wanted more laws to protect privacy; 86 percent favored the creation of an anonymous button that allows you to go online without being tracked; and 80 percent wanted a Do Not Track me list.

When the FTC announced in 2003 that it was creating the national Do Not Call registry, it acknowledged that the company-specific approach, which obliged consumers to inform each company one by one that they didn't want to receive tele marketing calls, was "seriously inadequate to protect consumers' privacy from an abusive pattern of calls from a seller or telemarketer," and that consumers were angered and frustrated by the telemarketing calls that they were receiving.

The FTC also said that industry's self-regulatory programs, such as the Direct Marketing Association's telephone preference service, fell short because they were voluntary, and to quote them, "to the

extent that sanctions exist for noncompliance, DMA may apply those sanctions only against its members, not nonmembers.”

The National Do Not Call Registry is a big success because it provides consumers who don’t want to receive telemarketing calls with an easy to use mechanism to opt out, and just as importantly, telemarketers have to honor their opt out request.

As noted in the privacy report released by the FTC yesterday, voluntary programs by individual companies and industry associations through which consumers can opt out of online tracking are not adequate. We agree with the FTC that these programs have not been implemented widely enough; that consumers are unaware of them; that consumers may be confused by the lack of clarity and uniformity in the way that these various programs work; that these programs may not—may result in blocking personalized advertising from being delivered to consumers but may in fact not stop tracking, which could be used for other purposes; and that because these programs rely on cookies, they are not necessarily effective against all forms of tracking or persistent.

Now is the time to create an easy-to-use mechanism for consumers who want to opt of online tracking if they wish to do and a legal requirement to honor their decisions, and this could be done in a way where consumers could give permission to specific trackers for specific purposes if they wished.

Our ideas about how Do Not Track would work have evolved over time. Again, this would not be a list like the Do Not Call Registry, but would instead be a setting in Web browsers that consumers could use to indicate that they don’t want to be tracked. The browsers would express the consumer’s preference to the Web sites that they visit.

I am not a technologist, but there are other experts from the Electronic Frontier Foundation and elsewhere, and we heard from the FTC that its experts concur that this mechanism would be easy to implement and simple for both consumers and trackers to use.

In our vision, all browsers would be required to include a Do Not Track mechanism as a standard feature at no extra cost to consumers, and, just as importantly, all trackers should be required to honor consumers’ preferences. Industry members would obviously have to work together, as they often do, in implementing technologies that have to be interoperable to ensure that these mechanisms work as intended.

And we think that the FTC would have to be required to perform audits and mystery browsing to ensure that trackers are indeed complying with consumers’ requests, since it is very difficult for consumers to tell themselves whether they are being tracked or how their information is being used.

Mr. SPACE. Ms. Grant, if I could ask that you wrap it up. Unfortunately, we have a lot of witnesses.

Ms. GRANT. I am sorry. That is why I am speaking so fast.

Let me just conclude by saying we have other concerns that will not necessarily be eliminated by Do Not Track. But to the extent that Do Not Track gives consumers an effective way to control the collection and use of their personal information, those concerns are

ameliorated. So we look forward to working with Congress on the creation of a Do Not Track tool for consumers.

[The prepared statement of Ms. Grant follows:]



Consumer Federation of America

1620 I Street, N.W., Suite 200 * Washington, DC 20006

Testimony of Susan Grant
Director of Consumer Protection
Consumer Federation of America
Before the House Committee on Energy and Commerce
Subcommittee on Commerce, Trade and Consumer Protection
December 2, 2010

"Do-Not-Track" Legislation: Is Now the Right Time?

On behalf of Consumer Federation of America, an association of nearly 300 nonprofit consumer organizations in the United States that was established in 1968 to advance the consumer interest through research, advocacy, and education, I am pleased to submit testimony on this important question: is now the right time for "do-not-track" legislation. The answer, simply put, is Yes.

As a recent Wall Street Journal investigative series¹ so clearly detailed, consumers are being tracked on the Internet wherever they go, whatever they do, without their knowledge and consent. Information about their online activities – what they search for, what they click on, what they purchase, what they share with others – is compiled, analyzed, and used to profile them. Sometimes information that is gathered about them offline is added to create even richer profiles. This "behavioral tracking" is primarily used for marketing purposes at this point, but it can also be used to make assumptions about people in connection with employment, housing, insurance, and financial services; for purposes of lawsuits against individuals; and for government surveillance. There are no limits to what types of information can be collected, how long it can be retained, with whom it can be shared, or how it can be used. As the Wall Street Journal characterized it in the beginning of its series, "one of the fastest-growing businesses on the Internet is the business of spying on consumers."²

If someone were following you around in the physical world – tailing you and making note of everywhere you go, what you read, what you eat, who you see, what music you listen to, what you buy, what you watch – you might find this disturbing. The argument that: "We don't know your name, just the make and model of your car, and we're only going to use this information to send ads to you," might not assuage your concerns about being stalked. On the Internet, even if the tracker doesn't know your name, you are not anonymous. As the Federal Trade Commission³ and members of Congress⁴ have

¹ Wall Street Journal, *What They Know*, series of articles from July 31-August 10, 2010, <http://online.wsj.com/public/page/what-they-know-digital-privacy.html>

² Julia Angwin, *The Web's New Gold Mine: Your Secrets*, Wall Street Journal, July 31-August 2, 2010

³ FTC Staff Report: Self Regulatory Principles for Online Behavioral Advertising, 21-25, February 2009 www.ftc.gov/os/2009/02/PO85400behavadreport.pdf

recognized, your Internet Protocol address and other unique persistent identifiers are essentially personally identifying information.

And as the Wall Street Journal put it, the skill of data handlers “is transforming the Internet into a place where people are becoming anonymous in name only.”⁵ The ability to cross-reference data makes it easy to make assumptions about people and treat them a certain way based on information that has been collected about their activities, even if you don’t know their names. Furthermore, as news reports and scholarly articles have described, it is relatively easy to re-identify data that is supposedly anonymous.⁶

With more and more people using the Internet as an essential tool for communications, education, managing their finances, researching health and other sensitive subjects, buying goods and services, sharing information through social networks, engaging in political and civic discourse, accessing government programs and benefits, and storing personal and workplace documents, it is crucial that they be able to exert effective control of the collection and use of information that is gleaned from their online activities. No matter what one thinks about the benefits and risks of online tracking – and there are many differing views on the subject – the fact is that individuals have a basic right to privacy and this right must be respected. As the United Nations stated in The Universal Declaration of Human Rights, which was adopted more than six decades ago:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interference or attacks.⁷

In many respects, our “home” is now the Internet, and much of our correspondence is now online, but our basic right to privacy remains unchanged. Congress recognized the fundamental importance of consumers’ privacy in the context of marketing when it enacted the Telephone Consumer Protection Act⁸ and the Telemarketing and Consumer Fraud and Abuse Prevention Act,⁹ which limited the times of day that telemarketing calls could be made and restricted other telemarketing practices, and gave the Federal Trade Commission the authority to promulgate rules governing telemarketing. In 2003 when the FTC amended the Telemarketing Sales Rule¹⁰ to create the national “do-not-call” registry, the agency

⁴ See discussion draft of privacy bill by Representative Rick Boucher (D-VA) and H.R. 5777 introduced by Representative Bobby Rush (D-IL), both of which define “covered information” to include any unique persistent identifiers including IP address.

⁵ Emily Steel and Julia Angwin, *On The Web’s Cutting Edge, Anonymity in Name Only*, Wall Street Journal, August 4, 2010, <http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html>

⁶ See Nate Anderson, “Anonymized” data really isn’t – and here’s why not, last updated September 8, 2009, <http://arstechnica.com/tech-policy/news/2009/09/your-secrets-live-online-in-databases-of-ruin.ars>; Arvind Naryanan and Vitaly Shmatikov, *Myths and Fallacies of “Personally Identifiable Information,”* Communications of the ACM, June 2010, Vol. 53, No. 6, http://www.cs.utexas.edu/~shmat/shmat_cacm10.pdf; Michael Barbaro and Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, New York Times, August 9, 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=2&ex=1312776000&pagewanted=all

⁷ Article 12, *The Universal Declaration of Human Rights*, December 10, 1948, <http://www.un.org/en/documents/udhr/index.shtml>

⁸ 47 U.S.C. § 227 *et seq.*

⁹ 15 U.S.C. §§6101-6108

¹⁰ 16 CFR Part 310

acknowledged that the company-specific approach, which obliged consumers to inform each company one-by-one that they did not want to receive telemarketing calls, was “seriously inadequate to protect consumers’ privacy from an abusive pattern of calls from a seller or telemarketer” and that consumers were “angered and frustrated” by the pattern of unsolicited calls they were receiving.¹¹ The FTC also said that industry self-regulatory programs such as the Direct Marketing Association’s Telephone Preference Service fell short because they were voluntary and, “to the extent that sanctions exist for non-compliance, DMA may apply those sanctions only against its members, not non-members.”¹² The national “do-not-call” registry provides consumers who do not want to receive telemarketing calls with an easy-to-use mechanism to opt-out, and just as importantly, telemarketers are legally obliged to honor their opt-out decisions. Now is the time to create an easy-to-use mechanism to enable consumers to opt-out of online tracking if they wish to do so, and a legal requirement to honor their decisions.

While online tracking is less visible to consumers than being interrupted at dinner by telemarketing calls, Americans in large numbers are clearly concerned about this practice. A 2008 poll by Consumer Reports National Research Center showed that 72 percent were concerned about their online activities being tracked and profiled by companies. Fifty-three percent were uncomfortable with Internet companies using their email content or browsing history to send them relevant ads, and 54 percent were uncomfortable with third parties collecting information about their online behavior. Ninety-three percent thought that Internet companies should always ask for permission before using personal information and 72 percent wanted the right to opt out when companies track their online behavior.¹³

A 2009 survey by researchers at the University of Pennsylvania and the University of California found that 66 percent of respondents did not want the Web sites they visit to show them ads tailored to their interest, and when the common tracking methods were explained, an even higher number rejected tailored advertising. For instance, 84 percent said No to tailored advertising if it was based on following them on *other* Web sites they had visited. More than 90 percent agree that there should be a law that requires Web sites and advertising companies to delete all stored information about an individual if the person requests them to do so, and 63 percent believe that advertisers should be required by law to immediately delete information about their Internet activities.¹⁴ More recently, a poll commissioned by the nonprofit organization Consumer Watchdog in July 2010 revealed that 90 percent of Americans wanted more laws to protect privacy, 86 percent favored the creation of an “anonymous button” that allows individuals to stop anyone from tracking their online searches or purchases, and 80 percent wanted a “do-not-track-me” list for online companies that would be administered by the FTC.

CFA and other consumer and privacy organizations first called for creating a “do-not-track” mechanism in joint comments to the Federal Trade Commission in 2007 in connection with an FTC Town Hall on “Behavioral Advertising: Tracking, Targeting, and Technology.”¹⁵ We proposed it as one of several proactive steps that the FTC should take in order to protect consumers as behavioral tracking becomes more ubiquitous.

¹¹ Federal Register Vol. 68 No. 19, January 29, 2003, p. 4631

¹² *Id*

¹³ Consumers Union news release, September 25, 2008, http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html

¹⁴ Turow et al, *Americans Reject Tailored Advertising*, http://repository.upenn.edu/asc_papers/137/

¹⁵ http://www.consumerfed.org/elements/www.consumerfed.org/file/other/FTC_sign-on_letter_Behavioral_Advertising.pdf, November 1, 2007

In 2008, in response to the FTC's proposed principles for online behavioral advertising, CFA submitted comments with Consumers Union urging stronger action, including creating a "do-not-track" mechanism.¹⁶ We argued that self-regulatory programs such as such as the National Advertising Initiative¹⁷ fail to provide consumers with an effective means of opting out of online tracking because consumers are not aware of them, there is no requirement that companies participate in them, there is no oversight or transparency, and there is no enforcement. Furthermore, we noted that the opt-out mechanisms that these voluntary programs provide to consumers, which are based on cookies, did not work for some tracking methods and fail to provide persistent protection from unwanted tracking since cookies may be deleted for a variety of reasons.

In July of 2009, a consortium of four trade associations proposed new voluntary principles¹⁸ for behavioral advertising and promised to implement a self-regulatory program in early 2010. It's late in starting, but, as a New York Times blog post pointed out, the proposal largely codified the practices that companies were already engaging in and failed to endorse ideas that "might give users more meaningful information and control over how their behavior is being tracked."¹⁹ One of those ideas is a browser-based mechanism for avoiding tracking, which I will discuss in more detail later.

The consortium's principles fall short of what we would like to see, even given the inherent limitations of voluntary initiatives, in several respects. For instance, they apply to tracking for advertising but not for other purposes. They do not apply to tracking by the Web site that the consumer is visiting if the site intends to use that information itself or to share it with its affiliates. No notice or choice is required for first party tracking and use and or for affiliate sharing. This is predicated on two false assumptions. The first is that consumers are not troubled by their activities on a Web site being tracked and used by the owner of the site for whatever internal purpose it wishes. The second is that consumers would know who the Web site's affiliates are and would have no objection to the information about their activities on the site being shared with affiliates.

Under these voluntary principles, Web sites could allow third parties to track consumers that visit them, without obtaining any consent from consumers. Those third parties would have to give notice and a "choice" mechanism, which since it does not have to be "opt-in" would undoubtedly be "opt-out."²⁰ But there are several different options for how the notice and choice could be presented to consumers and how they would exercise their choices. The principles also provide for the possibility of multiple self-regulatory programs that would manage centralized choice mechanisms for member companies that wish to use them. The principles and the systems they would put in place are complicated and confusing, and since the choice mechanisms would probably be cookie-based, they will not work with some tracking methods and they won't be persistent. Furthermore, though many companies will voluntarily sign up, not all will, and the enforcement powers of self-regulatory programs are limited to admonishing and expelling members.

¹⁶ <http://www.consumerfed.org/pdfs/CFA-CU-behavioralmarketingcomments.pdf>, April 11, 2008

¹⁷ See World Privacy Forum report, *National Advertising Initiative: Failing at Consumer Protection and at Self Regulation*, November 2007, http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.

¹⁸ www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209

¹⁹ See Saul Hansell, *Four Privacy Protections that the Online Ad Industry Left Out*, July 6, 2009, <http://bits.blogs.nytimes.com/2009/07/06/four-privacy-protections-the-ad-industry-left-out/?pagemode=print>

²⁰ Only Internet Service Providers and others that collect all or nearly all of consumers' Web traffic would be required to obtain opt-ins; opt-ins are also required under this self-regulatory program for collection and use of "sensitive" information, but that is too narrowly defined to offer adequate privacy protection.

In September 2009 CFA and several other consumer and privacy groups released a Legislative Primer for Online Behavioral Tracking and Targeting,²¹ which outlines the key elements that we believe are necessary to protect consumers. Once more, we called for a “do-not-track” mechanism. We are pleased that now this idea is finally starting to get the careful consideration that it deserves.

Our thinking about what this mechanism would be and how it would work has evolved over time. It would not operate in the same way that the national “do-not-call” registry does – there would be no need for consumers to provide their IP addresses or other personal information to a database, and therefore no cause for concern about the security of that information. It would not operate using cookies, one reason why the NAI approach has been a failure, since cookies are not always persistent and do not work with some tracking methods.

As we envision it, the “do-not-track” mechanism would be a setting in Web browsers that consumers could use to indicate that they do not wish to be tracked. The browsers would express the consumers’ preferences to the Web sites they visit. I am not a technologist but am fortunate to have colleagues in organizations such as the Electronic Frontier Foundation who explain that this mechanism would be simple for both consumers and trackers to use. It is easy to implement as an add-on; it is already being used as an add-on to the Mozilla Firefox browser,²² and it would be easy to implement for Web services. As consumers whose numbers are on the national “do-not-call” registry can opt-in to receiving calls from telemarketers on a company-by-company basis, so could consumers give permission for tracking by certain entities, in this case through their browser settings.²³

The FTC would not dictate the design of the technology but would set the overall goals that it should accomplish: providing consumers with a simple, easy-to-use mechanism that effectively and persistently enables them to exert control over online tracking. All browsers would be required to include a “do-not-track” mechanism as a standard feature, at no extra cost to consumers. And just as important, all trackers would be required to honor the consumers’ preferences.

Industry members would need to work together, as they often do in implementing technologies that must be interoperable, to ensure that these mechanisms work as intended. The FTC should be required to perform audits and “mystery browsing” to ensure that trackers are indeed complying with consumers’ requests, since it is very difficult for consumers themselves to know if their information is being tracked and how it is being used.

We have heard dire predictions that “do-not-track” will destroy the Internet and kill jobs. We heard the same predictions about the national “do-not-call” registry but, as an Associated Press article noted a year after it was launched, the sky did not fall and telemarketing survived.²⁴ Obviously, not all consumers will use a “do-not-track” mechanism, and some may decide to allow tracking by specific

²¹ <http://www.consumerfed.org/elements/www.consumerfed.org/file/OnlinePrivacyLegPrimerSEPT09.pdf>, September 1, 2009

²² See Christopher Soghoian & Sid Stamm, *Universal Behavioral Advertising Opt-out*, <https://addons.mozilla.org/en-US/firefox/addon/12765>.

²³ See Arvind Narayanan, “Do Not Track” Explained, September 20, 2010, <http://33bits.org/2010/09/20/do-not-track-explained/> and <http://donottrack.us/>, a website created by Mr. Narayanan, Jonathan Mayer and other researchers that provides information about how this “do-not-track” concept would work.

²⁴ *Telemarketing Firms Surviving “Do Not Call,”* LA Times, October 18, 2004, <http://articles.latimes.com/2004/oct/18/business/fi-telemarketers18>

entities but not others. Other means of advertising, such as contextual advertising, where ads are served based on what the consumer is looking at on a site at that time, will be unaffected. It is also important to note that serving ads to consumers is only one way that they find products and services they want online. They use search engines, Web sites that provide comparative information about products and services, recommendations from people they know, online auction sites, and other means to find what they need on the Internet. It would be a sorry state of affairs if the only way that ecommerce could survive is by spying on consumers to guess what they want.

We have other concerns about online tracking that will not be eliminated by creating a “do-not-track” mechanism. For example, we believe that there are some types of sensitive information, such as that related to health conditions or sexual preference that should not be tracked at all. We also believe that some uses of behavioral profiles created by tracking, such as for employment, insurance, housing or financial services, should not be allowed. First, the assumptions made about consumers based on their Web activities are not necessarily accurate. This may not matter much, at least to consumers, if it results in advertisements for pickup trucks being sent to people who would prefer sedans. But if these profiles are used to make inaccurate assumptions about people for purposes of credit, employment or insurance, it does matter.²⁵ Second, it is inherently unfair to follow consumers around the Internet to make decisions about them based on activities that may be totally unrelated to the job, product or service in question.

I may be searching online for information about cancer or HIV because a friend or relative is ill; I certainly would not want my insurance company to know about my searches or to make any determinations about me on the assumption that I have that condition. And I don’t think that anyone here would be comfortable with creditors using who your friends are in social networking sites and what you chat about as a factor for determining what kind of credit offer to make to you.²⁶ This is already happening, and Congress should act to stop it.

We also believe that there must be limits to the length of time that this data can be maintained, that consumers should have the right to see, correct and delete such data, and that access by the government or others for purposes beyond advertising should be limited.

Creating a “do-not-track” mechanism, while not a substitute for comprehensive privacy protection, could nonetheless help ameliorate these concerns. To the extent that consumers have real, effective control over information about their online activities, they can prevent that information from being collected and used in ways that they may find objectionable.

Thank you for holding this hearing to explore the need for a “do-not-track” mechanism. I hope that this will lead to legislation in the near future. We will be happy to provide any additional information that may be needed and to support “do-not-track” legislation.

²⁵ See Emily Steel and Julia Angwin, *On The Web’s Cutting Edge, Anonymity in Name Only*, Wall Street Journal, August 4, 2010, <http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html>, for a description of how online behavioral tracking is used to make assumptions about consumers to serve different credit card offers to them.

²⁶ See *Social networking: Your key to easy credit?* Erica Sandberg, <http://www.creditcards.com/credit-card-news/social-networking-social-graphs-credit-1282.php>.

Mr. SPACE. Thank you, Ms. Grant.

Our next witness, Mr. Joseph Pasqua, vice president of research, Symantec Corporation.

STATEMENT OF JOSEPH PASQUA

Mr. PASQUA. Mr. Chairman, Ranking Member Whitfield and members of the subcommittee, thank you for the opportunity to be here today as you consider a National Do Not Track proposal in an effort to protect consumer online privacy.

As the global information security leader, Symantec supports Congress's goal to protect privacy and to enhance consumer trust online. Today, I would like the committee to take away three key points from my testimony.

First, online privacy is not possible without security. Through spyware and certain harmful adware, online advertising can and increasingly does present a critical threat to security and therefore privacy on the Internet.

Second, while privacy legislation can help protect Americans in the online world, we urge the committee to focus on regulating malicious behavior rather than underlying technologies. Privacy laws should avoid the trap of defining good or bad technology in order to avoid undermining both innovation and security.

Third, while online privacy and security together are a critical foundation to trust on the Internet, the creation of a Do Not Track registry would be unlikely to advance these goals. Instead, Congress should focus on policies that foster an online environment where individuals and organizations can complete transactions with confidence, trusting each other's identities and the infrastructure on which the transactions run.

Symantec believes that online privacy is a cornerstone of consumer trust. And let me just say that Do Not Track, and that mechanism is only one piece, as an earlier witness said, of the overall privacy question online.

Without security, however, the expense of compliance and lost economic activity from individual privacy regulations may not be worth it. We urge Congress to deal with security first and not to inadvertently create impediments to security through new privacy laws or new safeguards which will amount to closing the barn door after the horses have left.

The advantages of doing business over the Internet are tremendous, but only if exchanging information in cyberspace is secure. Interaction with Web sites increasing demands personal information, yet sharing such data requires trusting business partners and the integrity of transaction records online so individuals do not become victims of identity theft or fraud.

The increased prevalence and complexity of online advertising make it a ripe target for attackers. Because an advertisement is basically a piece of software, the potential exists for that software to be malicious. Online behavioral advertising is not inherently bad, but it does carry with it, sometimes literally, collateral threats to information security.

A whole class of threats, commonly known as spyware or malicious adware has proliferated over the last few years. Fortunately, the marketplace is responding to the need to address these chal-

lenges. Cyber security companies are investing heavily until newer generations of behavioral detection and white-listing technologies to handle the increasing volume and variety of spyware and malicious code threats.

For our part, Symantec creates security programs that watch out for the most current malicious threats, as well as unknown software that exhibits suspicious behavior. The committee may find it of interest that given the millions of threats that Symantec products block every day, the detection most frequently encountered by our Norton antivirus users is a tracking cookie over everything else. And while many types of cookies serve a useful purpose and are used on most Web sites, tracking cookies are a privacy concern.

Given the prevalence malware, including harmful adware and spyware, it is no surprise that there has been so much discussion about preventing advertising networks from being able to track the Web sites that consumers are visiting and other information about those consumers.

The proposed Do Not Track list conceptually seems to be reasonable but, in practice, would be an extremely difficult technical task. In order to abide by an instruction not to track, a Web site must have a way to recognize that a given user connecting to that site has requested that they not be tracked. Because it is analogous to using phone numbers to identify a Do Not Call list, consideration has been given to using IP addresses to recognize a connecting user.

This approach is problematic. As has been discussed earlier, IP addresses aren't really analogous to phone numbers. They change. Tracking them introduces their own security concerns.

There is another concept, but basically a reverse, which would be a Do Not Track registry, which has also been discussed, and it implies advertisers would register their domains in a Do Not Track registry and browser plug-ins would enforce that.

Symantec believes that that scenario could cause disruption to the user experience, significant disruption, and could influence the habits and fluidity of users' experience on the Internet.

We have also heard today and in previous testimony about a proposed solution where a header, header information, is sent from the browser, from the user's computer, to the Internet, expressing the user's privacy preferences. That is a reasonable approach, but we would also like to indicate that the browser alone is not enough to support that. You have to have enforcement on the server side, and that can make things difficult.

In summary, I would like to just point out one other thing. We have been talking a lot about browsers and consumers today using Web sites, but that is just one form of tracking. In the coming years, everything is going to be connected to the Internet. Your DVR is connected to the Internet. Your dishwasher is going to be connected to the Internet. Certainly your mobile phone. Advertisers would, in theory, be able to know how many loads of laundry you are doing a day.

So we need to think about tracking and privacy in a broader scope than just browsers, though they are an important first step.

[The prepared statement of Mr. Pasqua follows:]



Prepared Testimony and
Statement for the Record of

Joseph Pasqua
Vice President of Research
Symantec Corporation

Hearing on

"'Do-Not-Track' Legislation: Is Now the Right Time?"

Before the

U.S. House of Representatives
Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection

December 2, 2010
2123 Rayburn House Office Building

Introduction

Chairman Rush, Ranking Member Whitfield, and Members of the Subcommittee, thank you for the opportunity to appear before you today as the Committee considers a national "Do-Not-Track" Registry as part of an overall effort to protect consumers' online privacy.

My name is Joe Pasqua and I am the Vice President of Research for Symantec Corporation¹. I am responsible for all activities within Symantec Research Labs², the company's global research organization.

Symantec welcomes the opportunity to provide our insights to the Committee as Congress, the Federal Trade Commission, the Department of Commerce and others begin to explore the merits of new privacy initiatives and legislation designed to provide consumers with greater protection, transparency and control of their information in the online world.

Symantec supports Congress's objective of protecting privacy and enhancing consumer trust. As the global information security leader, Symantec has over 25 years of experience in developing Internet security technology. Our Symantec and Norton brands protect more than 370 million computers or email accounts worldwide. We specialize in protecting our customers' computers, networks, information and interactions as they work and play online. No one knows more about how to protect users, their families and their information than Symantec. In short, we protect more people from more online threats than anyone in the world.

Today, I would like the Committee to take away at least three key points:

First, online privacy is not possible without security. Through spyware and certain harmful adware, online advertising can present a critical threat to security, and therefore privacy on the Internet.

Second, while privacy legislation can and should help protect Americans in the online world, we urge the Committee to focus on malicious behavior rather than allegedly malicious tools such as devices or software. We want to work with you to ensure that privacy legislation targets reprehensible behavior and avoids the trap of defining "good" or "bad" technology – an exercise that could have the unintended consequence of undermining cybersecurity or stifling economic activity.

Third, while online privacy and security together are a critical foundation to trust on the Internet, the creation of a Do-Not-Track registry would be unlikely to advance these goals. Instead, Congress should focus on policies that foster an online environment where individuals and organizations can complete transactions with confidence, trusting each other's identities and the infrastructure on which the transactions run.

¹ Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

² Symantec Research Labs (SRL) is Symantec's global research organization and has played a leading role in developing and commercializing numerous cutting-edge technologies across Symantec's business areas. Commercialized technologies from the group include industry leading rootkit protection, innovative browser protection technology to proactively block future exploits of known vulnerabilities, Symantec's first antispam technology, generic exploit blocking technology that proactively blocks fast-spreading threats, online consumer security services, and technology to help protect our nation's critical power-grid infrastructure. SRL also partners with outside organizations on joint projects, through its university and government research efforts.

No Privacy Without Security

As the world's largest internet security provider, we agree that online privacy is a cornerstone of consumer trust. Without security, however, the expense of compliance and lost economic activity from additional privacy regulations is hardly worth it. The lesson: deal with security first, and do not create impediments to security inadvertently through new privacy laws.

The advantages of doing business over the Internet are tremendous—but only if enterprises can ensure that exchanging information in cyberspace is secure. Interaction with Web sites increasingly demands personal information. Ordering products online requires personal shipping addresses and credit card information. Sharing data requires trusting business partners across open network architectures and relying on unknown data security infrastructures to complete transactions. When data and documents are transferred across poorly controlled networks and repositories of personal data are accumulated in hidden databases, the potential for corrupted information or compromised personal privacy increases. The integrity of business transaction records may become questionable, and individuals may become victims of identity theft or other fraud.

Clearly, security and privacy have become major issues for the Internet's personal and business users. The communications speed and document-management advantages of Internet use are tremendous, but these conveniences are diminished when users must proceed cautiously because of a lack of confidence in the robustness of security or real concerns about misuse of Internet-based information. Without security, additional privacy regulations will be ineffective in protecting individuals' ability to control their own information and will result in expensive formalities and lost economic activity.

The Evolving Online Advertising Business And Associated Threats

Online behavioral advertising is not inherently bad, but it does carry with it – sometimes literally – collateral threats to information security. Consider some of the overall trends related to Web advertising. First, the Web has exploded in popularity, and people are spending more and more time each day surfing their favorite sites. Second, online advertising has proven itself to be a viable business model for many companies. Countless Web sites are displaying more ads that are viewed by an ever greater number of people. Third, the online advertising supply chain is fairly complex. In the simplest incarnation, an advertiser might work with an ad network that will in turn arrange to have the ad published through one or more content publishers. In a more complex, but still quite common incarnation, an ad network might work with a syndicator and many sub-syndicators. Fourth, advertising itself has become very rich in content and applications. While text-based advertisements are still popular, we are seeing more elaborate ads that use technologies, such as Flash. The reality is that an online advertisement is more than just an ad – it is a small piece of software that runs on your machine in the context of your Web browser. And finally, browsers are becoming far more complex. In addition to the core Web browser, people often enhance their Web experience through one or more plug-ins. For example, Flash is enabled on a Web browser through a plug-in.

The increase in prevalence combined with the heightened complexity makes online advertising a ripe target for attackers. Because an advertisement is basically a piece of software, the potential exists for that software to be malicious. Symantec observed such a vulnerability in a popular social networking site in which one of the site's advertisements took advantage of a well known Windows vulnerability. More than one million people saw the advertisement. Although the vulnerability was known, and although a patch had been issued, it is likely that many people who viewed the ad did not have their patches up to date.

In such cases, a Web site that hosts advertising can be an otherwise innocent bystander; the advertisement content itself is provided by an ad network, not the host. What makes attacks leveraging online advertising especially powerful is that it is entirely possible for an otherwise trustworthy, popular, and well-meaning site to host an advertisement containing malicious code.

Also, the tools of the trade are fungible. Anything one can do in a scripting language like JavaScript can also be done in Flash. So, in principle, Flash-based advertisements can implement the same kinds of attacks that are possible through malicious JavaScript. These include scanning internal network hosts and “drive-by pharming.” Cutting through the technical jargon, all of this means that an attack can be perpetrated with whatever tool, or advertising software, is available. The tool is neutral, the attacker is not.

Symantec expects the number of malicious online ads to grow. The unfortunate moral here is that there are no real safe locations on the Internet. That should not deter consumers from surfing the Web; but they must realize how important it is to be protected.

The Use Of Adware And Spyware

A whole class of threats commonly known as adware and spyware has proliferated over the last few years with very few impediments. These programs are security risks that typically are used to gather marketing information or display advertisements in order to generate revenue. Not only are these threats far more widespread than traditional malware, but also they use more advanced techniques. No doubt this is because adware and spyware programs are being created by registered corporations with professional developers rather than by hobbyist virus writers.

Spyware and adware programs are related, and in some cases their functionalities may overlap; additionally, they may have similar functionality to viruses and worms, such as displaying text or gathering information. However, one important difference from viruses and worms is that they lack the property of self-replication.

There are also key differences between spyware and adware. For example, while they both may collect information about you or your activities, the types of information they collect tends to differ. Spyware programs may log your keystrokes, capture your email and instant messaging traffic, or harvest your sensitive personal information such as passwords and login IDs, or credit card details. The compromised data is then sent on to someone else. Depending upon their intention, they may use the information however they wish; for example, accessing and controlling your system remotely, or running up charges using your credit card information. Identity theft can also be facilitated by spyware.

Spyware can be introduced into your computer system from any number of vectors; essentially, any source of executable code can become a vector for spyware transmission. However, some routes are more common than others. For example, consumers frequently download spyware without knowing it – typically attached to shareware or freeware, when they click on links in email messages or instant messaging clients, or even when they accept the conditions of fake anti-spyware software licensing agreements. In some cases, simply visiting a Web site can result in an automatic install of unwanted software. This technique is known as “drive-by downloading.”

Adware, on the other hand, generally consists of components that work together to collect a different sort of personal information: the sites you visit, your browsing habits, and your apparent likes and dislikes. Adware then sends this data on to companies that have purchased the services of the adware provider to assist in

compilation of information on your personal preferences. This data can then be used to send tailor-made advertisements applicable to your interests. This data is typically not personally identifiable. It is also important to note that not all adware tracks behavior, but some simply displays advertisements to the end user through the program. While the risk posed by such applications is low, they can constitute a violation of organizational policy or introduce risk to the host system.

As with spyware, adware can be downloaded via the Web or by clicking on links in email messages or instant messaging clients. It is sometimes bundled with other software, and you may or may not be notified of its introduction onto your system. It is not uncommon for computers to have more than one type of spyware or adware installed; additionally, use of peer-to-peer file-sharing programs increases the risk of acquiring these programs. Finally, some adware and spyware adds a BHO (Browser Helper Object) to your system. A BHO is an add-on program that can add features to your browser. Loaded every time a browser is launched, a BHO can be used by adware and spyware for its own purposes.

Some programs classified as adware or spyware are commercially released programs that can be used in a variety of ways. In and of themselves, they are not malicious, but they can threaten your privacy or security, and the availability of your system. Because of these risks, some users may wish to be able to detect these programs. Thus, Symantec classifies programs based on a number of characteristics, including their potential impact on privacy, confidentiality, integrity, and system availability. Once categorized, they can be detected by Symantec's security products, and users can choose whether to keep or remove them based on their corporate or personal requirements.

How Prevalent Is The Problem Of Spyware And Harmful Adware?

How many spyware and adware programs are actually out there? How likely is it that these programs will impact your system? It is difficult to know exactly how much spyware and adware exists at any given time because the number is highly dynamic. However, various ways can be used to determine the programs that appear to be most prevalent and to assess the potential impact on users. Symantec publishes an annual Internet Security Threat Report³, which is a comprehensive compilation of Internet threat data and provides a unique perspective on the prevalence of spyware. The Report includes an analysis of network-based attacks, a review of known vulnerabilities, and highlights of malicious code and other security risks. According to our most recent Report, spyware and adware continue to be a serious security risk for consumers.

The latest Report reveals that attackers have adopted stealth tactics that prey on end users on individual computers via "staged downloaders." These machines install malicious code onto a compromised computer and allow attackers to alter the downloadable component to any type of threat to suit their changing objectives over time. Setting aside the most common type of attack for a moment, the second most prevalent downloader component observed by Symantec in 2009 was the Sality.AE virus. Once installed, Sality.AE attempts to contact certain IP addresses to download and install its secondary components. One of the files it attempts to install is an adware program that periodically displays pop-up advertisements. If clicked, these ads generate income for the malicious code author and possibly the adware developer.

³ Symantec's Internet Security Threat Report, Volume XV, April 2010. The Symantec Internet Security Threat Report provides an annual overview and detailed analysis of Internet threat activity, malicious code, and known vulnerabilities. The report also discusses trends in phishing, spam and observed activities on underground economy servers.

The Wimad Trojan¹⁴⁷ was the third most common staged downloader component in 2009. This Trojan arrives on computers as a license-protected multimedia file. When the file is opened, Wimad exploits the intended functionality of digital rights management (DRM) technology in order to open a window and access an attacker-controlled URL. When an attacker's Web page is processed, a deceptive message is displayed that asks the user to click a button. If clicked, the Trojan downloads other threats, including adware and spyware.

As an illustration of the scale of the problem, a report by the Organisation for Economic Co-operation and Development⁴, estimates that 59 million users in the U.S. have spyware or other types of malware on their computers.

Tracking Cookies Are Cause for Privacy Concern

Given the millions of threats that Symantec products block every day, you might find it interesting to know which detection consistently holds the top spot. It is not a worm such as W32.Stuxnet, a virus like W32.Virut, or even one of our long-term generic detections, such as Backdoor.Trojan. The detection most frequently encountered by Symantec antivirus users is tracking cookies.

Tracking cookies do what they say on the tin: they track your browsing habits. And while many types of cookies serve a useful purpose, and are used on most websites, tracking cookies can be considered a privacy concern. Some media companies that use them have found a way to resurrect deleted tracking cookies by using other cookies that are stored within Flash applications. These "Zombie cookies" can be detected by Symantec antivirus system scans, just as regular tracking cookies are, and can be removed from users' computers.

Social Engineering Banner Ads

The first challenge for adware and spyware vendors is to get people to install their software. Virus writers face exactly the same challenge and solve it by using social engineering techniques to entice users into running their creation. They use email messages with message bodies such as 'check out this message' and then attach their virus rather than legitimate content. Not surprisingly, similar techniques are used by adware and spyware vendors. Many websites use banner ad services. Unfortunately, many banner ads are completely misleading. Some banner ads use an image that mimics a Windows message box with an urgent message tricking computer users into clicking on the fake message box, then redirects the user to sites that initiate the installation of adware or spyware. Some of these fake message boxes will state the user's computer is infected or cite another system problem. When clicking the fake message box, the user is redirected to install software to correct the problem, when in fact the user was not infected.

Ban Bad Behavior, Not Technology

Fortunately, the marketplace is responding to the need to address the challenges of adware and spyware. Cyber security companies are investing heavily in newer generations of classification, behavioral detection and white listing technologies to handle the increasing volume and variety of spyware and malicious code threats. For our part, Symantec creates security programs that watch out for known malicious threats, as well as unknown

⁴ The Organisation for Economic Co-operation and Development (OECD), "*Malicious Software (Malware): A Security Threat to the Internet Economy*," June, 17, 2008.

software that exhibits suspicious characteristics. Symantec products classify and categorize programs according to functionality. This allows a user to select an acceptable risk level and detect only programs that fall outside the user's own acceptable limits. We continually add new definitions and new defenses to address the ever evolving dangers in the Internet threat landscape such as worms, spyware, spam, and phishing.

In addition, critical technologies such as web browsers are being revamped with more security as they increasingly become a focus for attacks. Web browser security is particularly important because browsers come in contact with more un-trusted or potentially hostile content than most other applications.

Symantec has delivered a number of highly innovative new security technologies introduced in Norton Internet Security and Norton Anti-Virus 2010. Our new reputation-based security, named Quorum, leverages the wisdom of Norton's tens of millions of participating customers to derive highly accurate security ratings for virtually every file available on the Internet. This empowers Symantec users to make far better choices about the software they download and install on their computers. In addition, we introduced a new generation of heuristics to detect unknown malware files before they can run and cause damage. This advanced approach detects new malware, spyware and adware strains without known fingerprints, searching files for suspicious sequences of instructions typically used by malicious software. Finally, Symantec completely redesigned the behavioral protection, enabling it to recognize and block thousands of new malware variants by analyzing the behaviors of running software, all without known fingerprints.

We believe, however, that in addition to the response of the marketplace, legislation can and should play a role in protecting privacy online. We believe that legislation should not prohibit specific technologies -- computers, software and the Internet are tools that are used in thousands of ways to enhance how we work, study, communicate and live. The fact that a number of bad actors have figured out how to use these tools for illegitimate purposes does not mean that the tools themselves are the cause of the harm. If technology was to be constrained or regulated, we would lose much of the richness and power that computing has brought to our modern lives. Let me put it a different way: we do not ban crowbars because some people use them to break into houses. We do not ban cars because some people use them to flee from the scene of a crime. Prohibiting conduct, rather than technology, avoids the danger of dictating the design and operation of computer software and hardware. Congress has wisely avoided imposing technology mandates and the U.S. technology industry remains the envy of the world.

A "Do-Not-Track" List

Organizations including consumer, privacy, and technology groups have proposed the development of a "Do-Not-Track" list in hopes of providing consumers the ability to prevent advertising networks from being able to track the websites consumers are visiting. The proposed "Do-Not-Track" list is modeled in large part on the idea of the "Do Not Call" list that the Federal Trade Commission implemented in 2003 with significant success.

Conceptually, the idea seems reasonable, but in practice it would be an extremely difficult, if not unrealistic technical task.

In order to abide by an instruction not to track, a Web site must have a way to recognize that a given user connecting to that site has requested that they not be tracked. This recognition could be accomplished by identifying the user such that the user's registered tracking preference can be retrieved from a do-not-track list (e.g., a database). Because it is analogous to using phone numbers to identify a do not call list, consideration has been given to using IP addresses to recognize a connecting user. However, this approach is quite

problematic, as it requires that a user register all of the IP addresses from which they may connect. Given that users have an ever increasing array of Internet connected devices such as desktops, laptops, smartphones, tablets, gaming consoles, DVD players, TVs, etc. whose IP addresses can change often, this is a very tedious and inaccurate way to implement this feature. In addition, it is common practice for many devices to connect to the Internet through a home, business, or publicly available router. For all devices attached to such a router, the router often presents to external sites a single shared IP address using what is called Network Address Translation, or NAT. A mobile device may connect to multiple routers over the course of a single day – the home router, the coffee shop router, the work router, and back to the home router, for example. Each time a device connects to a router, it is common practice to get a new dynamically assigned IP (Dynamic Host Configuration Protocol) address internal to the router, and each router has its own unique externally presented IP address (which is what a visited web site would see).

Further complicating this approach is the transition from IPv4 to IPv6 addresses – simply speaking, there are two types of IP addresses to consider, both types are in use, and thus all sites would need to support both types. This approach is therefore extremely difficult for both users to use and for sites to implement. Essentially, all participating users would have to register all IP addresses used by all devices they connect from. In addition, they would need to update the registration every time the IP addresses change. Another affect would be that sites must check for and support both IPv4 and IPv6 type addresses, causing both users and sites to contend with network address translation (NAT). Most users do not know what their IP addresses are, how to find out what they are, how to know if they have changed, and whether or not they are subject to network address translation (which causes multiple devices to share a single IP address).

A “Do-Not-Track” Registry

A concept similar to the Do Not Track list, but basically a reverse version, would be a Do-Not-Track *Registry*. We can speculate about a “Do-Not-Track” Registry approach based on comments in a letter⁵ submitted to the Federal Trade Commission in 2007 by various consumer groups when this proposal was first envisioned. That letter outlined how such a proposal would work and included the following:

“Companies providing web, video, and other forms of browser applications should provide functionality (i.e., a browser feature, plug-in, or extension) that allows users to import or otherwise use the “do not track” list of domain names, keep the list up-to-date, and block domains on the list from tracking their internet activity.”

The Do-Not-Track Registry implies advertisers would register their domains with the Federal Trade Commission. Users would install a browser plug-in and configure the plug-in by selecting what advertising domains to block. This solution requires -regulation in terms of advertisers registering the domains, and plug-in developers implementing the proper blocking mechanisms. The potential user experience disruption would be significant, and the obligation would be placed on the user to configure each device used in order to properly block tracking. Again, looking at the future of Internet browsing habits and the fluidity of how a user may transition

⁵ Letter submitted to Donald S. Clark, Secretary of the U.S. Federal Trade Commission in advance of the FTC Town Hall, “Ehavioral Advertising: Tracking, Targeting, and Technology,” held November 1-2, 2007 in Washington, D.C. by Ari Schwartz, Deputy Director, Center for Democracy and Technology; Linda Sherry, Director, National Priorities Consumer Action; Mark Cooper, Director of Research, Consumer Federation of America; Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation; Deborah Pierce, Executive Director, Privacy Activism; Daniel Brandt, President, Public Information Research; Robert Ellis Smith, Publisher, Privacy Journal; Beth Givens, Director, Privacy Rights Clearinghouse; and Pam Dixon, Executive Director, World Privacy Forum.

from one device to another throughout the day, this solution forces the user to configure each device used to browse the Internet in what is likely an unrealistic way. Additional hurdles are in play when shared computers are used. For example, how would a Do-Not-Track Registry work in a library or hotel business center, where each user may have different tracking preferences?

The Browser Header Attribute “x-notrack”

One solution described by researchers looks at an HTTP header attribute sent by the browser to tracking servers describing the user’s preference in tracking. The user would configure the browser at first launch defining the tracking preferences for the session. The setting would set the “x-notrack” attribute in the browser header. Actions by the browser alone, however, are not sufficient to protect the user. There is also a need to involve a server component in the solution. Here the advertising servers feeding advertisements would need to honor the browser header attribute for no tracking. Federal Trade Commission regulation in this case would not allow advertisers to set any persistent tracking cookies on the user system.

At first glance, this solution seems simple enough; but after working through implementation scenarios, we would likely begin to see a bifurcation of internet activity. A user with the no-track option enabled may be fed Web sites with limited content, while other users without the option set would see a richer web page and have a more robust browsing experience. A user may choose to allow first-party tracking in exchange for a more feature rich experience, for example, while preventing tracking from third party sites. By looking at configuration silos (first party tracking vs. third party tracking), we quickly move into the conflicts between End User License Agreements (EULAs) and Do-Not-Track/No-Track options.

The focus thus far has been on browser tracking habits, but are we limiting the tracking activities to only advertisers or are we addressing any and all tracking done on a device? With many day-to-day computer applications, when a user decides to use an application, the user accepts the EULA in order to complete installation. If the product tracks certain user activities, as is often the case, does the EULA now trump the Do-Not-Track option?

The real crux is this: How far would a “do-not-track” concept go? Is it limited to advertising and Web sites, or does it extend to ANY type of tracking? What about tracking in order to enforce licensing restrictions (is this software being used by the person it is licensed to, and only that person)? Is it okay to track usage patterns anonymously so that we can improve the usability of our product? Is it okay for us to identify a particular computer or user, but only anonymously so that we can implement our reputation security system as long as the tracked information cannot be tracked back to a specific user? It is not just what can be tracked “on a device”, but in combination between the device and observable attributes from the server side.

Until we can see a formal proposal by the Federal Trade Commission, it is difficult to access the merits and the technical specifications of a Do-Not-Track proposal. Details are also sparse about how a Do-Not-Track mechanism might actually be implemented. What is clear, though, is that there are a variety of possible technical and regulatory approaches to the problem, each with its own difficulties and limitations – many of which could potentially unintentionally impact cyber security.

We believe that consumers should have the right to visit or not visit a website as they see fit. Consumers already have protections, some provided directly from advertising organizations, as well as browser based

security protections, and anti-virus options to keep cookies, software, and other unwanted materials off of their systems.

Right now, implementing the same framework as used for the Do Not Call registry does not appear to be the best solution for today's online world. The comparison is still useful though, if only to caution against the assumption that Do-Not-Track will be as easy, or as successful, as Do Not Call. The differences between the problems at hand and the technologies involved are substantial. As mentioned earlier, the focus should not be in limiting technology and user experiences online but focused on the malicious behaviors that impact user safety and security while transacting online.

We are unsure exactly how a Do-Not-Track mechanism would be all that different from the opt-out link currently offered by the Network Advertising Initiative (NAI). Perhaps the most significant difference might be that the NAI includes only a limited number of companies, but a Do-Not-Track registry would presumably be universal. Given the technical challenges of a Do-Not-Track registry, we would instead recommend that Congress, the Federal Trade Commission, the Department of Commerce and private sector stakeholders participate in an effort to develop a voluntary but enforceable code of conduct. Companies that adhere to those voluntary principles could be given incentives to comply such as safe harbor protection.

Our approach to preventing and tracing cyber attacks includes improving identification and authentication of those who seek access to the system that must be protected. Our vision is for a future where individuals can voluntarily choose to obtain a secure, interoperable, and privacy-enhancing credential such as a smart identity card or a digital certificate on a cell phone, from a variety of public and private service providers, to authenticate themselves online for different types of transactions.

Symantec also supports efforts similar to those being pursued by the White House with the development of the "National Strategy for Trusted Identities in Cyberspace" (NSTIC), which seeks an online environment where individuals and organizations can complete online transactions with confidence, trusting each other's identities and the infrastructure upon which the transaction runs.

One of the challenges of a Do-Not-Track concept is that privacy, while not entirely arbitrary, is highly malleable and sensitive to non-normative factors. Understanding the value that individuals assign to the protection of their personal data is of great importance to policy makers, businesses, and researchers. What one user considers excessive tracking might be completely reasonable to others. A consumer may prefer that a trusted site tracks their online interactions, as this may result in a richer user experience and in more relevant messaging; but that same consumer may not want to be tracked by certain other sites or vendors.

Individual privacy preferences make a Do-Not-Track mechanism—or any other one size fits all approach—a rather awkward fit no matter how implemented. Users need simplicity, but it is doubtful that simple controls can adequately capture the nuances of individual privacy preferences.

Conclusion

The actions of many adware and spyware programs go beyond simply facilitating advertisements or gathering aggregate non-personally-identifiable data. Many adware and spyware programs use techniques akin to malicious threats from social engineering to exploit vulnerabilities. Once installed on the system, they use techniques to hide themselves and prevent their removal. In addition, many adware and spyware programs

gather personally-identifiable and confidential data and are able to correlate that data continually to build marketing profiles.

Overall user attitudes toward privacy, performance, ease of removal, and newly introduced spyware or adware program's characteristics will determine how they want their security product to deal with each individual situation. User expectations of computer virus protections have traditionally been for the product to assess functionality and risk, and then to make globally appropriate decisions on disinfection or removal of the viral threat. As the landscape has grown and evolved, however, a more user-centric approach is required. Thus, a useful approach is to detect all of these risks in a way that is non-intrusive, then to allow the user to make informed decisions based upon their own level of accepted risk.

Fortunately, the marketplace is responding to the need to address this challenge. Cyber security companies are investing heavily in newer generations of classification, behavioral detection and white listing technologies to handle the increasing volume and variety of spyware and malicious code threats.

The government should encourage private sector stakeholders to participate in an effort to develop a voluntary but enforceable code of conduct. Companies that adhere to those voluntary principles should be given incentives to comply such as safe harbor protection.

One safe harbor that Congress should consider including is a "Good Samaritan" provision for developers of anti-spyware solutions which are providing effective protection to computer users against online threats. Unfortunately, developers often are threatened with lawsuits for defamation and interference with their business by purveyors of spyware and harmful adware. These spurious threats force anti-spyware companies to divert resources to fight to protect themselves in court. This is intended to disrupt and deter the development of tools that empower consumers to stop unwanted software from being put on their computers.

Right now, applying the Do Not Call framework to the Internet does not appear to be the best solution for today's online world. The problems at hand and the technologies involved are substantial. One of the challenges of a Do-Not-Track concept is that privacy, while not entirely arbitrary, is highly malleable and sensitive to non-normative factors. Individual privacy preferences are arbitrary and would make a one-size-fits-all Do-Not-Track mechanism an impossible standard to establish.

Congress should instead focus on creating privacy policies which help foster an online trusted environment where individuals and organizations can complete online transactions with confidence, trusting each other's identities and the infrastructure that the transaction runs on.

Thank you for the opportunity to testify before the Committee today on the issues of privacy, online advertising and the concept of a Do-Not-Track registry. Symantec looks forward to continuing to work with Congress as these important issues move forward.

Mr. SPACE. Thank you, Mr. Pasqua.

Our next panelist is Ms. Joan Gillman, executive vice president and president of Media Sales, Time Warner Cable.

STATEMENT OF JOAN GILLMAN

Ms. GILLMAN. Thank you, Mr. Chairman, Ranking Member Whitfield, and other members of the subcommittee. I appreciate the opportunity to appear before you today to discuss consumer privacy, including the potential for Do Not Track legislation.

For Time Warner Cable, our relationship with our customers is the bedrock foundation of our business. We operate in a highly competitive marketplace, and our ability to succeed depends on winning and retaining the trust of our customers. It is our job to preserve and strengthen that trust while delivering content and services to meet consumer needs as well as introduce the benefits of innovative network technologies and capabilities.

I will make two points today. First, Do Not Track proposals cannot be considered in a vacuum but, rather, must be part of a larger conversation about the appropriate role of government in ensuring consumer privacy as more content, products and services move online.

Second, we believe it would be premature to require Do Not Track through legislation or regulation, given the still conceptual nature of such a requirement.

I will address each of these in turn.

Advertising has emerged as a key driver of an incredible array of online content services and applications available to users at little or no cost. The more effective the advertising, the greater the advertising revenues available to fund these products and services. Simply put, advertising is more effective if the message is more relevant. This makes advertising more valuable to both the consumer and the advertiser. Traditional advertisers have employed such practices for decades.

We would respectfully suggest that the appropriate framework for policy discussions is how to establish policies that encourage innovation while protecting privacy. In the first instance, policymakers should rely on industry best practices to achieve this result.

Consumers have a keen interest in safeguarding their privacy, but they also want information about products and services, and they want access to free or reasonably priced products and services. That is possible only with broadbased advertiser support. It is in this context that policymakers should review the appropriateness of a Do Not Track requirement.

Do Not Track raises some unique questions that make it significantly more complex than the popular Do Not Call list. For instance, how would Do Not Track affect consumers' online experience and expectations? Would they receive more pop-up ads? How would it affect diversity on the Internet? Would it negatively impact niche Web sites with small but loyal audiences? Would it prevent new Web sites from launching?

With Do Not Track still at the conceptual stage, the next step should be industry-led efforts to refine and test the concept, rather than legislation and regulation.

The codification of a Do Not Track requirement could quickly become moot in light of developing technologies. In contrast, self-regulation and best practices can quickly evolve to address the dynamic online environment. And while we believe that it is premature for Congress to move forward with Do Not Track legislation without further study, any privacy policy generally or Do Not Track policy specifically, whether adopted through industry best practice or government directive, should incorporate two principles: First, it should be focused on the kind of personally identifiable information that raises privacy concerns; and, second, it must be applied in the same way with respect to all entities operating in the Internet ecosystem.

Allowing some businesses to track individuals while precluding others from doing so will lead to consumer confusion. Consumers would be better served by a single standard applied uniformly, based on the data being collected and how it will be used. Regulation that disfavors one technology or business model would also deter entry, thwart innovation, and limit competition in the advertising marketplace.

We at Time Warner Cable look forward to working with you on these very important issues. Thank you, again, for the opportunity to appear before you today. I would be happy to answer any questions.

[The prepared statement of Ms. Gillman follows:]

STATEMENT OF JOAN GILLMAN
before the
Subcommittee on Commerce, Trade, and Consumer Protection
of the
Committee on Energy and Commerce
on
“Do Not Track” Legislation: Is Now the Right Time?

December 2, 2010

STATEMENT OF JOAN GILLMAN

Thank you, Chairman Rush and Ranking Member Whitfield. My name is Joan Gillman. I am Executive Vice President and President, Media Sales, at Time Warner Cable. In that capacity I lead Time Warner Cable's advertising sales initiatives. I appreciate the opportunity to appear before the Subcommittee today to discuss consumer privacy, including the potential for "do-not-track" legislation.

Do-not-track proposals cannot be considered in a vacuum. Rather, the advisability of do-not-track must be part of a larger conversation about the appropriate role for government in ensuring consumer privacy as interactive technologies continue to evolve and mature. One part of this conversation is recognition of the important role that advertising has played and will continue to play in providing essential financial support for online and other media content that in many instances simply would not be available without such support. Any measures considered must also take account of the risk that new regulations imposed on online businesses could inhibit innovation and growth of the Internet economy, and thwart the development of new technologies and new services.

Time Warner Cable appreciates this Subcommittee's diligent and balanced efforts to grapple with the complex and still-evolving interactive advertising marketplace and to assess its impact on consumer privacy. Protecting privacy is not only important as a matter of public policy, it is also central to the success of our business.

The bedrock foundation of our business is our relationship with our subscribers. We operate in a highly competitive marketplace, and our ability to succeed depends upon winning and retaining the trust of our customers. Our customers rely upon us to serve as a trusted medium for accessing and delivering content and services that reflect consumer tastes and

preferences. It is our job to preserve and strengthen that trust, while continuing to innovate and introduce the benefits of new network technologies and capabilities.

Presently, Time Warner Cable does not engage in targeted online advertising, as an ISP, based on our subscribers' web surfing activities or target ads based on consumers' search queries, web surfing, or related aspects of their usage.¹⁷ As we examine new advertising business models, Time Warner Cable is committed to ensuring the protection of our customers' privacy.

While industry must proceed with care as it explores new advertising initiatives, so, too, should the debate about privacy policy recognize the benefits of these initiatives. In particular, advertising has emerged as a key driver of the incredible array of online content, services and applications available to users at little or no cost. Because of advertising revenue, these websites and Internet content are available either without a separate subscription fee or at a subsidized price. Websites without offline outlets for their content are often wholly dependent on a robust advertising revenue stream in order to continue to offer their content without charge. Likewise, niche websites with small, albeit loyal, followings also benefit from the desire and ability of companies to tailor ads for specialized demographics and online user segments that may be particularly interested in their products.

The more effective the advertising, the greater the advertising revenues available to these websites. Tailoring ads to viewers is one way to make the advertising more effective – and more valuable to both the advertiser and the consumer. Such tailored advertising is by no means novel or unique to the online world. Advertisers using traditional media and marketers undertaking offline promotional campaigns have employed targeting techniques – based upon geography, demographics, interests and preferences, and purchasing patterns – for decades. In the online

¹⁷ We do rely on cookies and IP addresses to avoid repeating a single display ad too frequently and to prevent consumers from seeing out-of-market ads.

world, targeted advertising both responds to, and helps to preserve and promote, the rich diversity of the Internet. The FCC's National Broadband Plan expressly acknowledged the link between online advertising and the Internet features and capabilities that are most popular with consumers:

Whole new categories of Internet applications and services, including search, social networks, blogs, and user-generated content sites, have emerged and continue to operate in part because of the potential value of targeted online advertising.^{2/}

The appropriate framework for policy discussions, therefore, is not how do we impose the most stringent privacy regime, but rather how do we establish the policy that encourages innovation while protecting privacy. In the first instance, policymakers should rely on industry best practices to achieve this result. Consumers have a keen and important interest in safeguarding their privacy, but they also want information about products and services and they want access to content at a reasonable price that is possible only with advertiser support. Privacy policy should reflect both of these objectives. As FTC Chairman Jon Leibowitz has observed, targeted online ads are typically “good for consumers, who don't have to waste their time slogging through pitches for products they would never buy; good for advertisers, who efficiently reach their customers; and good for the Internet, where online advertising helps support the free content everyone enjoys and expects.”^{3/}

It is in this context that policymakers should review the appropriateness of a do-not-track requirement. Do-not-track remains largely a concept – “do not call” was successful, so let's extend that model to the collection of data about online activities. Depending on how do-not-

^{2/} *Connecting America: The National Broadband Plan*, Federal Communications Commission, at 53.

^{3/} “Leibowitz: FTC Not Interested in Regulating Behavioral Ads,” *Multichannel News*, May 12, 2010.

track is implemented, however, it could be a blunt instrument that upsets consumer expectations and negatively affects advertiser-supported content businesses (such as newspapers, magazines, and video – TV and movies) – even as these industries try to figure out how to create viable online business models. Do-not-track could hinder job creation within the advertising industry and by websites that rely on advertising revenues. It may also deter the provision of free online advertiser-supported content and inhibit innovation and the development of new services.

Do-not-track also raises technical and legal questions. Who would enable do-not-track – ISPs, browser makers, web servers, or some combination? What software or other technical changes would be required? Would a do-not-track election apply only with respect to identified websites? Another potential technical challenge is the fact that, unlike telephone numbers, IP addresses are dynamically assigned to users. While this may change with the assignment of IP addresses under IPv6, it will not change overnight. That means there is no stable one-to-one relationship between an IP address and a user's device, potentially undermining the permanence of a do-not-track election. Would websites be permitted to limit the content available to consumers who elect do-not-track? On the legal side, who would enforce a do-not-track rule? The Telephone Consumer Protection Act (the do not call law) includes both FCC and FTC jurisdiction. Would both agencies have a role in implementing do-not-track?

With do-not-track still at the conceptual stage, the next steps should be industry-led efforts to refine and test the concept rather than legislation or regulation. In contrast to the codification of a do-not-track requirement, which could quickly become moot in light of developing technologies, self-regulatory programs can quickly evolve to address the dynamic online environment. Do-not-track is a natural addition to the ongoing dialog with other industry and public stakeholders on privacy issues.

While it is premature for Congress to move forward with do-not-track legislation without further study, *any* do-not-track policy, whether adopted through industry best practice or government directive, should incorporate two principles. First, as I have just noted, the do-not-track mechanism should be focused on the kind of personally identifiable information that raises privacy concerns. Second – and this is a point the cable industry has made in connection with the broader privacy policy proposal embodied in Chairman Rush’s “BEST PRACTICES Act,” H.R. 5777 – any do-not-track requirement must be applied on a competitively neutral basis to so-called “edge” entities and network providers.

It makes no difference to an Internet user whether information is being collected from clickstream data or collected by an ad network, and there is no justification for imposing do-not-track on one participant in the ecosystem but not others. To the contrary, allowing some businesses to track individuals while effectively precluding others from doing so will lead to consumer confusion. An online user’s privacy rights should not vary based upon the identity of the entity collecting data, analyzing the information, or delivering the advertisement. Consumers would be better served by a single standard applied uniformly based on the data being collected and how it will be used. 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. Fewer choices for online ad sales could exacerbate the already significant financial pressure on advertiser-supported media. It would be particularly self-defeating to exclude edge-based providers from any do-not-track requirement, given their currently overwhelming share of the online advertising marketplace.^{4/}

^{4/} By one estimate, Google and DoubleClick (which is owned by Google) account for “more than 65%” of the market share for ad servers. The next closest competitor is AOL, which serves approximately 7% of all ads. “Yahoo! Ad Server share Drops By Half; Google DoubleClick Dominate Market,” Attributor, May 7, 2010, at <http://attributor.com/blog/yahoo-ad-server-share-drops-by-half->

By contrast, a common set of rules will create relative certainty for consumers and allow all businesses seeking to offer the benefits of targeted advertising to compete and innovate on a level playing field. It will also preclude any company from attempting to compete by leveraging preferential access to personal information in a clandestine or inappropriate fashion.

Rather than starting with do-not-track, we would urge this Subcommittee to continue its work, which it began with H.R. 5777, on identifying a set of fair information practices for targeted advertising. We continue to believe that those practices are most appropriately implemented through self-regulation and the adoption of industry best practices. As I noted earlier, targeted advertising offers substantial benefits to consumers. Advertising remains a critical way to fund content and services online, often for free. Advertising that is more relevant is likely to be of more practical value to the consumer and essential to ensure the continued explosion of new content and services. And more entry into the advertising marketplace will bring more innovation and choice, as well as more content and services, to consumers.

Fair information practices should be imposed in the first instance through industry self-regulation, which is inherently more able to adapt to the dynamic online marketplace than regulation, but in any event should apply to all providers of online targeted advertising in a competitively neutral manner. In fact, the most egregious privacy breaches of the past year have originated not from ISPs, but rather from edge providers. There is no basis in fact for any presumption that network-based data collection poses a more serious threat to privacy than collection by edge providers.

google-doubleclick-dominate-market-2/. A recent survey found that the "Google Ad Network led the October Ad Focus ranking with a reach of 93.4 percent of Americans online, followed by Yahoo! Network Plus with an 86.3-percent reach and AOL Advertising with 86.2 percent." Inside the Ratings (U.S. Edition) Oct. 2010, comScore Media Metrix (audience measurement services), at http://www.comscore.com/Press_Events/Press_Releases/2010/11/comScore_Media_Metrix_Ranks_Top_50_U.S._Web_Properties_for_October_2010.

Thank you again for the opportunity to appear before you today. As you continue to develop privacy policy, we respectfully urge you to consider issues concerning online privacy in their full context – framing requirements in a manner that permits the continued growth and innovation in advertiser-supported services and treating all participants in the ecosystem on a competitively neutral basis. We at Time Warner Cable look forward to working with you in this effort.

I'd be happy to answer any questions you have.

Mr. SPACE. Thank you, Ms. Gillman.

Our next witness, Eben Moglen, legal advisor, Diaspora; professor of law, Columbia University; and founding director, Software Freedom Law Center.

Mr. Moglen.

STATEMENT OF EBEN MOGLEN

Mr. MOGLEN. Thank you, Chairman Rush, Ranking Member Whitfield, Mr. Space, and other members of this subcommittee. I very much appreciate the invitation to testify, and I would like to express my particular gratitude for the committee's strong respect for free speech in the legislative process.

I think it would be useful to begin with a technical clarification. The receipt of advertising on the Web is already completely optional. I receive no advertisements in my browser, on my laptop or on my mobile devices. Any member of the committee or any member of the listening on C-SPAN, using the Firefox browser, could search briefly for Adblock Plus and discover that advertising is already optional to receive entirely, whether it is targeted advertising or nontargeted advertising.

The apparent connection made in the course of this discussion between the economics of the advertising business and whether surveillance ought to be authorized or acceptable on the Web therefore escapes me.

It is already possible for anyone wishing to receive no advertising to do so. Civilization has not collapsed. The distinguished businesses represented here are still in business. And I believe there is no justification for the conclusion that legitimate control of surveillance on the Web in the public interest would have any effect on the economics of the situation, since a blanket ban on receipt of advertising by individual consumers is already fully implemented and available at no charge.

I also believe that the concept of tracking is perhaps a part of the general mystification in which consumers find themselves. We should, I think, be more clear with consumers who do not have our level of interest in or expertise in these questions if we simply pointed out that the Internet has become a very highly surveilled locale relative to all previous social environments.

As Mr. Markey pointed out earlier this afternoon in his questioning, we already have a world in which more than half a billion people live all of their social lives online inside a service provider structure, which puts everything they do, everything they say to one another, every photograph they post, every piece of information they distribute about their social lives, in one great big database owned by a single for-profit business which Mr. Markey named.

I think we ought therefore to conclude that the idea of Do Not Track, which really ought to be described to the public whose interests we are protecting as "Do Not Surveil," is a problem more serious and more comprehensive than the problem of addressing behavioral advertising, which is merely one wrinkle in a rapidly changing technical environment, as others have noted.

The problem we really face is the problem of identifying the level of surveillance of human beings in their daily activities, the "online

oxygen” that Mr. Markey referred to. How much surveillance is socially tolerable?

Never mind whether it is for profit or for the protection of people from wrongdoing of one kind or another. How much are we prepared to abandon our traditional human understanding, that what we do, when we read, when we speak to our friends, when we go about our social lives, is nobody’s business except the business of the people with whom we choose to share?

Many technologies, including technologies being developed by my client base, the client base of nonprofit entities who make software for everyone to share, freely and at no cost, many technologies under development would allow us to achieve the enormous benefits of the Web we know now, along with many other benefits of the Web we will still enjoy, with minimal levels of surveillance.

That will undoubtedly bring significant economic change, as the Web itself has brought economic change during the last 8,000 days, which is the total life of the Web. In the next 8,000 days, we can decide whether what we want is all the benefits of social networking and all of the benefits of online culture with comprehensive spying going on all the time or without comprehensive spying going on all the time.

As public servants, all of us, I think our role is to arrange to have as little spying as we can. I do not think that is an obligation we can trade off against any other, because I think it reaches directly to the heart of what constitutional freedom is.

In my judgment, what we require is a comprehensive national privacy policy act in which Congress does what Congress does best: set large, general, societal goals and empower all Federal agencies in the conduct of their activities to achieve those goals.

The National Environmental Policy Act has within one generation done enormous amounts to clean our water, our air and our environment because of Congress’s wisdom in the declaration of broad general principles for the protection of the public interest.

Privacy online is the single largest environmental issue in the online world, and it should be addressed with the same degree of seriousness and comprehensiveness with which the physical environment was addressed by Congress one generation ago.

Businesses will naturally regard such regulation as burdensome, and that is not a big deal. We must have a clean environment to live in, and we must have a clean online environment that protects our freedom. Our principles acknowledged, there will be plenty of money for everybody to earn, but without our principles acknowledged, we will buy our convenience with our freedom, and that is far too high a price to pay.

Thank you for your time. I am happy to answer your questions.
[The prepared statement of Mr. Moglen follows:]



Software Freedom
Law Center

Eben Moglen
+1-212-461-1901
moglen@softwarefreedom.org

Testimony of Eben Moglen

1995 Broadway, 17th Floor
New York, NY 10023-5882

tel +1-212-580-0800
fax +1-212-580-0898

www.softwarefreedom.org

December 2, 2010

US House of Representatives
Committee on Energy and Commerce
Subcommittee on Commerce, Trade & Consumer Protection

Mr. Chairman and Members of the Subcommittee,

Thank you for the invitation to appear today to help the committee address this very important subject.

“Social networking” offers immense economic, educational and personal opportunities for people everywhere. Rapid adoption of technologies for sharing information among socially connected but geographically dispersed groups is changing how we live, how we work, and how our children learn about the world. But social networking as we presently use it is technically arranged as “centralized” services, in which one party—let us call it “Facebook” for convenience—keeps all the data that everyone is sharing with everyone else in one big database. The service provider absolutely controls this database, which they can access however they like, regardless of the controls over third party access to the data, and which they can build profitable “data mining” activities atop.

This situation, in which one business controls all the shared data of hundreds of millions of people, is not a technical requirement, but rather a bad design decision grown out of control. The Internet and the World Wide Web, which are the technical infrastructures on which social network applications sit, does not require centralized control of shared data. All the technical features people like about social networking could be delivered to them without centralized data storage and the resulting privacy invasions.

Facebook and similar centralized social networking services like to talk about their “privacy settings.” This is mere deception, a simple act of deliberate confusion. These “privacy settings” merely determine what one user can see of another user’s private data. The grave, indeed fatal, design error in social networking services like Facebook isn’t that Johnny can see Billy’s data. It’s that the service operator has uncontrolled access to *everybody’s* data, regardless of the so-called “privacy settings.”

Facebook holds and controls more data about the daily lives and social interactions of half a billion people than 20th-century totalitarian governments ever managed to collect about the people they surveilled. As viewers of a recent motion picture are aware, Facebook was not the result of careful, thoughtful development by technologists concerned with the ethical dimension of information technology. Instead, immature technology created by immature people has become popular, and valuable, despite its manifest defects. Because those defects are potentially profitable, giving the holder of social network databases unparalleled access to people’s internal lives, unregulated commercial activity will not solve the problem of initial technological misdesign: commercial motives uncontrolled by regulation in the public interest will make the problem worse.

The nature of the technological redesign required to give people everywhere the ubiquitous benefits of social networking without the negative consequences of centralized for-profit spying is well-understood. Mr. Rafael Sofaer, from whom you have already heard, is one of the young technologists working to replace the poor design that yielded Facebook with designs that can serve individual needs without harming the public interest in maintenance of individual privacy. He and his colleagues in the Diaspora project, along with hundreds of other volunteers in the free software and open source movement who make great computer software to share, are already bringing into existence the second-generation social network architecture that offers sharing to everyone, without putting anybody in the middle, holding all the data for everybody else. Using a social network service like Face-

book means that every time you *access* anybody else's shared data, you're making a record about yourself. Facebook knows not only what everybody posts, but also what everybody reads. Users of systems like Diaspora, however, can be sure that only the parties actually sharing know who accesses their data: no one else knows whether Susie is checking Billy's page, and everything Billy shares he shares from a safe place under his own, not Mr. Zuckerberg's, control.

But regulation of social networking technology in the interest of privacy can't work by regulating technology. Government cannot determine what innovations *will* happen, let alone determine what *should* happen. Nor can agency rulemaking—which is a slow and complex process that powerful businesses can more easily influence than individuals—be counted upon to respond with speed and agility to market developments that harm the public interest.

Instead, Congress should look at privacy questions from the same regulatory perspective used to address the issue of environmental quality, when—under the Nixon Administration—the Federal Government began making serious attempts to improve the environmental health of the United States. We need a National Privacy Policy Act, like the National Environmental Policy Act, in which Congress declares the clear overall national goals to be pursued, and requires federal agencies to assess all their regulatory activities in light of those goals. As with environmental law, Congress needs to entrust a lead agency with the primary responsibility for bringing to bear technical as well as legal and political resources in that effort. The Federal Trade Commission is plainly suited to the role of lead agency on privacy, and its traditional mode of activity since 1915, namely the investigation and “prosecution” of complaints, is the appropriate regulatory style. The FTC can and does behave with the agility and perseverance necessary to obtain compliance with the public interest in complex and fast-changing marketplaces. Empowered by clear and specific Congressional declarations of national privacy policy, the Commission would be well positioned to use its traditional tools to protect the public interest.

Precise delineation of national privacy goals will require full public debate and careful Congressional consideration. As with environmental policy, businesses with bad records of deteriorating the public interest can be expected to demand inaction, rather than reinvigorated protection of the public. But poor technological design with profoundly unethical public consequences does not become sacrosanct once it makes a lot of money.

Thank you.

Mr. SPACE. Thank you, Dr. Moglen.

Our final panelist, Mr. Daniel Castro, senior analyst, Information Technology and Innovation Foundation.

STATEMENT OF DANIEL CASTRO

Mr. CASTRO. Mr. Chairman and members of the committee, I appreciate the opportunity to appear before you. I would like to talk with you about why a government mandated Do Not Track program would be a mistake.

If widely adopted, this type of mandate would significantly harm the current funding mechanism for the Internet ecosystem, resulting in less free content and fewer free services online. In addition, it would be costly to implement, difficult to enforce, and result in more intrusive and less relevant advertising for consumers.

First, it is important to understand that the Internet ecosystem is a significant source of economic activity in the United States, accounting for approximately \$300 billion, or roughly 2 percent of GDP, and online advertising is the fuel powering this economic dynamo.

Online advertising has grown dramatically over the past decade. As of 2009, the online advertising market was about \$23 billion in the United States, and analysts predict that, of the \$600 billion spent globally on advertising each year, an increasingly larger share of this will go to the online sector.

Many of the Web sites that millions of Americans use daily for work and play would not be around today without advertising. Of the top five most popular Web sites in the United States, Google, Facebook, Yahoo, YouTube, all of these used advertising almost exclusively to support their products and services, and number five on that list, Amazon.com, uses it to supplement theirs.

Targeted ads represent a growing proportion of online ads on these Web sites. Targeted ads are a benefit to consumers, who get more utility from these ads. The percent of users who actually click on an ad are as much as 670 percent higher for targeted ads than nontargeted ads, and advertisers are willing to pay more to reach their desired audience. Advertising rates are almost three times higher for these targeted ads.

Targeted advertising does not involve selling data about users. These Web sites match ads provided by advertisers to users based on their interests, often without even using any personally identifiable information.

I want to emphasize that the impact of policy changes For online privacy can be profound. There is a study by professors at MIT and the University of Toronto on the impact of EU's privacy directive. The directive limits the ability of advertisers to collect and use information about consumers for targeted advertising.

The study found that, in Europe, the privacy directed resulted in an average reduction in effectiveness of online ads by approximately 65 percent. Similar limits on targeted advertising in the United States, especially through a Do Not Track proposal, would be even more harmful. Not only would it eliminate the billions of dollars that targeted advertising pumps into the Internet economy, it would stunt the huge potential growth in innovation for new con-

tent and services that would come with more of these higher value ads.

Do Not Track would also be costly to implement and difficult to enforcement. The most popular proposal right now on how Congress or FTC or anyone else can mandate a Do Not Track mechanism is through a modification of the HTTP header. Such a change would require substantial retooling of existing Web sites, Web browsers and other related software and devices, the cost of which, of course, would ultimately be borne by consumers.

In addition, the proposal leaves much ambiguity about what does or does not constitute tracking. Do Not Track may allow sites which have large databases of user information to continue to provide targeted advertising but would hurt the ability of smaller publishers to rely on third party ad networks to deliver personalized ads. It may also not apply to other emerging forms of online advertising, such as deep packet inspection.

Congress should be careful not to devise policies around a particular business model that would end up hurting some businesses while helping others. It should also not forget that consumers today have many tools to protect their privacy online.

Finally, Do Not Track would result in more intrusive and less relevant advertising for consumers. Do Not Track, of course, doesn't actually stop online advertising. It only limits the ability of ad networks to deliver ads that the user might actually want. Users who opt out of tracking would receive more, not less, unwanted advertising.

In addition, advertisers would likely resort to overlay and pop-up ads, which users may find annoying, but actually are more effective at getting their attention. The reason for this is that the small text-based ads are significantly less effective unless they can be tailored to a user's interest. If Do Not Track were widely implemented, another option, of course, is that Web sites may simply choose to block users who do not allow tracking.

In short, privacy is important, but it must be balanced against competing goals, including usability, cost, future innovation and consumer benefit. A Do Not Track requirement would do more harm than good, and for that reason, I urge the Federal Government to not go forward with this approach.

Thank you.

[The prepared statement of Mr. Castro follows:]

Daniel D. Castro
Senior Analyst
Information Technology and Innovation Foundation
“Do-Not-Track” Legislation: Is Now The Right Time?
Before the
Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection

December 2, 2010

Mr. Chairman and members of the Committee, I appreciate the opportunity to appear before you to discuss the implications of “Do Not Track” legislation for the Internet. My name is Daniel Castro. I am a senior analyst at the Information Technology and Innovation Foundation (ITIF) and a former IT auditor at the Government Accountability Office. ITIF is a nonpartisan research and educational institute whose mission is to formulate and promote public policies to advance technological innovation and productivity.

Privacy concerns associated with information technology (IT) and the Internet must be taken seriously, but it is important to keep a sense of perspective. Historically, major new technologies have prompted what in hindsight were overblown privacy fears. To cite an example, some people objected to easy-to-use cameras, fearing that an individual’s activities would no longer be private when walking down the street.¹ Or to cite another example, when transistors were first developed, there was a short-lived privacy scare that everyone would be able to be snooped on using small electronic “bugs.” In fact, a *Life Magazine* cover story trumpeted “Insidious Invasions of Privacy” and Congress even went so far as to hold hearings on the matter.² Of course, all this fuss was much ado about very little.

Society has always learned to manage these so-called threats in large part because of the fact that many—but certainly not all—of the concerns raised by privacy activists then as well as now are hypothetical and speculative.³ Given the large amount of information in digital format today, it is worth asking how much harm has been done to date. Notwithstanding all the fear and gloom from privacy activists, there simply have not been widespread privacy violations caused by existing privacy laws and regulations. Moreover, the debate on privacy to date has been driven largely by privacy fundamentalists (i.e., those individuals who value personal privacy above all other values) that advocate protecting individual privacy above all else, no matter the costs or consequences. However, as with most issues, policymakers should take a balanced approach that

considers both the needs of individuals and the impact on society, rather than focusing exclusively on the demands of individuals that come at the expense of the collective good.

Online advertising is a crucial part of the Internet ecosystem, but unfortunately it has been misunderstood by some. For the last few years privacy fundamentalists have called for a national Do Not Track feature for online activity modeled after the national Do Not Call Registry managed by the Federal Trade Commission (FTC). The purpose of a Do Not Track feature would be to provide consumers a single, centralized mechanism to opt out of all online profiling for targeted advertising. However, such a mandate would impose unnecessary costs that would ultimately be borne by consumers, result in more intrusive and less relevant advertising for consumers, and, if widely adopted, significantly harm the current funding mechanism for the Internet ecosystem, resulting in less free content and fewer free services online. In short, a Do Not Track requirement would do more harm than good and for that reason ITIF urges the federal government to not go forward with this approach.

Online Advertising Benefits Consumers

The Internet ecosystem is a significant source of economic activity in the United States accounting for approximately \$300 billion in activity (or roughly 2 percent of GDP⁴), and online advertising is the fuel powering this economic dynamo.⁵ ITIF estimates that the annual global economic benefits of the commercial Internet equal \$1.5 trillion, more than the global sales of medicine, investment in renewable energy, and government investment in R&D, combined.⁶ Policymakers should consider carefully any attempts to limit the use of online advertising, and its effect on the Internet at large, before tampering with the foundation of its growth.

As shown in Figure 1, Internet advertising has grown dramatically over the past decade. In the United States, non-search online advertising expenditures have grown from \$6 billion in 2002 to \$13 billion in 2007. Similarly paid search has grown from \$1 billion in 2002 to \$8 billion in 2007.⁷ The Internet Advertising Bureau estimates the cumulative U.S. Internet online advertising market to be \$22.7 billion as of 2009.⁸ The Kelsey Group found that worldwide Internet advertising reached approximately \$45 billion in 2007, out of a total \$600 billion advertising market, and predicts online advertising will grow to over \$147 billion by 2012.⁹ IDC reports similar figures estimating that worldwide spending on Internet advertising reached \$61 billion in 2009. In addition, IDC predicts that advertisers will increasingly use the Internet for advertising, with online ad spending growing from 10 percent of all ad spending in 2009 to almost 15 percent by 2013.¹⁰

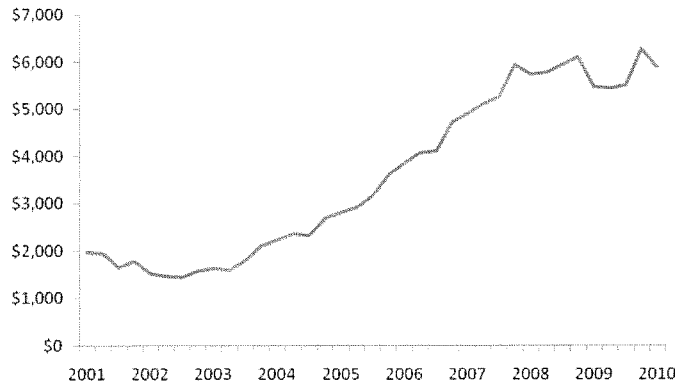


Figure 1: U.S. Quarterly Internet Ad Revenue since 2001, Source: IAB/PWC¹¹

Internet advertising supports the creation and maintenance of new online content, applications and services including news, videos, music, games, social networking, reference, email and other online services. Indeed, many of the websites that millions of Americans use daily for work and play would not be around today without online advertising. In fact, of the top five most popular websites in the United States—Google, Facebook, Yahoo, and YouTube all use online advertising almost exclusively to support their products and services and Amazon.com uses it to supplement theirs.

In particular, online advertising benefits online publishers like news outlets. Policymakers concerned with the decline of print media should note that greater revenue from targeted online advertising will likely be necessary for journalism to survive in the Internet age.¹² We are already seeing some evidence of this. For example, the Los Angeles Times announced in 2009 that its online advertising revenue was sufficient to cover its entire editorial payroll.¹³ And online advertising will be important for the so-called “long tail” of small websites and content producers supported by ad revenues. After Google introduced a revenue-sharing program in 2007 for YouTube, various Internet entrepreneurs began turning their videos into a lucrative business. For example, Josh Chomik, a teenager in New Jersey earns around \$1,000 a month from ad revenue generated by his YouTube videos.¹⁴

Consumers download many different types of applications supported by online advertising. These include products from major U.S. technology companies like Google and Microsoft. For example, Google Apps, which includes free Internet-based applications for word processing and email, is funded by online advertising. Similarly Microsoft Office Live is available in a no-cost, ad-supported version and Microsoft Office Starter 2010, a reduced-functionality version of

Microsoft Office which includes display advertising, is available to consumers for free. Fast-growing start-ups like Evernote which has over 5 million users offers both an online application and a desktop application for taking notes at no cost with advertising. IT professionals routinely use free, ad-supported software like Spiceworks to monitor and manage their networks. Even the fast-growing health IT field has advertising-based products: Practice Fusion is a no-cost, web-based electronic health record solution for doctors.¹⁵ Rather than charge doctors a monthly fee, the hosted service is provided for no charge to doctors who use the ad-supported service. Alternatively, health care providers can pay a \$100 per month to access the service without ads.

If online advertising is central to the health of the U.S. Internet ecosystem today, then ensuring that online advertising revenue continues to grow will be central to the Internet's growth and success tomorrow. One key way websites gain more value from online advertising is by providing more relevant ads—a benefit both to consumers who get more utility from these ads and advertisers who are willing to pay more to reach their target audience. Targeted ads based on information about a user—such as the user's browsing history or other user-specific data—help deliver higher-value ads. Many of these ads can be delivered using non-personally identifiable information since the interests of the user often do not need to be tied to an actual identity.

Targeted advertisements are more effective than non-targeted online ads since they are more relevant to users' interests. Click-through-ratios, or the percent of Internet users that click on an ad, are as much as 670 percent higher for targeted ads than non-targeted ads.¹⁶ These ads also generate more revenue. Advertising rates for online ads that use behavioral targeting are significantly higher than online advertising that do not use behavioral targeting (one study found it to be 2.68 times as much).¹⁷ Moreover, unlike niche websites that focus on a particular topic or demographic, without learning more information about users, general interest websites like online newspapers cannot deliver targeted ads to users since they know very little about the interests of each individual. Yet even though the importance of online advertising to the greater Internet economy and American consumers has been well-documented, some advocates and policymakers seem intent on imposing data privacy regulations that would limit the ability of Internet publishers to tailor advertising to users based on their interests.

Part of this may be due to a misconception about how targeted advertising works. When Google first offered ads to users of its free Gmail service based on contextual information in emails, privacy advocates objected to Google "reading people's email."¹⁸ Yet these claims do not distinguish between ads delivered to Internet users through automated computer technology and an individual snooping through a person's emails. In the former, providing targeted computer-matched ads poses no more privacy threat to users than simply having their emails stored on remote servers because there is no additional information to which Google has access.

Similarly privacy concerns have been raised about online advertisers like Facebook with fictional claims of the company selling its user's data because of misunderstandings about the mechanisms of targeted advertising. Targeted advertising works by matching ads to users based

on the information in their profile. For example, a wedding photographer in Dallas can pay Facebook to serve an ad to everyone in Dallas who switches their relationship from “single” to “engaged.” This benefits everyone—the photographer gets more clients, the users get more relevant ads, and Facebook is better able to fund its free services. But at no time does the photographer learn who sees the ads, unless a user chooses to make contact.

Web-Based Tracking Used For More Than Just Online Advertising

Like online advertising, Internet-based “tracking” is also misunderstood. One problem with the term “tracking” is that it is an overly-broad term that does not correlate to a specific technical activity. Many activities could be considered tracking: setting unique identifiers for users in their web browser cookies, logging IP addresses on a server, monitoring IP packets over a network, and building unique profiles for users on a website. Policymakers should remember that companies collect data for many purposes besides providing targeted advertising. Google, for example, uses data provided by consumers for everything from tweaking its search results to developing its free email service to improving its speech-to-text engine that is now used on mobile phones. Many websites use consumer data to deliver personalized services to deliver content to users based on information they, or a third party, know about the user. Online newspapers like the Washington Post use information provided by social networks to display articles recommended by a user’s friends. The online music service Pandora can use information from an individual’s Facebook profile (with the user’s permission) to create a customized web-based radio station tailored to that user’s musical preferences. Even when used for online advertising, companies do not just collect data to deliver customized user ads. Online advertisers use logs, for example, to create an audit trail so that they can prove to their customers that they have delivered the number of ads that they have sold and prevent criminal activity, including click fraud.

When privacy activists refer to online tracking they are most commonly referring to cookie-based tracking of users. Many websites use HTTP cookies—small data files stored on a user’s computer by a web browser. When a user visits a website, the website can request that the user’s web browser store certain data in a cookie. By default, most web browsers allow this activity. A cookie may be used to store temporary data, such as the contents of a shopping cart for e-commerce, or to remember a user on subsequent visits to the website, such as for customizing a website. Each cookie is accessible only by the Internet domain that created the data.¹⁹

For many privacy activists the risk from cookies is as follows: under some circumstances, cookies can be used to help website operators track website usage over time and build a profile of the activity of an instance of a web browser with the cookies on it (which may or may not tie back to a specific user). This profile can then be used to deliver targeted ads to a user based on his or her interests, such as travel or sports. In addition, if the website collects personally identifiable information, the website operator could link some browsing activity to individual identities instead of just the computer or browser being used. This could potentially lead to the

intentional or accidental disclosure of an individual's web browsing history—a clear violation of a user's expected level of privacy. Privacy advocates see the collection and misuse of such data to be the primary threat of cookies.

However, cookies also offer many benefits to consumers. Website developers use cookies to create robust online applications that offer a better user experience. Perhaps the most common use of cookies is to facilitate online commerce. Online shopping cart applications routinely use cookies to maintain the list of which items a shopper wants to purchase. In addition, if the user accidentally closes the web browser or the browser crashes, the user can often return to the website without having to reload items back into the shopping cart. Cookies facilitate these functions transparently to the user. Cookies also enable users to customize websites. For example, users can personalize settings such as preferred language or region so the website will recognize their preferences on subsequent visits. Weather.com uses cookies to remember a returning user's zip code and automatically displays the weather report for that user's geographic area. For websites requiring a login, cookies can be used to authenticate users so that the user does not have to always enter a username and password to access a website. Website operators also use cookies to learn how to best engage with their audience and measure the success of online content and online advertising. Cookies help website developers produce more advanced website analytics to better understand how users interact with their website. For example, cookies allow website developers to learn how many of their visitors are new or returning users.

Cookies can be classified based on the source of the cookie and the lifespan of the cookie. When classified by the source, cookies come in two flavors: first-party cookies and third-party cookies. First-party cookies refer to cookies created by the domain of the website that the user entered in the web browser. Third-party cookies are those created by affiliated domains, such as advertising networks used by the primary website visited by the user. For example, a user that visits CNN.com not only will receive cookies for CNN.com, but also for other domains used by online advertisers employed by CNN, such as doubleclick.net, revsci.net, and questionmarket.com.²⁰ Advertisers can use third-party cookies to track user preferences across multiple websites for targeted advertising. All major web browsers include the option to block third-party cookies.

When classified by lifespan, there are two types of cookies: session cookies and persistent cookies. Session cookies, as the name implies, last only as long as the user is on a particular website. Session cookies enable websites to remember data about users as they navigate from page to page on the same website.²¹ For example, session cookies enable technologies like online shopping carts. Persistent cookies last beyond the initial web browsing session. The cookies can be set to expire at a certain time or last indefinitely.²² These types of cookies are useful so that a website can recognize a returning user. For example, a website can use a persistent cookie to recognize a user on return visits, thus saving the user from having to log in at every visit.

Why Do Not Track Would Not Work

While the Do Not Track proposal is not new, it has received renewed attention in recent months. FTC chairman Jon Leibowitz testified in front of Congress in July 2010 that the Commission was exploring this proposal in its upcoming report on privacy and FTC Commissioner Julie Brill endorsed the Do Not Track proposal in October 2010.²³ A coalition of privacy organizations, including the Center for Democracy and Technology (CDT), the Electronic Frontiers Foundation (EFF), and the World Privacy Forum, first began advocating for the Do Not Track proposal in 2007. These groups reasoned that since consumers benefited from the popular Do Not Call regulations for telemarketing, consumers would similarly benefit from Do Not Track regulations for online advertising. While the proposal may be intriguing at first glance, a closer look reveals that the idea is illogical, impractical, and would hurt, not help, consumers.

Understanding the problems with Do Not Track first requires understanding how such a proposal could work. Comparisons between Do Not Call and Do Not Track are not useful from a technical perspective. The Internet is not the same as the telephone network. Individuals do not have a single unique identifier on the Internet. The closest unique identifier to a telephone number on the Internet is an Internet Protocol (IP) address, but users share and change IP addresses frequently which would render any IP-based opt-out list impractical.

A mandate by Congress to implement a Do Not Track mechanism would therefore have to be fulfilled through other means, including through changes in Internet browsers and other Internet-connected applications that show ads or modifications to the HTTP standard. CDT, which endorsed the Do Not Track idea in 2007, suggested the former.²⁴ They proposed that advertisers be required to provide the FTC a list of the domain names used to set persistent unique identifiers and track users across multiple websites. In addition, companies that make web applications such as web browsers and plug-ins would have to develop new functionality to block these domains and keep the list up-to-date.

An alternative implementation for Do Not Track would require modifying the HTTP protocol used for web browsing so that users could signal to the web server that they do not want to be tracked. The server would in turn be required to detect this flag and then refrain from setting any unique persistent identifiers for that particular user. Implementing this for all users would require that all software using HTTP be updated to the new standards. This proposal would only apply to HTTP traffic. Non-HTTP applications that use targeted ads would require a separate implementation. Clearly, such a change would require substantial retooling of existing websites, web browsers and other related software, the costs of which would ultimately be borne by consumers, the majority of which are not bothered by targeted advertising on the Internet.²⁵ This implementation of Do Not Track would also likely not apply to other emerging forms of online advertising such as that provided by Phorm or the now defunct NebuAd which uses deep packet inspection to deliver targeted advertising in coordination with ISPs. Policymakers should be careful not to devise policies around a particular business model that would end up harming some businesses and business models while helping others.

Although comparisons are often made between the two, there are many differences between the existing National Do Not Call Registry and the Do Not Track proposal. The National Do Not Call Registry is designed to reduce the amount of unwanted telemarketing phone calls that consumers receive. The purpose is to make it easier and more efficient for consumers to stop getting unwanted telemarketing calls.²⁶

In contrast (and somewhat ironically) the Do Not Track proposal would have the opposite effect of the National Do Not Call Registry since users who opt out of tracking would receive more, not less, unwanted advertising. Do Not Track would not stop online advertising, but rather would limit advertisements based on an individual's interests thus increasing the amount of irrelevant (and therefore unwanted) advertising for each user that opts out. In addition, advertisers would likely resort to overlay and pop-up ads which users may find annoying but are more effective at getting their attention. As professors Goldfarb and Tucker found in a study of the impact of European privacy regulations on online advertising, small, text-based ads are significantly less effective unless they can be tailored to a user's interests.²⁷

The federal government would also not be able to effectively enforce a Do Not Track proposal. While it is easy to determine if someone violates a Do Not Call list, it is significantly more difficult to determine if someone is violating a requirement not to record certain data about users as they visit a website. 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 standards bodies. Would U.S. consumers be stopped from downloading browsers made in other nations that are not covered by this regulation?

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.²⁸ 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 benefitting from the willingness of the majority to divulge some 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.

This is why the analogy to Do Not Call is fundamentally flawed. When consumers choose to opt out of unsolicited telemarketing calls they are not at the same time receiving some free service that is linked to the telephone call. It would be one thing if, for example, the telephone company said in exchange for free telephone service marketers get to call your phone every evening at dinner time. But that is not the deal. There is no quid pro quo. These unsolicited calls are simply

an added cost to the economy and an annoyance to most consumers. So it makes sense to have an easy-to-use opt out system for unsolicited telephone calls.

In contrast, Do Not Track is like getting the free telephone service without taking the marketing calls. When consumers go online, in the vast majority of cases they are receiving some free content or service (e.g., email, search, data storage, social networking, news, information, entertainment, etc.). And the way they “pay” for these free services is by agreeing to be shown advertisements. And to cover the cost of all of these services companies increasingly need to show ads that are actually of interest to consumers. By opting out of this mutually beneficial relationship, some consumers are trying to get something for nothing.

This is essentially a case of the famous prisoner’s dilemma. If no one opts out of targeted advertising, the overall Internet ecosystem continues to grow and consumers continue to benefit through the creation of more free content, applications and services. If one person opts out, but other users do not, the overall value of the Internet ecosystem diminishes by a very small amount. But if everyone, or a large share of Internet users, opts out, then the overall value of the Internet ecosystem diminishes by a significant degree. In this case, what may appear to be rational for the individual is irrational and destructive to society. The last thing government should be doing is making it easier for individuals to act in a way that is harmful to society.

This is not to say that consumers should not be able to avoid targeted advertising. But the way to do that is to not access sites that display this type of advertising and use existing tools to manage online privacy. But just as users cannot “opt out” of paying for a magazine at a newsstand, users should not be able to opt out of targeted advertising and still receive access to the free content. Similarly, customers at a grocery store who use a loyalty card receive a discount and those who choose to keep their shopping behavior private do not. Of course privacy activists pushing for Do Not Track want to have their cake and eat it too. If the marketplace could evolve to the point where website operators only made content available to individuals who permit targeted advertising, many privacy advocates would likely start clamoring for legislation to prevent companies from “discriminating” against users who opt out of targeted advertising.²⁹ They might even call for public funding of Internet content so that users would not have to see advertising.

Finally, policymakers should remember that online privacy is complex. While some users may not want certain online activities (e.g. online medical research) tracked and used to deliver targeted ads, others may welcome this advertising (e.g. ads targeted to their health concerns). Similarly, some users may consent to receiving targeted ads based on their activity on a single website but not based on their activity across different websites. Depending on how Do Not Track is applied it could limit targeted advertising to information gathered on a single domain but prohibit targeted advertising across multiple domains. This may allow sites like Amazon.com or Facebook which have large databases of user information to continue to provide targeted advertising but would likely hurt the ability of smaller publishers who rely on third-party

advertising networks to deliver personalized ads. A government-imposed, one-size-fits-all solution for privacy will not provide users what they want.

Policymakers Should Avoid Policies That Would Halt Innovation Online

The Internet is a vital part of economic and social life and policymakers must be vigilant against expensive and ineffective policies that would curtail beneficial uses of data. Congress should not implement heavy-handed privacy regulations without seeking a better understanding of how these changes will affect the Internet economy, and by extension, the overall economy and society. A recent example in Europe shows that the impact of these policies is not always evident at the outset. As discussed above, Goldfarb and Tucker analyzed the impact of the European Union's Privacy and Electronic Communications Directive (2002/58/EC) which was implemented in various European countries and limits the ability of advertisers to collect and use information about consumers for targeted advertising. The authors find that after the new privacy laws went into effect they resulted in an average reduction in the effectiveness of the online ads by approximately 65 percent (where the effectiveness being measured is the frequency of changing consumers' stated purchase intent). The authors write "the empirical findings of this paper suggest that even moderate privacy regulation does reduce the effectiveness of online advertising, that these costs are not borne equally by all websites, and that the costs should be weighed against the benefits to consumers."

Targeted advertising is crucial for supporting the websites responsible for the majority of the free and low-cost content online. This is particularly true for general-interest sites (like news websites) that have little ability to determine what ads their users would be most interested in without the cues that better targeting enables (in contrast to some special-interest sites which can do so somewhat more easily). Not surprisingly, Goldfarb and Tucker found that the negative impact on ad effectiveness from the European privacy regulations was strongest among these sites. The negative impact was also stronger for non-obtrusive ads (e.g. smaller ads or ads not using multimedia) which suggests that small, text ads will be significantly less effective unless they can be tailored to a user's interests. The authors also note that if European advertisers reduced their spending on online advertising in line with the reduction in effectiveness resulting from stricter privacy regulations, "revenue for online display advertising could fall by more than half from \$8 billion to \$2.8 billion."³⁰ And as Beales notes, a reduction in ad revenue directly hurts online publishers since more than half of ad network revenue goes to publishers who host the ads.³¹

It is therefore not surprising that U.S. Internet companies lead the world and European companies do not.³² European companies are at a disadvantage compared to U.S. companies because the government is essentially limiting their revenue to less than half of what they could otherwise earn. As a result, Europe has struggled to be an effective player in the Internet economy compared to the United States where there are significantly fewer restrictions.

As ITIF has noted, proposed privacy regulations in the United States would restrict targeted online advertising by limiting the collection of certain types of data, requiring opt-in consent for collecting data, or providing mechanisms to encourage users to opt-out of targeted ads.³³ Like the European privacy regulations, these types of restrictions would limit targeted advertising and harm the Internet-powered economy. These kinds of privacy regulation would reduce revenue flowing into the U.S. Internet ecosystem, which means not only fewer websites and less valuable content, but also less spending by Internet companies on servers and bandwidth. The net result will be fewer jobs. In addition, if the Internet is less valuable to consumers because there is less useful content, applications and services, users are less likely to subscribe to broadband.

Does this mean that policymakers should avoid all privacy regulations? Of course not. But it does suggest that policymakers should tread lightly and focus more on preventing harms from privacy violations than on legislating expensive and revenue-reducing regulations.³⁴ The evidence clearly suggests that the tradeoffs of stronger privacy laws result in less free and low-cost content and more spam (i.e. unwanted ads) which is not in the interests of most consumers.

Proponents of stricter privacy laws often ignore the benefits that online advertising confers on consumers. For example, Google and Facebook, two of the companies most vilified by privacy fundamentalists, are at the forefront of offering low or no-cost content, applications and services to consumers unimaginable a decade ago. Yet when these companies use targeted online advertising to fund their operations, privacy fundamentalists object. Unfortunately, these objections reflect the prevailing message of privacy fundamentalists that privacy trumps all other values. However, policymakers should recognize that privacy, as with any other value, must be balanced against other competing interests and can, as it will here, come at a real financial cost—fewer jobs, less investment, and less free content for users.

Current Privacy Tools Provide Consumers Various Means of Managing Their Privacy

Consumers today have many different options for controlling their online privacy that are more cost-effective than the Do Not Track proposal. Every major web browser includes many features to allow users to manage their online privacy settings, such as the use of cookies, and this is a continued source of innovation and differentiation among competing web browsers. Consumers can also download third-party web browser plug-ins like Adblock and NoScript which block online advertising. Internet users can also use new applications like Bynamite which provide individuals a third-party interface to the profiles maintained about users by online advertisers and allows users to change, delete or add to their list of interests for targeted online advertising (e.g. a user could specify that they are interested in receiving ads for the categories “politics” and “education” but not “cooking”).

Online advertisers are developing industry best practices to provide consumers with transparency and choice when using sites with targeted advertising. The Digital Advertising Alliance, an industry coalition, has created a self-regulatory program for online behavioral advertising, a

unique icon so consumers can identify interest-based ads, and an online tool to allow consumers to select their advertising preference for over 50 participating ad networks.³⁵ Individual ad networks have also created their own tools to allow users to manage their advertising preferences. For example, Google, a major online ad network, allows users to opt-out of targeted advertising using the DoubleClick cookie or through an optional opt-out plug-in for their web browser (the plug-in is available for Chrome, Firefox and Internet Explorer). Many third-party online advertisers, such as those belonging to the Network Advertising Initiative have also made a similar opt-out tool available online for users to more easily avoid targeted online advertising.³⁶ In other words, citizens increasingly have tools to ensure that online interactions occur on their own terms. And for the relatively small share of Americans who want to consume free Internet services while not allowing themselves to be served more relevant ads, these options for them to opt-out are sufficient.

Policymakers Should Pursue Privacy Policies That Foster Innovation

Do Not Track is an attempt by privacy fundamentalists to stop behavioral advertising which they find repugnant and invasive. Indeed, some of the “consumer advocates” behind Do Not Track seem to oppose advertising in general as predatory and anti-consumer.³⁷ 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.

Do Not Track does not actually solve the primary privacy concern that most people have: that their personal information will be used to unfairly harm or disadvantage them. If the goal is to protect consumers from harm, instead of a Do Not Track list, the government would be better off creating a Do Not Harm list. With a Do Not Harm list, organizations would not be permitted to take discriminatory or other harmful actions against individuals who register on this list. Imagine the possibilities: Do you not want your employer to fire you based on health information discovered about you online? Do you not want your bank to raise your credit card interest rates based on financial activity it managed to glean from your web browsing history? Do you not want the government to spy on your personal shopping history? Then sign up for the Do Not Harm list!

Of course it is clear that such a list is unnecessary—all citizens should be protected from basic discriminatory and harmful activities by businesses and government. Consumers ultimately care about how their data is used, not whether data is obtained by tracking Internet usage, consumer sales data or information that an individual discloses on a social networking site. It is impossible to eliminate all risk of a security breach and so some private consumer data will unfortunately always end up being exposed as a result of security failures. The goal should be to minimize the impact and frequency of these incidents. And that should be the purpose of government privacy regulations—to promote good security practices, to create and clarify the protections available to citizens, to define recourses available to them in case of a privacy breach, and to institute policies

that will minimize harms when sensitive data is known about them. Targeted advertising, like any other technology, will improve over time and it would be a mistake to halt the progress of such a promising innovation.

Conclusion

As data on individuals and their actions increasingly is collected and stored electronically, it is important for policymakers to consider the effect this has on privacy. This hearing provides a welcome opportunity to explore the best ways of protecting individual privacy while avoiding constraints on business innovation and unintended negative impacts on the economy, U.S. competitiveness, and consumers. Do Not Track would not be an effective tool to achieve this end because of its significant costs and shortcomings. Privacy is important, but it must be balanced against competing goals including usability, cost, future innovation and consumer benefits.

Notes

1. For a modern day example of misplaced privacy fears, see Daniel Castro, "I Spy a Luddite: Why the Lawsuit over Google Street View is Absurd," Information Technology and Innovation Foundation, Washington, D.C., April 25, 2008, <http://www.itif.org/files/WM-2008-03.pdf>.
2. John Neary, "Electronic Snooping—Insidious Invasions of Privacy," *Life Magazine*, May 20, 1966, http://www.bugsweeps.com/info/life_article.html.
3. Robert D. Atkinson, "RFID: There's Nothing to Fear Except Fear Itself," remarks at the 16th Annual Computer, Freedom and Privacy Conference, Washington, D.C., May 4, 2006, <http://www.itif.org/files/rfid.pdf>.
4. John Deighton and John Quelch, "Economic Value of the Advertising-Supported Internet Ecosystem," Hamilton Consultants, June 10, 2009, <http://www.iab.net/media/file/Economic-Value-Report.pdf>.
5. Daniel Castro, "Stricter Privacy Regulations for Online Advertising Will Harm the Free Internet," Information Technology and Innovation Foundation, September 2010, <http://www.itif.org/files/2010-privacy-regs.pdf>.
6. Robert Atkinson et al., "The Internet Economy 25 Years After .com," (Washington, D.C.: Information Technology and Innovation Foundation, 2010), <http://www.itif.org/files/2010-25-years.pdf>.
7. John Deighton and John Quelch, "Economic Value of the Advertising-Supported Internet Ecosystem," Hamilton Consultants, June 10, 2009, <http://www.iab.net/media/file/Economic-Value-Report.pdf>.
8. "IAB Internet Advertising Revenue Report," IAB, April 2010, <http://www.iab.net/media/file/IAB-Ad-Revenue-Full-Year-2009.pdf>.
9. "Interactive Advertising Revenues to Reach US\$147 Billion Globally by 2012, According to The Kelsey Group's Annual Forecast," press release, (Chantilly, VA: The Kelsey Group, 2008), <http://www.kelseygroup.com/press/pr080225.asp>.
10. "Number of Mobile Devices Accessing the Internet Expected to Surpass One Billion by 2013, According to IDC," IDC, press release, December 9, 2009, <http://www.idc.com/getdoc.jsp?containerId=prUS22110509>.
11. "Internet Advertising Revenues Hit \$5.9 Billion in Q1 '10, Highest First-Quarter Revenue Level On Record," IAB, May 13, 2010, http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-051310.
12. Robert D. Atkinson, "Federal Trade Commission Workshop on Journalism in the Digital Age," (Washington, D.C.: Information Technology and Innovation Foundation, 2010) <http://www.itif.org/publications/federal-trade-commission-workshop-journalism-digital-age>.
13. Jeff Jarvis, "History in the making in LA as online ads hit target," *The Guardian* [UK] 12 Jan. 2009, <http://www.guardian.co.uk/media/2009/jan/12/la-times-online-advertising>.
14. "YouTube channel earns college money for N.J. teen," *NJ.com*, 7 April 2009, http://www.nj.com/news/index.ssf/2009/04/youtube_channel_earns_college.html.
15. "Free Electronic Medical Record (EMR)," Practice Fusion, n.d., http://www.practicefusion.com/pages/free_ehr.html.

16. Jun Yan, Gang Wang, En Zhang, Yun Jiang, & Zheng Chen, "How Much Can Behavioral Targeting Help Online Advertising?" (Madrid, Spain: WWW, 2009), <http://www2009.eprints.org/27/1/p261.pdf>.
17. Howard Beales, "The Value of Behavioral Targeting," 2009, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.
18. Robert Atkinson, "Google E-mail, What's All the Fuss About?" (Washington, D.C.: Progressive Policy Institute, 2004) http://www.ppionline.org/ppi_ci.cfm?knlgAreaID=140&subsecID=288&contentID=252511.
19. Other similar technologies, such as web beacons (AKA "web bugs" or "tracking pixels") and Flash cookies (AKA "local shared objects") have also been criticized by some privacy advocates.
20. Data from author experiments on May 11, 2009.
21. Cookies enable a stateful web browsing experiences over HTTP—a stateless protocol.
22. Technically the cookie has an expiration date, but this can be set to a date beyond the expected lifespan of the computer.
23. Jon D. Leibowitz, "Consumer Online Privacy," Testimony before the U.S. Senate Committee on Commerce, Science and Transportation, July 27, 2010 and Julie Brill, "Remarks by Commissioner Julie Brill United States Federal Trade Commission," Proskauer on Privacy, October 19, 2010, <http://www.ftc.gov/speeches/brill/101019proskauerspeech.pdf>.
24. "Operation of the Do Not Track List," Center for Democracy and Technology, October 31, 2007, <http://www.cdt.org/privacy/20071031donottrack.pdf>.
25. One such implementation of an HTTP header is described here: Harlan Yu, "Do Not Track: Not as Simple as it Sounds," Freedom to Tinker, August 10, 2010, <http://www.freedom-to-tinker.com/blog/harlanyu/do-not-track-not-simple-it-sounds>.
26. The National Do Not Call Registry does not limit all telemarketing—calls from political organizations, charities and telephone surveyors are permitted as well as calls from organizations from which the consumer has purchased an item in the previous 18 months.
27. Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," (2010) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.
28. Sites like the Washington Post and the New York Times require users to register to access content. ArsTechnica ran an experiment where it blocked users who were running ad blocking software for 12 hours. Ken Fisher, "Why Ad Blocking is devastating to the sites you love," ArsTechnica, March 2010, <http://arstechnica.com/business/news/2010/03/why-ad-blocking-is-devastating-to-the-sites-you-love.ars>.
29. A sample post along these lines can be found here: <http://activerhetoric.wordpress.com/2010/11/08/do-not-track-means-do-not-track/>
30. Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," (2010) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.
31. Howard Beales, "The Value of Behavioral Targeting," 2009, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.
32. Robert D. Atkinson, Stephen J. Ezell, Scott M. Andes, Daniel Castro, and Richard Bennett, "The Internet Economy 25 Years After .com," Information Technology and Innovation Foundation, March 15, 2010, <http://www.itif.org/files/2010-25-years.pdf>.
33. Daniel Castro, "ITIF Comments on Draft Privacy Legislation," (Washington, D.C.: Information Technology and Innovation Foundation, 2010), <http://www.itif.org/files/2010-privacy-legislation-comments.pdf>.
34. Daniel Castro, "Data Privacy Principles for Spurring Innovation," (Washington, D.C.: Information Technology and Innovation Foundation, 2010), <http://www.itif.org/files/2010-privacy-and-innovation.pdf>.
35. "Opt Out From Online Behavioral Advertising (BETA)," Digital Advertising Alliance, n.d., <http://www.aboutads.info/choices/> (accessed On November 29, 2010).
36. "Opt Out of Behavioral Advertising" Network Advertising Initiative (NAI), http://www.networkadvertising.org/managing/opt_out.asp (accessed May 11, 2009).
37. "Online Behavioral Tracking and Targeting: Legislative Primer September 2009," Center for Digital Democracy, September 2, 2009, <http://www.democraticmedia.org/doc/privacy-legislative-primer>.

Mr. SPACE. And thank you, Mr. Castro.

That is our final panelist, and now Members will be permitted to ask questions.

And I would ask the chairman of this committee, Mr. Rush, if he intends to use his time.

Mr. RUSH. Thank you, Mr. Chairman.

And before I ask the question, let me also join with previous commentary from those on the subcommittee in thanking you for your outstanding service to this subcommittee. You have been a very valuable part of this process that we are now engaged in and have been engaged in. And I certainly have always welcomed your friendship and your leadership, your insight and your commitment to the affairs of the American people. So congratulations on an outstanding job that you have done.

And I do have just a couple of questions that I want to ask a couple of the panelists.

On October the 4th, 2010, the Council of Better Business Bureaus, a group of the Nation's largest media and marketing trade organizations, announced their "Self-Regulatory Principles for Online Behavior Advertising." They also launched an industrywide "Advertising Option Icon," which was to be displayed on Web pages that collect user information for behavior advertising.

Now, I have to ask Ms. Grant and Ms. Gillman, Mr. Pasqua and Mr. Castro, I am going to ask you two questions, and you can take your time to answer these questions.

Have you had the opportunity to review the new consumer opt-out platform? And, two—which is part of the advertising alliance that was released on the said date?

And the second question is, in its current configuration, what are some of the consumer opt-out platform's limitations? What are the limitations of the opt-out platform?

Ms. Grant, I will start with you, and we will just go down the line.

Ms. GRANT. I have read the principles and the explanation for them for this new program, actually several times because it is extremely complicated. It was supposed to actually be launched in July. I don't believe that it is really functioning yet, at this point, so I don't think that we can tell much about how it is going to work.

But one thing that troubled me was that there were many different options that companies had for, for instance, how they would explain to consumers what they were doing with their information, who was responsible in the chain of companies for doing this, where consumers would go to opt out, whether to a central Web site that some companies but not all companies would use or to individual companies' Web sites.

I found the whole thing very potentially burdensome for consumers. And I don't think that it is the one-stop-shopping, easy mechanism that we are looking for.

Mr. RUSH. Ms. Gillman.

Ms. GILLMAN. Yes, I did read it, but it was some time ago. I will tell you that we applaud the initiative that they took. The issue is complex, and I think it is early days; it is too soon to actually judge the effectiveness.

I think a lot of the complexity is that many of the participants have very different businesses and systems, and they are trying to figure out the best way to do this. And no one today knows the best solution. So the fact that they are trying, I think, is heading in the right direction.

I would also—you asked about limitations. I think it is time, it is consumer education, and it is applying many of these best practices and really learning from them. So it is just time, at this point, that is the limitation.

Mr. RUSH. Mr. Castro.

Mr. CASTRO. Thank you.

Yes, I have had a chance to review it. I would say the limitations are that obviously it is in its nascent stages, but, when you look at it, you know, this is certainly an iterative process, as all technology improvements are. And if you see the progress they have made in the past 6 months to a year to 5 years, I think, you know, it is very good.

One thing that I think is important when you evaluate these solutions, you know, they don't have to necessarily come up with the best solution. They just have to have a platform that other people can apply a good solution to. In that sense, they are making a lot of progress.

And the other main limitation that I see is that this is obviously only one type of advertising, display advertising on Web sites. You know, we need to look broadly at creating a fair platform so that all types of online advertising can be competitive.

Mr. RUSH. The CFA has said before that, quote, "Online opt-out should be as well-known and as easy as the Do Not Call list," end quote, and that a Do Not Track list should be aimed at preventing tracking for, quote, "advertising purposes."

Can you be more specific in terms of what you mean by "advertising purposes"? Can you be more precise about it? What of these online tracking tools and technologies would be permitted and they don't fall into, quote/unquote, "advertising purposes"?

Ms. GRANT. Well, we have heard today that there are already some solutions out there for consumers. It is not clear how widely known they are. And, in some cases, there are things that consumers have to pay for to protect their privacy.

It is a challenge whenever you are educating consumers. You have to have very simple, central messages to give them, and you have to have very practical, easy things for them to do.

Right now, if I was advising a consumer about how to avoid online tracking, I wouldn't be able to give that person very easy, practical advice about what to do, because there is not one easy-to-do thing, as we are advocating with a Do Not Track mechanism. There are various things out there that have their pros and cons, all of which people have to download or take various steps to do, not as easy as flipping the switch that we envision on one's browser with a Do Not Track mechanism.

Mr. RUSH. Ms. Gillman, would you take a stab at it from your perspective, in terms of what is—would you more precisely define "advertising purposes"?

Ms. GILLMAN. Can you actually rephrase the question? Because I would like to make sure—

Mr. RUSH. OK, let's try to define, quote, "advertising purposes" with a little bit more precision. What other uses of these online tracking tools and technologies would be permitted as not falling into, quote, "advertising purposes"?

Ms. GILLMAN. Oh, you are asking what would not be considered advertising use?

Mr. RUSH. A more precise definition of what an advertising purpose would be.

Ms. GILLMAN. I am not a lawyer, so trying to actually draft that language is challenging. I think it is worth a deep discussion. Today, the advertising industry is a large industry, \$250 billion. It encompasses communication with consumers through direct mail, through advertising in terms of display advertising. And the information that is often used to inform those campaigns is information that, you know, can cover purchase information and it can cover interests that they know about that individual, publicly available information about their college education, their level of education, their income.

So, to me, the information that might be needed to be used is broad. But most, if not all, major advertising initiatives today do not actually need to use personally identifiable information to deliver marketing messages on the Web. So I don't know if that addresses it, but it is a lot of blended information, depending on the business.

Mr. RUSH. Ms. Grant.

Ms. GRANT. Can I take a stab? Because I may not have understood your question properly.

Beyond the demographic information that is often used in advertising to target it to certain markets, increasingly we are seeing more sensitive kinds of information used—health information, other information—to do exactly what we have heard described, to personalize the advertising.

And there are great concerns about that. There may be some people who are not troubled by that, but we know that there are a lot of other people who are, and that those people need an easy-to-use tool to prevent that kind of information from being collected if they don't wish it to be.

Mr. MOGLEN. Mr. Chairman, may I comment?

The purpose of advertisers is to collect information concerning the capabilities and intentions of the potential buyer and to affect that buyer's behavior. Oddly enough, those three points—collection of information about capabilities and intentions for the purpose of affecting behavior—is also the definition of what intelligence services do. There is, in fact, no practicable distinction between the public activity we call "collecting intelligence" and the private activity we call "targeting advertising." They are both spying.

The purpose of spying has got to be one which the public would find in its advantage and not merely in the advantage of the institution performing the spying. We do that with respect to public intelligence services because they are under democratic control. We don't do that with respect to advertisers. They are under nobody's control but their own, unless they are regulated.

Thank you.

Mr. RUSH. Well, thank you.

I yield back.

Mr. SPACE. Thank you, Mr. Chairman.

Thank you, also, for allowing me the opportunity to chair this hearing. This seat is much more comfortable than I imagined.

The chair recognizes Ranking Member Whitfield from Kentucky.

Mr. WHITFIELD. Mr. Castro, you just heard Dr. Moglen's comment about advertising. And I was just curious, would you have any comment to what he just said?

Mr. CASTRO. Sure, absolutely. I mean, I think it is actually inaccurate. Spying is very different. Spying, you know what somebody is doing very specifically; it is identifiable. It is implied that it is harmful.

In this case, what is happening for most targeted advertising, most of the collection and use of information online—you know, when we are talking about this problem, 95 percent of everything that we talk about is things that most people are comfortable with. It is this, kind of, 5 percent gray area that is the exception.

But, you know, overall there are a lot of good things that are being done with this data and good things that are helpful to consumers. You know, data is collected and used so that Web sites are more accessible, more usable, they are displaying more accurate information. Information is collected so that search engine rankings can be improved. Data is collected, you know, of course, to do targeted advertising. And all of these things help users, and I don't think most consumers would consider that they are spied on when they are given something that they want.

Mr. WHITFIELD. Would you like to respond to that in any way, Mr. Moglen?

Mr. MOGLEN. Well, it seems to me that it heightens, again, the point that thinking about targeted advertising in isolation is probably not a good idea. But if Mr. Castro is correct, we could test it with a very simple regulatory approach which would simply require businesses to disclose to consumers on request everything the business knows about them and what they have done with it. Then we will find out whether people are comfortable with what actually happens as opposed to what they can see.

Online advertising firms are very secretive in their nature. I don't compare them lightly to intelligence services. They both protect very jealously their methods of collection of information and analysis, and they both protect very jealously what they do with the information that they have.

I think, if Mr. Castro is correct that what is actually going on would be acceptable to consumers, then there ought to be no objection to regulation that would require consumers to have the power to get exact information about what is known about them and what is done with what is known.

Mr. WHITFIELD. Yes.

Mr. CASTRO. Sir, I would like to respond to that.

Of course, the issue that we are talking about today and the broader issue with online tracking and implementing Do Not Track is there are lots of costs involved. So the question is always, is the cost necessary and appropriate?

I do absolutely agree that, you know, broadly speaking, we do want government to look out for consumers' privacy rights. One

way of doing this is looking specifically at harms—what harms are out there and how can we prevent harms from occurring. Because it doesn't matter to the consumer how somebody got data about them. They care if something bad happens to them. They care if somebody is discriminating against them or their information is being used in a harmful way. And so I think that is a very appropriate way that Congress can address these kinds of privacy concerns that are out there.

Mr. SPACE. OK. And the ranking member had to step out, so I will reserve his 2 minutes and 13 seconds.

And that leaves me. I do have some questions I would like to ask.

Dr. Moglen, actually, you said something during your response to one of the questions I think asked by Chairman Rush—and while you equated the act of surveillance or tracking to spying, I am not sure I would agree with that. But you did say something that I think really gets to the heart of matter, and that is, who benefits from it?

And I have heard testimony today from various people that not only does the advertiser or the digital company that is engaging in the tracking benefit, but there is some suggestion that consumers benefit, as well, specifically not just in terms of convenience but it allows, for example, low-income consumers easier access because of cheaper costs. Perhaps the argument could be made that it could allow telecommunication companies the flexibility of extending or expanding their networks to serve underserved and unserved areas.

And I am curious—I am going to ask Mr. Castro—whether you have any qualifiable, measurable data that would provide us with details on how tracking legislation or an overall blanket prohibition would affect the business model within the industry.

And then I am going to ask you, Ms. Grant, the extent to which you are concerned about the economic consequences of legislative action that might prohibit this kind of activity as it relates to the business model of the telecom companies and their ability, then, to reach and provide services to low-income and rural—or unserved customers.

Mr. CASTRO. Yes, so, you know, would this affect the industry? Certainly, when you look at the numbers, there are two numbers you have to look at. One is how much is being spent now and then what the trends are, so how much will be spent in the future.

There have been studies on, of course, the effectiveness of online advertising and the impact of regulations. And I point to the study by Tucker and Goldfarb from MIT and University of Toronto that looked at the impact of the European privacy directive. And that study did find a loss in effectiveness.

And what they did as the next step was they said, you know, what would that impact be if advertisers changed their spending in direct correlation to the effectiveness of the ad, which is, you know, a very logical thing. So they could either increase their spending, you know, and double the number of ads and get the same effectiveness or decrease it in line.

So if they decrease it—and I think this was applied to the U.S. economy—if it was decreased, it would be something like a loss of revenue of about \$5 billion.

Mr. SPACE. Five billion dollars?

Mr. CASTRO. Five billion dollars. It was from around—I can pull out the number in a minute, if you would like the exact—it was over \$5 billion.

Mr. SPACE. Whose estimate was that?

Mr. CASTRO. This was Tucker and Goldfarb from the University of Toronto and MIT.

Mr. SPACE. Who commissioned this study, or was it an academic—

Mr. CASTRO. It was an academic study.

Mr. SPACE. All right.

Ms. Grant, having heard those numbers, \$5 billion is a lot of money and, not just conceivably but in all probability, might affect the ability of low- to middle-income consumers to obtain access and, again, underserved or unserved consumers to obtain access.

What is your response to those monetary concerns?

Ms. GRANT. Well, first of all, if I understand correctly, this was a study of the EU privacy directive. So I don't think that it is exactly on point.

I don't know what the impact of Do Not Track would be on telecom companies. But I would like to say a few things that I think would be helpful here.

One is that we are not talking about no advertising. There are consumers who might not avail themselves of Do Not Track so would continue to receive tailored advertising. There are consumers who now and in the future will continue to get contextual advertising, which is based on what they are looking at at the time on the Internet and doesn't involve following them around and compiling a dossier of what they do and who they talk to.

And consumers find information on the Internet about the products and services that they want in other ways, as well. They do it using search engines. They do it using price-comparison Web sites.

So there are lots of ways that people find what they are looking for online. And behavioral advertising is one part of this, but it is certainly not the main or only part. And I don't think that doing away with it will have a—or not doing away with it, but giving consumers control over whether they want to be tracked or not will create a great economic upheaval or turn the Internet dark overnight.

I am sure that the Federal Trade Commission wouldn't be supporting the concept of a Do Not Track mechanism if it felt that it would have that effect either. We are all very concerned about the economy and making sure that it is strong and that e-commerce continues to grow, but we don't want to sacrifice consumers' privacy.

We don't let companies do whatever they want just because it is profitable. I am sure that bombarding consumers with telemarketing calls was probably effective even though a lot of people didn't like it. It made money. But we drew the line. We drew the line in terms of time of day that telemarketers could call con-

sumers, that they couldn't call with annoying frequency. And then we gave consumers a tool to actually use to reduce unwanted telemarketing if they chose. And that is the kind of thing that we are talking about here.

Mr. SPACE. Thank you, Ms. Grant.

Mr. MOGLEN. May I comment, Mr. Space?

Mr. SPACE. Yes, in one moment, Dr. Moglen. I am going to call on you to comment.

But I would like to know from Ms. Gillman whether Time Warner, for example, can quantify and give us some indication as to how this affects your business model and your ability to provide cable services to consumers at current pricing. Have you done studies? Is there any measurable data that we can look at?

Ms. GILLMAN. We have not done a study that looked at that specifically. But I can speak to the fact that we need to innovate every day to adapt to consumer interests, consumer needs. They look to us to make improvements to our service every day. And this debate being a very important debate, the risk one runs is that there are unintended consequences of a Do Not Track policy, in that it prevents companies like ours from innovating.

I would also like to add, though, that the vibrancy of the Internet is extremely important, as well. And what should be explored around this debate and discussion is really the unintended consequences for the smaller content providers and service providers, the small businesses in and around this ecosystem. The smaller the Web site, the smaller the audience, the more challenging times they have selling contextual advertising. So they do not have a large enough audience.

So we really want to encourage innovation in the Internet ecosystem, and we want new players entering. And we want to make sure that any discussion around this debate does not prevent that from happening.

Mr. SPACE. OK.

Dr. Moglen, you have the last word.

Mr. MOGLEN. I very much doubt, Mr. Chairman, that there is any person in this room whose life has not been altered by Wikipedia, which has provided opportunities for underserved populations of the kinds that you were talking about to conduct research and to learn at a level which is otherwise inaccessible to them.

Wikipedia is unsupported by advertising. And of the 100 most visited sites on the Net studies by the Wall Street Journal in the series previously referred to, it was the only one of the 100 not in any way surveilling or tracking its users.

I think, once again, that the attempt to connect the advertising business model to the importance of vibrant content on the Net or life-changing possibilities of expansion of access to underserved populations is poppycock.

Mr. SPACE. OK. With that, does the chairman have any additional questions?

Mr. RUSH. Mr. Chairman, in the interest of time, I am going to just pass, because I think that you and the other members of this panel have been here for quite some time. And I would be taking

advantage of my freshness, my first legs if I were to ask another question, so I am going to pass.

Mr. SPACE. Thank you, Mr. Chairman.
And Ranking Member Whitfield?

Mr. WHITFIELD. How do you spell "poppycock"?

Mr. SPACE. Yes, how do you spell "poppycock"?

Mr. MOGLEN. I will modify my remarks to spell it out. Thank you.

Mr. SPACE. All right. With that, this hearing is adjourned.

[Whereupon, at 2:34 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

**Statement of Rep. Henry A. Waxman
Chairman, Committee on Energy and Commerce
“‘Do-Not-Track’ Legislation: Is Now the Right Time?”
Subcommittee on Commerce, Trade, and Consumer Protection
December 2, 2010**

Thank you, Chairman Rush. I would like to commend you for your continued leadership on the issue of consumer privacy. Through your work on this Subcommittee, and in conjunction with Mr. Boucher’s work on the CTI Subcommittee, you have helped shine the spotlight on the growing trade in consumers’ information both in the online and offline contexts and the privacy concerns that this ever more pervasive collection and use of information could raise.

Mr. Whitfield and Mr. Barton have also shown a keen interest in privacy issues, and I appreciate their contributions to this ongoing dialogue.

Although we will each find ourselves in different roles in the next Congress, I look forward to continuing our work together next year on this issue. I believe that this is an issue on which we might be able to work across party lines.

For today, I think there's one thing most of us can agree on: the pervasiveness and invasiveness of information collection about consumers has grown to levels that warrant our close attention.

This is happening both offline and online, but our focus today is the online context. The Internet is a remarkable tool. It has made the world more open and interconnected. It helps us share information in ways and to a degree that none of us could have ever imagined. It has also become a key driver for our economy. The innovations sparked by the Internet have been positive. And we must be careful not to stifle this innovation.

The Internet has dramatically increased the availability of consumer information. And it has done so in ways that a lot of people don't know about. A lot of consumers don't know it, but they are being followed from website-to-website by a growing tracking industry intent on decoding their interests, wants, and needs in order to pedal products through so-called behaviorally targeted advertising.

I appreciate that the reasonable collection and use of information can provide benefits to both consumers and businesses. Consumers can get advertising that is actually relevant to their wants and needs. Businesses with products to sell get access to consumers that are more likely to be interested in buying from them. Moreover, targeted ads are part of a larger online advertising revenue stream that helps online publishers continue to supply consumers with mostly free content.

So we face a complicated balancing act with respect to making sure consumers' expectations of privacy are respected and the desire to let the Internet continue to flourish and innovate. Both are important goals. I look forward to hearing the views of both panels on how we might achieve that balance, whether these two things have to be competing goals, and where something like a "Do Not Track mechanism" fits in this debate.

I would like to thank the witnesses from both panels for being here today.

I would also note that yesterday the FTC made public its proposed framework for protecting consumers' privacy. I understand we will soon see something from the Department of Commerce expressing the Administration's views regarding Internet privacy.

These reports have been the result of a very long process with input from a large number of interested stakeholders. I expect that both of these reports will help inform our work here. Yet both are in proposal form, and call for even more feedback from stakeholders. There is a point where dialogue has to come to an end, and we have to move forward with concrete action in some form. It's my hope that the FTC and the Administration will move quickly to finalize their views and recommendations on this issue.

As we do move forward on the issue of privacy, I'm optimistic we can work in a bipartisan fashion with all members of the Committee. And I hope that this will be just one of many areas where we will be able to work together in the next Congress.

Statement of
Representative John D. Dingell
Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection
Hearing on “Do Not Track Legislation: Is Now the Right Time?”
December 2, 2010

Thank you, Mr. Chairman, for convening today’s important hearing. I am pleased that the hearing, as its title suggests, is exploratory in nature. I have many questions concerning the matter of data privacy, and in particular the question of potential “do not track” requirements, just as I suspect my colleagues on this subcommittee do.

I have long held that Americans have a reasonable right to privacy and consequently sought to incorporate this belief in all manner of legislation. The great success of the “Do Not Call List” would have us believe, *prima facie*, that a compelling argument for a similar requirement related to Internet privacy might be made. Nevertheless, and with the benefit of several years’ experience in these matters, I suspect a more nuanced approach may be warranted, especially given the inherent complexity of the Internet. As the Architects say, God resides in the details.

With this in mind, I intend, with the assistance of our witnesses today, to achieve a measure of understanding about the function and effects of “do not track” requirements. Specifically, I will ask witnesses to offer their opinions about the following broad issues:

- What impact will privacy regulations, whether “do not track” or otherwise, have on the way consumers presently enjoy the Internet;
- How will such requirements engender uniform consumer protections, especially given that a single user may access the Internet using many different devices; and
- Should industry be left to regulate itself with respect to data privacy, or is legislation required, and if so, what shape should such legislation take?

In closing, I note that no federal law comprehensively governs the collection, use, and dissemination of consumer information. I urge my colleagues to adopt the view that if “do not track” requirements become necessary, their implementation should come at the direction of the Congress.

I thank the Chairman for his courtesy and yield the balance of my time.

**Statement of the Honorable Joe Barton
Ranking Member, Committee on Energy & Commerce
Hearing on “‘Do-Not-Track’ Legislation: Is Now the Right Time?”
December 2, 2010**

I'd like to thank Chairman Rush for convening us to hear more about a 'Do-Not Track' Registry for online advertising. While I'm not sure that I support this particular approach because it would put Congress in the job of picking web browser functions, I certainly agree with the privacy principles behind it. Consumers should have control and notice over the use of their own, personal data.

As we all know, the Internet has evolved and transformed financial services, news, social networking, and entertainment. This new cyber-world brings many new opportunities for marketing goods and services, and one way that businesses connect with likely customers is through behavioral advertising. Tracking a person's behavior across various sites and searches allows companies to build profiles and try to turn a broad population of consumers into their paying customers. Additionally, as The Wall Street Journal reported this summer, some companies now exist purely to gather and sell consumer profile data to marketers. It may be brilliant marketing, but doesn't it also debase a person's inherent right to privacy and personal data ownership?

There is no doubt this system of delivering relevant advertising has the potential to benefit all parties involved. For e-commerce retailers, it can allow their

advertising dollars to be spent far more effectively, efficiently, and profitably. For consumers, it allows them to take fuller advantage of an electronic marketplace tailored to deliver more of what they actually want. Finally, tracking and targeting advertising can benefit every kind of content provider from bloggers to small businesses by turning efficiency into profits. The more businesses that do well, the more consumers will benefit from increased competition. But again, the question is whether people should be made to sacrifice their own privacy for commercial efficiency?

For the consumer, the benefits are accompanied by serious risks. User data -- whether aggregated or anonymous -- can be exploited by unscrupulous actors both on and off the Internet. Recently, we learned that users who provided personal information to a popular social networking site had their personal data transmitted to advertisers by third-party applications without the users' knowledge. In that situation, users at least knew what information they had provided. But in most areas of the Internet, the default setting is often that one's data is collected, stored, used, and sold with little or no notice of what's being collected, who's storing it, how it's being used or to whom it is sold. Surely most consumers have never heard of the majority of the companies that are building and selling their online profile to other companies.

I also want to reiterate that I support and encourage nearly every tool created by the free market to bring goods and services to people at lower cost. I am encouraged that some companies are developing ways to give consumers more control over their information, but no one should be happy that their number remains so small.

I believe consumers need to know how their data is being collected and used before that collection and use occurs, not after they're advised of a threatening security breach. As I stated earlier, a custom-made Internet can benefit all participants in e-commerce, but only if consumers know the risks and benefits and have the opportunity to choose how much benefit they want and how much risk they willing to take. In the current paradigm, I believe the user is not fully offered that chance.

Finally, as a proponent of free markets, I believe we should work with the private sector to achieve our privacy goals. Government intervention typically has perverse unintended consequences that can do more harm than good. While the concept of a 'Do-Not-Track' registry is inspired by our own, very successful 'Do-Not-Call' Registry, on-line tracking and targeted advertising are packed with hazard where unwanted telemarketing was more maddening than dangerous. That being said, I thank Chairman Rush for holding this hearing and advancing the

conversation about online privacy. I look forward to hearing the witness' testimony and I yield back.

Congressman John Barrow Committee Statement 12/2/10

Thank you Mr. Chairman.

I'm glad the Subcommittee is holding this hearing on the critical issue of online privacy and data tracking. The technological advances of the last few decades have been an incredible boon to our economy and our way of life. But every advance in technology poses a new challenge. One of those challenges is that so much of our critical personal information is exposed to others.

Many of us have read the reports about online information gathering and the extent to which Internet user activity is being monitored. In this age of information tracking and data mining, it's important to know "who knows what," and what is being done with personal information and records we'd rather not disclose.

As the tracking industry grows, we have a responsibility to do all we can to make sure that individual citizens maintain control over their own privacy. I believe that today's hearing is a step in that direction, and I look forward to hearing today's witnesses address these concerns.

Thank you.

Opening Statement

Congresswoman Mary Bono Mack

December 2, 2010

Subcommittee on Commerce, Trade and Consumer Protection

hearing on

“Do Not Track Legislation: Is Now the Right Time?”

Good Morning Chairman Rush, Ranking Member Whitfield and distinguished panel. Thank you for holding this hearing on this important topic.

I appreciate the fact that the Subcommittee is taking time to give attention to the subject of online privacy. As more commercial activity and communication is conducted online – it’s important we work to make consumers aware of these issues.

As a matter of context, on multiple occasions I have brought forth legislation to address consumer safety online.

Specifically, I was the first to advocate for legislation to combat harmful spyware and, more recently, the first to put forth legislation to call consumers attention to the potential harm being caused by ‘Peer to Peer’ software. So I do take

consumer privacy in the online space seriously and have shown a willingness to act when necessary and feasible.

My experience in crafting these legislative solutions - which I must note are immensely complex and technical - has taught me that we must be extremely thoughtful and respect the law of unintended consequences. The magnitude of this issue is made clear in the Wall Street Journal series on this topic.

Technologies that benefit individuals and industries continue to develop at an increasingly rapid pace and there is no going backward. Our role should be to help ensure that there is an appropriate balance between informing and protecting consumers and respecting the dynamic and constantly evolving world of e-commerce and personal communications. Make no mistake, law breakers should be held accountable and consumers should have the ability to make informed choices that protect their privacy; but, at this time, I am not convinced that an overly broad regulatory or legislative remedy is the appropriate policy approach.

It is important that we fully analyze the issues before us to determine the best path forward, and I look forward to today's discussion.



UNITED STATES DEPARTMENT OF COMMERCE
National Telecommunications and
Information Administration
Washington, D.C. 20230

February 3, 2011

The Honorable Henry A. Waxman
Ranking Member
Committee on Energy and Commerce
House of Representatives
Washington, DC 20515

Attention: Jennifer Berenholz

Dear Representative Waxman:

Thank you for your letter of December 28, 2010, forwarding questions for the record for the December 2, 2010, hearing of the Committee's Subcommittee on Commerce, Trade and Consumer Protection entitled: "Do Not Track Legislation: Is Now the Right Time?"

My responses to the questions are enclosed. If you or your staff have any additional questions, please do not hesitate to contact me or James Wasilewski, NTIA's Director of Congressional Affairs, at (202) 482-1551.

Sincerely,

A handwritten signature in black ink, appearing to read "Daniel J. Weitzner", with a long horizontal line extending to the right.

Daniel J. Weitzner
Associate Administrator
Office of Policy Analysis and Development

Enclosure

**Questions for the Record for NTIA Associate Administrator Daniel J. Weitzner
December 2, 2010 Hearing before the House Subcommittee on Commerce, Trade, and
Consumer Protection**

The Honorable Henry A. Waxman

1. The House of Representatives on December 8, 2009, passed H.R. 2221, the “Data Accountability and Trust Act,” and sent it to the Senate – which has failed to act on the legislation. The Department of Commerce’s Internet Policy Task Force in its green paper addressing online privacy issues recommends: “Consideration should be given to a comprehensive commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows States to build upon the framework in limited ways.”

- a. Section 3 of H.R. 2221 provides for notification of an information security breach. Among other things, Section 3 requires, following the discovery of a security breach, any person engaged in interstate commerce that owns or possesses data in electronic form to notify the FTC and each individual whose personal information was acquired or accessed as a result of the breach. A person is not required to provide notice if he determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct. In the Question for Further Comment on this issue, the Task Force asks “what factors should breach notification be predicated upon?” Do you believe there are factors other than those contained in HR 2221 upon which notification should be predicated and included in a comprehensive security breach notification law?

A comprehensive national approach to commercial data breach must provide clarity to individuals regarding the protection of their information throughout the United States, streamline industry compliance, and allow businesses to develop a strong, nationwide data management strategy. Consistent with this approach, the Department of Commerce supports legislative measures that generally require any person or third-party agent that owns or possesses data in electronic form containing personal information to notify each individual whose personal information was acquired or accessed, as a result of a breach of their system’s security.

At this point, the Commerce Department has not formulated a complete list of factors upon which data breach notification should be predicated. In its recently released report, entitled Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (“Green Paper”), the Commerce Department’s Internet Policy Task Force (“Task Force”) has asked for input on such factors. All comments were due no later than January 28, 2011. Once the Task Force reviews public comments to this Green Paper recommendation, it plans to contribute to an Administration position, and the Administration looks forward to sharing our views on any additional factors other than those contained in H.R. 2221.

- b. Section 2 requires certain entities that are engaged in interstate commerce that own or possess personal information, or that contract with a third-party to

maintain such data, to establish and implement information security policies and procedures in compliance with regulations to be set by the FTC. The regulations must require policies and procedures regarding: (1) collection, use, sale, other dissemination, and maintenance of personal information; (2) identification of an officer or other individual responsible for management of information security; (3) identification and assessment of any reasonably foreseeable vulnerabilities in data systems, including regular monitoring for a breach of security of such systems; (4) preventive and corrective action to mitigate any foreseeable vulnerabilities; (5) disposal of electronic data containing personal information; (6) destruction of paper documents and other non-electronic data containing personal information. Some businesses could be determined by the FTC to be in compliance with the requirements of section 2 if they are currently in compliance similar federal regulations to maintain standards and safeguards for information security. Do you believe the policies and procedures called for by H.R. 2221 cover the areas that strict data security protocols would encompass?

Information and communications networks are largely owned and operated by the private sector, both nationally and internationally. Thus, addressing computer and network security issues requires public-private partnerships, with the relevant government agencies working together with the private sector to develop clear guidance on safeguarding personal information. The Department of Commerce greatly appreciates your leadership in crafting policies and procedures for stricter data security mechanisms and section 2 of the legislation provides a solid foundation for further discussions. Moreover, once the Task Force reviews stakeholder comments on the Green Paper, we plan to contribute to an Administration position and look forward to sharing additional views on data security legislation in the future.

- c. **Section 6 provides for preemption of any provision of a state law that expressly requires information security practices and treatment of data containing personal information similar to any of those required under section 2 and requires notification to individuals of a security breach resulting in unauthorized access to or acquisition of electronic data containing personal information. This section is intended as a limited form of preemption. To what extent do you believe a comprehensive data security breach law should preempt existing state laws? Please explain what the Task Force meant when it stated that states should be allowed to build upon a comprehensive data security breach framework “in limited ways”? Can you provide information regarding costs to businesses specifically attributable to variations in state security breach laws? Can you provide specific example of other burdens on businesses resulting directly from variations in state security breach laws?**

Once the Task Force receives public comments to this Green Paper recommendation, it plans to contribute to an Administration position and we look forward to sharing our views in the near term. As part of our process, we are consulting with State Attorneys General, so that we have the benefit of their views on these issues during our deliberations.

Generally, nearly all of the NOI comments that addressed Federal laws or regulations favored preemption. Agreement on this issue crystallized around state security breach notification laws. The National Business Coalition on E-Commerce and Privacy, for example, was unequivocal in its recommendation, framed by the fact that nearly every State has its own state security breach notification laws, stating: "Our members are happy to comply with whatever policies are enacted into law, but they simply do not wish to have to comply, nor should they have to, with an ever-shifting 'patchwork' of different State laws that can actually change, as between the various States, several times in any given year." (Comment of Coalition, 4.)

In the Green Paper, the Commerce Department expressed support for consideration of a comprehensive data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows States to build upon the framework in limited ways. Overall, the many State laws, and years of experience with them, provide valuable data for constructing a federal law. Along with the Federal Trade Commission, individual States should have the authority to enforce any framework. We would consider giving States latitude to add requirements of particular concern for their jurisdictions provided they are consistent with national standards.

- d. **Do you believe that H.R. 2221 embodies the type of comprehensive data security breach framework envisioned by Task Force? Are there any additional elements not included in H.R. 2221 that should be included in a comprehensive data security breach law? Are there any elements included in H.R. 2221 that should not be included in a comprehensive data security breach law?**

Consistent with H.R. 2221, the Commerce Department's Green Paper recommends the consideration of a national commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows States to build upon the framework in limited ways. Once the Task Force has had an opportunity to review and assess stakeholder reactions and comments to the Green Paper, we plan to contribute to an Administration position and the Administration looks forward to further sharing our views on H.R. 2221 with your Office.

- e. **Do you believe that measures to protect personal information collected and maintained by commercial entities should be treated and considered separately from measures to protect personal information maintained and collected by government entities?**

The Green Paper's recommendations apply solely to personal data in the commercial context. The report does not contemplate changes to the Federal Privacy Act. These issues present different concerns, with different regulatory environments.

2. **The Task Force in its green paper states: "Focusing on the principles of purpose specification and use limitations can help to align [information] practices with [consumer] expectations. Purpose specification and use limitations would not involve externally imposed, prescriptive rules that govern how companies can use**

personal information. Rather, they would require companies to provide clear notice of their practices and would prevent companies from deviating from the purposes and uses to which they commit. . . . The combined forces of the purpose specification and use limitation principles stands in contrast to the related principles of collection limitation and data minimization.” Do you believe there are any mandatory use limits that should be included in a privacy policy framework? Do you believe collection limitation and data minimization principles have a role to play in a privacy policy framework? Please explain.

The Green Paper describes a broad range of U.S. privacy laws. There is certainly a role for statutory use limits when data is very sensitive or when serious harm results. As illustrated by the Fair Credit Reporting Act (FCRA), which limits the use of a consumer’s credit report to certain purposes, the Health Insurance Portability and Accountability Act (HIPPA), which limits certain uses of a patient’s health information for patient care and related purposes, and the Genetic Information Nondiscrimination Act (GINA), which prevents a person’s genetic information from being used for health insurance and employment purposes, mandatory use limits for information can help foster a robust and dynamic privacy policy framework.

Along with use limitations, the Commerce Department has recommended that the following fair information practice principles receive a high priority: enhancing transparency, encouraging greater detail in purpose specifications, and fostering the development of verifiable evaluation and accountability programs.

Finally, the Green Paper should not be read to suggest that collection limitation and data minimization should be left out of a FIPPs-based commercial data privacy framework. FIPPs are, to some extent, interdependent and the Commerce Department recommends that collection limitation and data minimization principles have a role to play in a privacy policy framework.

3. **The green paper recommends that “[v]oluntary, enforceable codes of conduct should address emerging technologies and issues not covered by current application of baseline FIPPs.” It suggests that the FTC could enforce those voluntary codes or baseline FIPPs where there is no voluntary code in force. In addition, the green paper throughout its discussion and inquiries on this issue seems to suggest that the FTC might be able under its current authorities to enforce FIPPs. For example, the green paper states in a question for comment: “Should FIPPs be considered an independent basis for FTC enforcement, or should FTC privacy investigations still be conducted under Federal Trade Commission Act Section 5 “unfair and deceptive” jurisdiction, buttressed by the explicit articulation of the FIPPs?” Can you please clarify whether you are suggesting that the FTC currently has the authority to enforce FIPPs against organizations that decline to be bound by voluntary codes? If so, can you please explain why you believe the FTC has the authority to enforce FIPPs either independently or under Section 5? If the FTC lacks this authority, how could it act as the enforcer envisioned in the green paper?**

The Commerce Department recommends that the FTC remain the consumer privacy enforcement agency for the U.S. Government. As one option, the Department notes that baseline commercial

data privacy legislation could give the FTC a specific statutory basis for bringing privacy-related enforcement actions to enforce FIPPs against organizations that decline to be bound by voluntary codes. Either way, the FTC's enforcement authority will remain integral to commercial data privacy protections. Thus, the Department's Green Paper posits a series of questions to stakeholders about possible legislative enhancements to the FTC's enforcement authority.

The FTC's current commercial data privacy enforcement authority is based on its jurisdiction under the Federal Trade Commission Act Section 5. Existing FTC statutory authority enables the Commission to investigate data collectors that violate their stated privacy policies or codes of conduct, but the Commission does not, as a general matter, have the authority to require a given company to adopt a particular code of conduct. The discussion at pages 51-52 of the Green Paper raises and discusses issues concerning FTC commercial data privacy enforcement authority, should a legislative proposal for baseline FIPPs in the commercial context emerge. It is in the context of this possible legislative development that the question about the FTC's Section 5 authority, versus other authority to enforce FIPPs, is best understood.

4. **The green paper states: "If [Privacy Impact Assessments] were published, they would provide consumers with a road map to an organization's collection and use of personal information." It also states that "a revitalized set of FIPPs, coupled with a PIA requirement...would provide more uniform commercial privacy protection across industries and data uses." The green paper nonetheless stops short of expressly calling for the requirement of PIAs and instead ponders potential incentives to encourage their use. Are there concerns with requiring, rather than merely encouraging, the use of PIAs? If notice to consumers "is most helpful, when the relevant notice is sufficiently clear and simple," how would PIAs provide consumers with easily understandable information regarding information practices to help guide their technology choices? Do you believe PIAs might be better understood to be a mechanism of accountability rather than transparency and that the ultimate outcome of this process should be organizational decision-making guided by due regard for risks to consumers from information practices?**

The Green Paper recommends that a revitalized set of FIPPs, coupled with a PIA requirement, would provide more uniform commercial privacy protection across industries and data uses. Widespread use of PIA's, for example, might lead companies to consider consumer reactions to products or features that are similar to those that they plan to introduce. The Commerce Department is assessing what incentives could be provided to encourage the development and adoption of all practical mechanisms to protect consumer privacy, with PIAs as only one mere illustration, so that consumers have clearer descriptions of an organization's data collection, use, and disclosure practices. The Department's Task Force has also asked for comment on the elements of a "meaningful PIA" in the commercial context to ensure that consumers are presented with easily understandable information regarding information practices to help guide their technology choices. Once the Task Force reviews stakeholder comments, we will supplement our views on how to best ensure widespread use of PIAs.

TO: Honorable John D. Dingell, Member, House Committee on Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection

FROM: Susan Grant, Director of Consumer Protection, Consumer Federation of America

DATE: January 14, 2011

RE: Answers to questions in connection with the December 2, 2010 hearing entitled "Do Not Track Legislation: Is Now the Right Time?"

Question 1. I happen to be a big fan of the Do Not Call list because it is easy to use and a fine solution to annoying calls that consumers hate. Naturally, then, I feel Do Not Track might be an equally elegant solution for consumers who do not wish to be tracked online. I understand, though, that the online environment is much more complex, and regulation may be difficult to implement and enforce with the myriad sites and services available to consumers. I would like to know what industry is doing or is willing to do to solve this problem on its own. For example, I know that consumers who do not want to be tracked must read long privacy policies to find tools that vary from site to site. What is being done to change that?

Answer:

As I stated in my testimony, we believe that voluntary efforts by industry fall short of providing easy-to-find, easy-to-use, and effective tools for consumers who do not wish to be tracked online. The National Advertising Initiative, which has offered an opt-out cookie for online profiling since 2000, is woefully inadequate because consumers do not know about it, there is no requirement that companies engaged in online tracking participate in the program (and some major players do not), there is no oversight or transparency, and there is no enforcement. Furthermore, opt-out cookies do not work for some methods of tracking and fail to provide persistent protection from unwanted tracking since cookies may be deleted for a variety of reasons.

In July 2009, four trade associations jointly proposed voluntary principles for online tracking, which included providing "choice" mechanisms for consumers (since "choice" is not defined as opt-in, it will likely be offered as an opt-out). The principles contain many exceptions – for instance, no choice need be given for tracking by the website that the consumer is visiting or its affiliates. While the proposal calls for creating a centralized choice mechanism, which has only recently become available, companies that subscribe to the principles do not have to use it; they can provide their own choice mechanisms instead if they wish. It is also envisioned that there may be multiple self-regulatory programs in connection with the principles. While it is too early to assess the effectiveness of the principles or the choice mechanisms offered under this initiative, we believe that this approach is likely to be very confusing for consumers and to suffer from the same drawbacks as the NAI program: participation is voluntary, with no real oversight or enforcement, and the choice mechanisms will probably be based on cookies. There are some positive aspects of the proposal by the four trade associations. One is the development of an icon that companies can use to indicate that online tracking is taking place. To the extent that a standardized icon becomes widely used and familiar to consumers, this may be helpful in making tracking more visible. However, consumers may get the wrong impression if they do not see the icon – it will not mean necessarily mean that that tracking is not taking place, since using the icon is voluntary. We believe that self-regulatory programs can be a useful complement to legal requirements and prohibitions, but not a substitute.

2. It seems that Do Not Track, as it is presently discussed, is all or nothing, meaning that either a user permits his data to be collected or he does not allow any of his data to be collected. Could a middle-of-the-road approach be adopted, and could it be structured in such a way that would be easy for consumers and industry to use?

Answer:

Do Not Track, as we envision it, would not necessarily be an all-or-nothing proposition. It is simply a way for computer users to tell websites and other Internet entities not to track them, much like putting a "No Trespassing" sign on your property. But on the Internet, the sign can be interactive, enabling you to selectively allow tracking if you wish. It is very important, however, for there to be a clear legal definition of tracking. We believe that the Federal Trade Commission should be mandated to define the term. We also believe that clear disclosures should be required to explain what is being tracked and for what purposes the information will be used, and that these disclosures should be made in a standardized format. In order for consumers to make well-informed decisions about when to turn Do Not Track mechanisms on and off and how to respond to requests by specific entities to allow tracking, this information must be provided in a timely and easy-to-understand form. The FTC should also determine what exceptions for Do Not Track would be appropriate and if consumers should have any choices. For instance, in telemarketing, companies that have established business relationships with consumers may call them even if their numbers are on the federal Do Not Call registry, but consumers have the right to tell them not to call them, and that right must be respected. Should websites be able to track consumers while they are on their sites and use that information for their own purposes, even if the consumers have indicated that they do not wish to be tracked? Should those purposes be limited? Should consumers have the right to opt out of such "first party" tracking? How should affiliates be defined and treated? What information is needed to fulfill a consumer request, to prevent fraud, to serve a contextual advertisement based on what the consumer is looking at on the website, or for other purposes that may not cause privacy concerns? Are there kinds of information, such as health conditions, that should not be tracked? Some uses of information? These are questions that could be addressed through an FTC rulemaking.

3. Advertising plays an essential role in the support of free web sites and internet applications. What impact would a Do Not Track proposal have on that support?

Answer:

Do Not Track mechanisms will probably have some impact on certain types of online advertising, but we believe that dire forecasts about the overall impact on free websites are overblown and lack factual basis. The New York Times agrees, stating in a December 4, 2010 opinion piece:

Giving Americans the choice to opt out of data tracking does not mean everybody will. Moreover, even if regulation limits advertisers' ability to precisely target their ads according to consumers' tastes, they will still need to advertise. They will just do it differently. Advertising spending in the United States amounted to 1.8 percent of G.D.P. last year. In 1990, before Yahoo even existed, it amounted to 2.2 percent of G.D.P. It has remained within that range over nearly two decades.¹

¹ "Protecting Online Privacy," New York Times, http://www.nytimes.com/2010/12/05/opinion/05sun2.html?_r=1

Many tools already exist and are deployed by consumers to block all advertisements, not just ads based on behavioral tracking. Adblock Plus is one of the most popular applications on the Web, yet free websites remain strong. Blocking ads, however, is not the same as blocking tracking. As we envision it, Do Not Track would only affect advertising that is based on tracking consumers' behavior across multiple websites, to the extent that consumers choose to use a Do Not Track mechanism. We do not think that it should bar contextual advertisements, which do not raise the same level of concern.

Another witness at the December 2 hearing cited a recent academic study, which contends that the enactment of the European Union's Privacy and Electronic Communications Directive (2002/58/EC) had a harmful impact on online advertising revenues in Europe,² as evidence that a Do Not Track mechanism would be harmful for the online advertising industry in the United States. The findings in the study, however, were much more nuanced. Only a particular type of online ad, standard banner ads, was less effective in terms of changing viewers' stated purchase intent than they had been in the time period before the Privacy Directive was enacted (though not completely ineffective). Ads that were larger, or that were dynamic and/or media rich, or that were specific to the websites where they were placed (e.g. car ads on car websites) were not impacted. The types of websites on which the ads appeared also factored into their effectiveness. The study's authors acknowledged that there were several limitations to the research. For instance, the campaigns in their sample were not random but were provided by members of the advertising industry and the consumers whom the advertisers surveyed were not randomly selected. We also note that the study does not provide information about the extent to which behavioral advertising was used in Europe prior to the Privacy Directive's enactment, or what privacy laws had already existed in the various EU member countries.

In any case, the comparison between a Do Not Track mechanism and European law is not apt. We are not proposing to ban behavioral advertising – we want to empower consumers to avoid online tracking when and if they wish to do so. Some people will never turn a Do Not Track mechanism on, others may turn it on and off depending on what they are doing online. Some people will decide to allow tracking by specific entities. Online advertising will not disappear. Indeed, as the academic study shows, there are many ways to advertise effectively without tracking consumers' online behavior. Another effective advertising method that is not mentioned in the study and that would not be impacted by Do Not Track is serving ads on search sites based on what consumers are searching for. Many in industry claim to want to give consumers "choice" in regard to online tracking, but their objections to more effective Do Not Track mechanisms seem to indicate that they don't want consumers to be able to easily exercise that choice. We believe that effective Do Not Track mechanisms will enhance consumers' confidence in using the Internet, which will ultimately have a positive impact on the Web-based economy.

One more point that is important to make: Do Not Track is not just about advertising. Online tracking can be used for many other purposes; it is already being used, for instance, by life insurers to predict people's longevity³ and there are no limits to its use. That is why we must act now.

4. Is it practical to expect that on a technologically neutral basis, the federal government or private entities will be able to create and maintain a list that prevents people from being tracked on the multiple devices they use to access the Internet?

² Goldberg and Tucker, "Privacy Regulation and Online Advertising," <http://ssrn.com/abstract=1600259>

³ "Insurers Test Data Profiles to Identify Risky Clients," Wall Street Journal, November 19, 2010, <http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html>

Answer:

When we first raised the Do Not Track idea in 2007, we envisioned a list of online trackers' domains that the Federal Trade Commission would maintain and that consumers could download to avoid tracking by those domains (we have never advocated a list of IP addresses of consumers who do not want to be tracked, which would be somewhat analogous to consumers putting their phone numbers on the federal Do Not Call registry, because of privacy and security concerns). Our thinking has evolved, however. We believe a more effective solution would be a tool that would be included or installed in web browsers and that would send information, called a "header," to the websites that consumers visit telling them that the consumers do not wish to be tracked. The browser-header would not physically prevent tracking – it would simply convey the request to the website that the consumer is visiting. Ideally, the website would honor the request and would convey the request to any third parties that collect behavioral data from the site.

Recently, Microsoft announced that the next version of its web browser would accommodate lists of the type that we first envisioned. The company is not proposing to create such lists; it would simply ensure that its browser can accommodate them. The FTC has not proposed that the government create or maintain such lists, either, so it appears that this would be left to the private sector. We think that lists might be useful, but more as a complement, not a substitute, for the browser-header approach that we are advocating. From a practical standpoint, there are many concerns about the list approach: How would consumers know which list is best among multiple lists that may be offered? Would inferior lists leave consumers exposed to unwanted tracking? How would the lists be kept updated? Would consumers have to pay to subscribe to lists and/or keep them updated? Furthermore, while one advantage of using a list of tracking domains is that it would actually block tracking from those domains, this can easily be defeated by using other tracking technology, such as "fingerprinting," from domains that are not on the list. The list approach is also less flexible than the browser-header approach, since it would block any information from being exchanged between consumers' computers and the domains on the list. On balance, we believe that the browser-header approach would work better for consumers and be easier to implement from a technological standpoint.

5. Should a Do Not Track mechanism involve simply no collection of information, or should it also include a prohibition on the use of such information to target consumers?

Answer:

A browser-header Do Not Track mechanism could be flexible from both a technical and a regulatory standpoint. It could be designed to block any data from being collected about consumers' online activities or allow some data to be collected but not other data. We believe that some types of data gleaned from consumers online behavior should not be collected because of its sensitivity, even if consumers allow themselves to be tracked, and that it may be appropriate to limit certain data uses. Furthermore, some data may be necessary to use for truly "operational" purposes even when consumers have turned on a Do Not Track mechanism. These issues should be addressed in an FTC rulemaking proceeding.

6. How should Do Not Track requirements be enforced against entities that continue to collect information about consumers who have not opted out or not authorized such collection?

Answer:

We assume that you mean “who have opted out,” not “who have not opted out.” As we envision it, a Do Not Track mechanism would enable consumers to opt out of online tracking with the flexibility that we described earlier. We believe that there must be underlying legislation to require consumers’ requests not to be tracked to be honored and to authorize the FTC to set other reasonable parameters. The FTC and the states should have the authority to enforce the law. The FTC should also have greater authority to impose fines on bad actors. In addition, consumers should have private rights of action against entities that violate Do Not Track requirements. The consumer privacy class-action lawsuits filed against NebuAd, QuantCast, Facebook and others have clearly had a positive impact on industry practices and are an important part of the enforcement toolbox. Industry should also play an important role in enforcement. Companies are likely to know what is happening in the industry and are often the first to learn about abusive conduct by others. They also have a responsibility to ensure that their partners are following the law.

7. I understand that a comprehensive privacy framework, whether enforced by governmental or private entities, does not exist in the United States. Rather, there exists a patchwork of federal and state laws and regulations that impose varying requirements on entities. Do you believe such laws and requirements be standardized for the entire country to apply equally to all parts of the Internet “ecosystem,” so to speak? Would this better serve consumers and be more conducive to innovation?

Answer:

We believe that a comprehensive privacy framework is needed in the United States. Because the issues are myriad and complex, it will take time to enact such a framework. In the meantime, there is no reason why legislation regarding Do Not Track should not be enacted.

There are good reasons why we have imposed special obligations under current law on certain entities, such as those that handle our medical information or communications, because of the sensitivity of that information. Any attempt to standardize privacy rules and fill the gaps should be careful to avoid lessening these special obligations where they are needed. We also believe that the states have a legitimate and vital role to play in protecting consumer privacy as laboratories of democracy. It is often easier for states to act on privacy protection than the federal government. California’s landmark data breach notification law is a good example. Many states have followed California’s lead, but Congress has been unable to enact federal data breach notification requirements. Industry has been able to adapt to state laws, and innovation by the states helps to spur industry innovation. We believe that a comprehensive privacy framework at the federal level should be a floor, not a ceiling, and we do not support preemption of state privacy protection laws.

HENRY A. WAXMAN, CALIFORNIA
CHAIRMAN

JOE BARTON, TEXAS
RANKING MEMBER

ONE HUNDRED ELEVENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (207) 225-2827
Minority (207) 525-3641

December 28, 2010

Mr. Daniel Castro
Senior Analyst
Information Technology and Innovation Foundation
1101 K Street NW, Suite 610
Washington, DC 20005


Dear Mr. Castro:

Thank you for appearing before the Subcommittee on Commerce, Trade, and Consumer Protection on December 2, 2010, at the hearing entitled "Do Not Track Legislation: Is Now the Right Time?"

Pursuant to the Committee's Rules, attached are written questions for the record directed to you from certain Members of the Committee. In preparing your answers, please address your response to the Member who submitted the questions.

Please provide your responses by January 14, 2011, to Jennifer Berenholz via e-mail to jennifer.berenholz@mail.house.gov. Please contact Jennifer Berenholz at (202) 225-2927 if you have any questions.

Sincerely,



Henry A. Waxman
Chairman

Attachment



January 14, 2011

The Honorable John D. Dingell
 Committee on Energy and Commerce
 Subcommittee on Commerce, Trade and Consumer Protection
 2125 Rayburn House Office Building
 Washington, DC 20515-6115

Dear Rep. Dingell,

Thank you for your written questions submitted for the record. Below please find my responses to your questions:

1. First, the comparison between Do Not Call and Do Not Track is flawed. When consumers choose to opt out of unsolicited telemarketing calls they are not at the same time receiving some free service that is linked to the telephone call. It would be one thing if, for example, the telephone company said in exchange for free telephone service marketers get to call your phone every evening at dinner time. But that is not the deal. There is no quid pro quo. These unsolicited calls are simply an added cost to the economy and an annoyance to most consumers. So it makes sense to have an easy-to-use opt out system for unsolicited telephone calls. In contrast, Do Not Track is like getting the free telephone service without taking the marketing calls. When consumers go online, in the vast majority of cases they are receiving some free content or service (e.g., email, search, data storage, social networking, news, information, entertainment, etc.). And the way they “pay” for these free services is by agreeing to be shown advertisements. And to cover the cost of all of these services companies increasingly need to show ads that are actually of interest to consumers. By opting out of this mutually beneficial relationship, some consumers are trying to get something for nothing.

But to more specifically address your question, online advertisers are developing industry best practices to provide consumers with transparency and choice when using sites with targeted advertising. The Digital Advertising Alliance, an industry coalition, has created a self-regulatory program for online behavioral advertising, a unique icon so consumers can identify interest-based ads, and an online tool to allow consumers to select their advertising preference for over 50 participating ad networks. Individual ad networks have also created their own tools to allow users to manage their advertising preferences. For example, Google, a major online ad network, allows users to opt-out of targeted advertising using the DoubleClick cookie or through an optional opt-out plug-in for their web browser (the plug-in is available for Chrome, Firefox and Internet Explorer). Many third-party online

advertisers, such as those belonging to the Network Advertising Initiative have also made a similar opt-out tool available online for users to more easily avoid targeted online advertising. And third-parties, such as developers of web browsers and browser plug-ins, are developing tool to allow users to better manage their privacy online and help consumers understand their choices.

2. A moderate approach to online privacy can help consumers better understand how their data is collected and used and make more informed choices about which online services they want to use. It is important to remember that every user has different preferences for what data to share and who to share it with. Federal policies should be designed that recognize and respect the fact that many people are willing to trade access to personal data in exchange for free or discounted products and services. This business model should be preserved. To allow for different consumer preferences, one focus of government policy should be to work with industry to develop best practices for creating policies that are transparent and understandable to consumers.

3. The Do Not Track proposal could substantially reduce the advertising revenue that supports the Internet ecosystem. Overall, approximately \$23 billion is spent on online advertising in the United States. Targeted advertising, which is a fast growing segment of online advertising, would be most affected by this proposal. A reduction in this ad revenue would likely lead to fewer free and low-cost applications and services being available to consumers online.

4. A Do Not Track list maintained by the government or the private sector would simply be unworkable since there is no single identifier used to conduct all online transactions. It would create potential privacy and security risks of its own and be ineffective at consistently protecting user privacy across multiple devices, profiles, and applications.

5. The government should absolutely not prohibit the use of information to “target” consumers. To “target” a user means to deliver personalized or customized content to the user, an activity that should be encouraged as it provides consumers a better online experience. As noted earlier, consumers have complex preferences about the collection and use of their personal data. A distinction should be made between what information is collected and how that information is used.

6. One problem with the Do Not Track proposal is that enforcement is difficult. While it is easy to determine if someone violates a Do Not Call list (the consumer receives an unsolicited call), it is significantly more difficult to determine if someone is violating a requirement not to record certain data about users as they visit a website. Moreover, the federal government would have difficulty enforcing this requirement for many non-U.S. websites.

7. Conflicting state laws do impose a cost on the Internet ecosystem as businesses must spend limited resources on compliance. Standardizing the policies could benefit consumers and innovation if the standardized requirements were not excessively burdensome. One way to ensure that consumers are protected without harming innovation is to focus on regulating harmful uses of data (e.g. using online data for discriminatory hiring practices) rather than the collection and use of such data for benign purposes. The government should also build on existing self-regulatory systems that the private sector has already developed or is in the process of developing.

Sincerely,

A handwritten signature in dark ink, appearing to read "Daniel Castro", with a stylized flourish at the end.

Daniel Castro

Senior Analyst
Information Technology and Innovation Foundation

