

S. HRG. 113-550

A STATUS UPDATE ON THE DEVELOPMENT OF VOLUNTARY DO-NOT-TRACK STANDARDS

HEARING

BEFORE THE

COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

APRIL 24, 2013

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



U.S. GOVERNMENT PUBLISHING OFFICE

93-065 PDF

WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

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

BARBARA BOXER, California	JOHN THUNE, South Dakota, <i>Ranking</i>
BILL NELSON, Florida	ROGER F. WICKER, Mississippi
MARIA CANTWELL, Washington	ROY BLUNT, Missouri
FRANK R. LAUTENBERG, New Jersey	MARCO RUBIO, Florida
MARK PRYOR, Arkansas	KELLY AYOTTE, New Hampshire
CLAIRE McCASKILL, Missouri	DEAN HELLER, Nevada
AMY KLOBUCHAR, Minnesota	DAN COATS, Indiana
MARK WARNER, Virginia	TIM SCOTT, South Carolina
MARK BEGICH, Alaska	TED CRUZ, Texas
RICHARD BLUMENTHAL, Connecticut	DEB FISCHER, Nebraska
BRIAN SCHATZ, Hawaii	RON JOHNSON, Wisconsin
WILLIAM COWAN, Massachusetts	

ELLEN L. DONESKI, *Staff Director*

JAMES REID, *Deputy Staff Director*

JOHN WILLIAMS, *General Counsel*

DAVID SCHWIETERT, *Republican Staff Director*

NICK ROSSI, *Republican Deputy Staff Director*

REBECCA SEIDEL, *Republican General Counsel and Chief Investigator*

CONTENTS

Hearing held on April 24, 2013	Page 1
Statement of Senator Rockefeller	1
Statement of Senator Thune	3
Statement of Senator McCaskill	4
Statement of Senator Heller	5
Statement of Senator Johnson	6
Statement of Senator Blumenthal	64

WITNESSES

Harvey Anderson, Senior Vice President, Business and Legal Affairs, Mozilla .	6
Prepared statement	8
Luigi Mastria, CIPP, CISSP, Managing Director, Digital Advertising Alliance	14
Prepared statement	15
Justin Brookman, Director, Consumer Privacy, Center for Democracy & Technology	24
Prepared statement	26
Adam Thierer, Senior Research Fellow, Mercatus Center, George Mason University	33
Prepared statement	35

APPENDIX

Response to written questions submitted to Harvey Anderson by:	
Hon. John D. Rockefeller IV	69
Hon. Barbara Boxer	69
Hon. Frank R. Lautenberg	71
Hon. Amy Klobuchar	72
Hon. Brian Schatz	72
Hon. Ron Johnson	73
Response to written questions submitted to Luigi Mastria by:	
Hon. John D. Rockefeller IV	74
Hon. Barbara Boxer	75
Hon. Ron Johnson	78
Response to written questions submitted to Justin Brookman by:	
Hon. John D. Rockefeller IV	86
Hon. Barbara Boxer	88
Hon. Frank R. Lautenberg	89
Hon. Amy Klobuchar	90
Hon. Brian Schatz	91
Hon. Ron Johnson	93
Response to written questions submitted to Adam Thierer by:	
Hon. Barbara Boxer	96
Hon. Frank R. Lautenberg	97
Hon. Ron Johnson	97

A STATUS UPDATE ON THE DEVELOPMENT OF VOLUNTARY DO-NOT-TRACK STANDARDS

WEDNESDAY, APRIL 24, 2013

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

The committee met, pursuant to notice, at 2:38 p.m., in room SR-253, Russell Senate Office Building, Hon. John D. Rockefeller IV, Chairman of the Committee, presiding.

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

The CHAIRMAN. All right. This hearing will come to order.

In February 2012, the Digital Advertising Alliance pledged that the online advertising industry would honor Do-Not-Track requests made by consumers. That commitment was supposed to happen by the end of the year which is called 2012. We are past that time.

What it was supposed to mean, what that statement was supposed to mean was that when consumers made it clear they did not want advertisers to collect information about their Internet activities, the advertisers would respect their wishes. It is now April 2013, and consumers are still waiting for these Do-Not-Track standards.

Advertising folks are continuing to ignore Do-Not-Track headers and consumers' requests for privacy. There is a broad feeling that the advertisers, brokers, et cetera, data brokers, are just dragging their feet, and I believe they are, and I believe they are doing it purposely.

I personally have long expressed skepticism about the ability or the willingness of companies to regulate themselves on behalf of consumers when it affects their bottom line. It is just the way I am made. It is my experience. And my service in West Virginia makes me have that—and my service on this committee really makes me feel very strongly about that.

And that is why for the past two Congresses, I have introduced legislation that would create meaningful Do-Not-Track standards for consumers. I do not believe that companies with business models based upon the collection and monetization of personal information will voluntarily stop these practices if it negatively impacts their profit margins. I just think that is the way corporations, with obviously a number of exceptions, are run.

They are there to make money. And consumers, particularly when you get something like the Internet, which everybody wants, worships, and loves, that is even more so.

Having said that and disclosed what is a genuinely troublesome feeling that I have about the nature of corporations with a chance to make money, particularly when people don't know what they are doing, in spite of that, I want to be open-minded today. I want to do my best, Senator Thune, to be open-minded. And I want to hear all sides on the matters at hand.

For months, industry stakeholders, consumer groups, academics, and other interested parties have been in negotiation with the World Wide Web Consortium, known as W3C, attempting to reach an agreement on voluntary Do-Not-Track standards. But conflicting reports about W3C negotiations continue to surface.

On one side, I hear that online advertising industry is deliberately dragging its feet, moving the goal posts, and refusing to stop collection practices that undermine the very essence of a meaningful Do-Not-Track standard. On the other side, I hear two software developers, in particular Microsoft and Mozilla—which I know are not necessarily popular with all of those at the desk that I am looking at in front of me—have prevented the W3C from forging consensus on voluntary Do-Not-Track standards.

In other words, people who want to do it by default, which, in many ways, I think is the best way to go, they don't want to put up with that. So there is a meeting coming up in May, in Sunny-side, California. And I think the same problems will be stopping us then as are now.

Today, I want to get to the bottom of this controversy, and I have got a great prosecuting attorney over there ready to jump in. I want the witnesses to publicly explain exactly what they believe has gone wrong and what they are prepared to offer to make Do-Not-Track a reality for consumers, as they said they were going to do.

However, while I want to be fair and hear from all sides, I do not want to hear some of the familiar talking points that deliberately serve no purpose but to confuse the debate. I will interrupt if that stuff starts coming up.

I do not want to hear that Do-Not-Track would jeopardize anti-fraud efforts, cybersecurity, or the Internet itself with a strict prohibition on any collection of information because it is simply not true, and you know it is not true because we have written that into our latest bill. Small companies will be protected.

Everyone acknowledges that some limited collection of information is necessary in order to fulfill basic functions. My own bill clearly provides for this.

Furthermore, I do not want to hear assertions that the current self-regulatory scheme fulfills Do-Not-Track requests. You can try it. After I have heard it one and a half times, I will just stop it.

A meaningful Do-Not-Track standard prohibits the collection of online information except for a few narrow purposes, and we all know what those are. Under the current Ad Choices Campaign operated by the advertising industry, companies continue to collect vast amounts of consumer information and only promise to not use this information for specific purposes, such as targeted advertising.

In addition to my concerns that consumer choices are not being honored, I am also worried about the escalating rhetoric that we have witnessed in the past few months, that Chairwoman Ramirez

was subject to when she spoke recently at a meeting, basically on-line advertisers about Web browser developers.

Browsers are attempting to provide consumers with greater privacy protections, and ad networks are resisting these efforts. If you can say that I am wrong, please prove it to me.

I am disturbed with the rhetoric from advertisers that suggest they might try to circumvent the sensible privacy protections that Web browsers are providing consumers. The nuclear option or the destruction—the end of the Internet, all this kind of stuff that you hear constantly from people who don’t want to do what they need to do.

I urge everybody to take a deep breath, myself included, and tone down the rhetoric. We all need to remember that this debate is about consumers and their choices. That is what we do on this committee.

Consumers who may be happy to have their information collected for targeting advertising in some situations, but who may want advertisers to completely leave them alone at other times. It is their choice.

In this regard, I believe all sides should be prepared to compromise in order to maximize protection for consumers. And I urge all of the witnesses today to spend less time attacking their opponents and spend more time thinking about how we can honor and respect consumer preferences.

That is the end of my statement.

I call upon my distinguished and most excellent colleague, Senator Thune.

**STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA**

Senator THUNE. Thank you, Mr. Chairman, and thank you for holding this hearing as the Committee discusses and evaluates consumer habits in the digital online economy.

Thank you also to all of the witnesses who are here today for providing testimony.

Online commerce and Internet use are a substantial and growing part of our overall economy and everyday lives. According to the research firm eMarketer, nearly 150 million Americans were digital buyers in 2012, collectively spending more than \$340 billion online. To court this growing consumer base, more than \$37 billion was spent last year on digital advertising.

As large as the online market already is, estimates for coming years predict continued growth. Both digital advertising and consumer spending are projected to grow by more than 50 percent by 2016, when 25 million more Americans are expected to be digital consumers.

The growing digital advertising industry provides thousands of small Web publishers, the so-called long tail of the market, with the revenue that they need to maintain their online presence. Contextual advertising, like an ad for running shoes on a website catering to runners, and general display ads make sense for some websites, but don’t necessarily make sense for all websites.

The market has responded by developing new and innovative ways to deliver relevant ads and content to Internet users, but this has raised questions about consumer expectations and privacy.

It is my hope that today's hearing will be a thoughtful discussion on how we can provide consumers with greater choice of services and products, as well as increased confidence that their Internet experiences will be safe. Federal Trade Commission Chairman—as you mentioned, Mr. Chairman—Ramirez recently gave a speech to the American Advertising Federation in which she said, and I quote, “An online advertising system that breeds consumer discomfort is not a foundation for sustained growth.” I agree.

And it is precisely because of that dynamic that I believe Web publishers, browsers, social networks, data analysts, and advertisers have an incentive to develop their practices to meet the evolving interests of consumers. I am interested to learn how efforts to regulate and legislate the intricacies of online commercial activity could impact the digital space.

Will efforts to improve, or I should say will efforts to impose Do-Not-Track rules better protect consumers and grow online commerce, or are there situations where they might diminish consumer privacy, inhibit consumer choice, or raise barriers to entry for new competitors in the online market? The largest browsers and publishers have the means to adapt and survive in any environment, but smaller online companies and the choices they provide for consumers may not.

I have faith that consumers armed with knowledge will take the time to make informed decisions in their own best interests. Consumers expect and seek more transparency, understanding, and control as they increasingly interact with online resources, and the market is responding.

New tools are being presented and refined in response to consumers' expectations. This spurs growth and innovation, which benefits both consumers and producers.

I am interested in our witnesses' views on the dynamic Internet ecosystem and the value and the status of industry-developed standards for online conduct.

I thank all the—again, the witnesses for being here today. I look forward to hearing your testimony and to interacting with you as we ask you some questions.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, sir.

And now Senator McCaskill, who is Chair of the Subcommittee, and then Senator Heller.

**STATEMENT OF HON. CLAIRE McCASKILL,
U.S. SENATOR FROM MISSOURI**

Senator McCaskill. I am just a little nervous because I am afraid you are going to cut me off.

The CHAIRMAN. I doubt that.

[Laughter.]

Senator McCaskill. You doubt that I am nervous, or you doubt that you are going to cut me off?

The CHAIRMAN. I have never seen you nervous.

Senator McCASKILL. I have not prepared any opening statement. I am anxious to question the panel.

I think privacy is an all-American goal, but so is the most vibrant part of our economy. And what tech has done, the Internet has done for our economy is huge, and I want to make sure that we are balanced as we look at this issue in a way that protects consumers, but also makes sure that we don't end up with one or two or three giant Internet companies with none of the little guys.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Senator Heller?

**STATEMENT OF HON. DEAN HELLER,
U.S. SENATOR FROM NEVADA**

Senator HELLER. Thank you, Mr. Chairman. Thanks for taking time on this important issue. I know it is important to you.

I want to thank our witnesses for being here also today, and those who are interested in today's discussion.

I appreciate this hearing today to understand where the private sector is on voluntary Do-Not-Track agreements. This issue crystallizes the transactional nature of using the Internet.

Whether consumers realize it or not, there is an exchange taking place when an individual launches their Internet on whatever device they are using. In exchange for services, such as free search engines, free e-mail, free content on websites, free travel to destinations such as Las Vegas, free car rental bookings in places like Las Vegas—

[Laughter.]

Senator HELLER.—free dinner bookings to world-class restaurants like in Las Vegas, these consumers, whether they know it or not, are being tracked. Some people don't even know they are being tracked, and I, frankly, think some people don't care.

And as we all know, the World Wide Web Consortium, or W3C, has been working on an international set of standards in an effort to improve user privacy and user control by defining what a user should expect when opting for no tracking during their online sessions.

We have been hearing from some of the W3C—for some time that W3C is spinning their wheels, unable to come to an agreement. The W3C, as a majority, has a major opportunity here on May 6 through 8 in California to come together and decide if they can reach an agreement, and I hope this will happen. I think that a result on this issue by the private sector is the most appropriate way to go.

I would encourage the W3C to try to find to the fullest extent possible to uphold just a few principles, first being any solution must be technology neutral. Second, it must be business model neutral, and third, it must not pick winners and losers.

I also want to point out how difficult a consensus will be to achieve. I think it is going to be very difficult. The W3C is made up of privacy groups, Web browsers, first-party advertisers, third-party advertising companies, and experts in the public sphere. There are many, many competing agendas here.

It is important that this committee attempts to better understand why coming to an agreement here is fleeting and perhaps encourage that the private sector be able to reach a consensus. It is also important to understand that any solution that blocks third-party advertising companies from placing cookies on the Internet will have economic consequences.

This sector provides many jobs and generates multibillions of dollars of economic activity, even in Las Vegas. Understanding exactly what first- and third-party tracking online and whether the consumer is harmed in some fashion or even cares is incredibly important for all of us to understand, especially if a Government solution is being considered. I think the last thing any member wants is to propose a solution that chills investment and innovations.

The question really being discussed here is not whether tracking is happening, because it is. The question is whether harm actually exists, and what is that harm, and what is the appropriate solution to that? I believe the goal here is consumer education and choice, but it should be from the private sector.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much, Senator Heller.

And with no disrespect to you, sir.

**STATEMENT OF HON. RON JOHNSON,
U.S. SENATOR FROM WISCONSIN**

Senator JOHNSON. I am fine. Thanks.

The CHAIRMAN. OK. Well, I know that.

[Laughter.]

The CHAIRMAN. Let us go right to questioning, and I will start. Oh, no, no, no. I do that all the time.

[Laughter.]

The CHAIRMAN. I am so in love with what I have to say that I just don't even bother listening to the witnesses. So why don't we try my bothering to listen to the witnesses today.

Let us start with you, Mr. Anderson. Actually, I think that is the third or fourth time I have done that. Oh, well.

**STATEMENT OF HARVEY ANDERSON, SENIOR VICE
PRESIDENT, BUSINESS AND LEGAL AFFAIRS, MOZILLA**

Mr. ANDERSON. Thank you, Chairman, Ranking Member Thune, and other members of the Committee. We appreciate the opportunity to testify today on the status of Do-Not-Track.

I am Harvey Anderson. I lead the business, legal, and public policy teams for Mozilla. Mozilla is the maker of the Firefox browser used by 450 million people worldwide. We developed Firefox to bring competition to the browser market nearly 10 years ago and to promote an open, innovative Web.

We were the first to include Do-Not-Track with the setting as Do-Not-Track off by default. We try to be an agent for the user to help users navigate their digital lives in ways that make sense to them.

A couple comments. The Internet is the most significant social and technological development of our time. However, the Internet is very, very young, maybe 9,000 days young. Let us put that in perspective in terms of the World Wide Web.

So this means that mainstream users do not necessarily have a historical set of norms or expectations to guide their digital choices. The Web has also created new and unparalleled opportunities online that produce unimaginable amounts of data. At the same time, there are no clear parameters or boundaries on data practices other than those that are codified by law or regulatory bodies. So acceptable collection and use norms are still evolving.

We cannot often not predict what models the current technology will enable. Lou Montulli and John Giannandrea, they were colleagues of mine at Netscape, developed the cookie to solve a very real technical problem, to store state and invent the notion of a session over several HTTP requests. Few would have imagined a whole industry built upon the cookie.

The online ad business, as you mentioned, has grown to a record-breaking \$37 billion in 2012. This means change will be met with resistance by incumbent interests with arguments that I have heard such as change is bad for competition or that it will decrease revenue. We should question whether protecting business models that lack transparency is actually protecting competition.

Historically, there have been many profitable business models that have challenged our norms, but profits don't always justify practices. Similar arguments were made when Firefox blocked pop-up ads. They said it will destroy the industry, but it seems it has not hindered the success of the online ad industry today.

It was nearly a year ago when my colleague Alex Fowler reported on the status of DNT before this committee, and since that time, the industry has not moved forward quickly enough, in our opinion. Consumers have shown increased concern about online tracking and privacy. More users are sending DNT signals than ever, and yet the efficacy of the Ad Choices Program remains questionable.

Consumer concerns over online tracking persists, as shown by numerous independent studies referenced in our written testimony. Our own adoption of consumer sentiment data shows support for DNT. Do-Not-Track adoption by Firefox users in the U.S. is roughly 17 percent. It is pretty consistent across all the states.

Consumer engagement with the DAA Ad Choices Program remains low. Last month, the industry reported more than a trillion ads per month included the Ad Choices icon, but only 1 million users have opted out of all interest-based advertising.

The claims that this low opt-out rate prove that consumers are OK with the tracking and collection belie the facts as shown by the actual DNT adoption and consumer surveys. Currently, DNT signals are largely ignored by ad networks. We estimate that Firefox users send more than 135 million DNT signals every day. That is more than 4 trillion every month, 4 trillion every month, that go unanswered.

Over the past year, we have observed the trends that characterize the DNT work of the W3C as part of industry self-regulation. The W3C is neither the industry nor a self-regulatory effort on its own. The W3C codifies technical standards for issues that are either well understood and agreed upon in advance or problematic for a set of stakeholders motivated to find a common solution. It is also not designed to replace regulation and enforcement.

Ultimately, the question here is not about the standards process, but about responding to the 45 million Firefox users and IE users who are simply saying don't track me. The DNT standard doesn't have to be final at the W3C to get started. We would like to see more of the industry move forward and begin implementing DNT now.

We applaud leading companies like Twitter, AP, and Jumtap, and the quiet supporters, many who are DAA members, who adopted DNT, all without waiting for a final W3C spec. Apparently, it takes neither a law nor a finalized W3C spec to do the right thing.

What is at stake is not money here, but trust. To date, the debate is focused on the threat to those revenue models that are based on tracking. But the loss of user trust is far more dangerous than the potential lost revenues.

Trust is the true currency that needs to be protected. The lack of trust stems from users not understanding the value proposition of online tracking. This is where industry can really make a difference. If users don't understand what happens to their data, how it is used, or the tradeoffs, they will inevitably seek more protective blocking options.

Efforts to protect the status quo further erode people's trust, thereby compromising future expansion of commerce and innovation online. We want to help the ad and publishing industries create a paradigm of trust that both respects users and supports commerce.

We recognize the current opt-out system represents significant efforts. The work the DAA has done is—should be acknowledged. That is a lot of work to get industry to do one thing comprehensively.

We also know that legislating technology is risky. Given the current environment, though, it is clear that more is required, including continued congressional oversight. As we and industry thought leaders have observed, there is a better way to gain the users' trust. Real transparency of data practices, combined with meaningful user choice, will engender the confidence users expect.

Thank you again for the opportunity to testify today.

[The prepared statement of Mr. Anderson follows:]

PREPARED STATEMENT OF HARVEY ANDERSON, SENIOR VICE PRESIDENT, BUSINESS
AND LEGAL AFFAIRS, MOZILLA

Chairman Rockefeller, Ranking Member Thune, and other members of the Committee, thank you for the opportunity to testify on the need for privacy protections, the status of self-regulation and Do Not Track (DNT).

I am Harvey Anderson, I lead the business, legal, and public policy teams for Mozilla. In addition to commercial and legal responsibilities, this role also captures the intersection of product and policy initiatives such as DNT, leadership on open Internet issues, net neutrality, copyright reform, and Internet governance. I have practiced in the technology sector for the past 20 years, and have worked in the Internet domain since I first joined Netscape in the mid 1990s.

Mozilla is the maker of the Firefox browser used by 450 million people worldwide. We developed Firefox to bring competition to the browser market, and to promote openness, innovation, and opportunity online. We do not own or operate a search or advertising business, yet like most online ventures, our revenues are based on advertising and commerce. We view ourselves as "an agent of the user" whose role is to help users navigate their digital lives in ways that make sense to them. Mozilla

was voted the Most Trusted Internet Company for Privacy in 2012 by the Ponemon Institute, as well as a top 20 overall trusted brand for privacy.¹

When we testified here last time on this topic, we told you that:

- Industry self-regulation can work when it is a multi-stakeholder process that reflects the views of all of the relevant parties involved in data transactions.
- Regulatory measures can introduce unintended consequences that can be harmful to a fragile Web ecosystem.
- Enabling economic ecosystems on the Web is essential to a robust and healthy Internet; however, commercial imperatives and user choice/control are not mutually exclusive. They can and must coexist through a combination of technical capabilities and user-centric business and data practices.
- The multi-stakeholder process occurring at the W3C will result in a consensus on both the meaning of DNT and how websites should respond.

Those statements stand true today and are still timely for your consideration. Our goal today is to provide further context, an update on recent market developments, and insights that can assist your evaluation of whether current self-regulatory efforts are adequate. To achieve this, I will touch on the following topics:

- The Internet environment;
- What has happened since the June 2012 hearing by this committee on DNT; and
- Expectations of the W3C standards process for online tracking.

My testimony today will not cover Mozilla's current evaluation of a new third-party cookie policy in Firefox. That work is ongoing as we engage with the full spectrum of stakeholders, including our users, developers, advocates and business leaders. We would be pleased to come back at a later date to update members of this Committee on browser product features that give more options to manage cookies.

Internet Environment

The Internet is the most significant social and technological development of our time. However, the Internet is young, very young—maybe 9,000 days since the evolution of the World Wide Web. As a result, we are all still finding our way in this evolving environment. This means that mainstream users do not necessarily have a historical set of norms or expectations to guide their digital choices, they do not always understand the consequences of their online actions and the trade-offs implicit in getting services for “free,” or what happens “behind the scenes” with their data.

The Web ecosystem has also created new and unparalleled opportunities online that produce unimaginable amounts of data and possibility for new products, services and relationships. Google's Eric Schmidt observed in 2010 that “we create as much information in two days now as we did from the dawn of man through 2003.”² At the same time, there are no clear parameters or boundaries other than those that are codified by legislative and regulatory bodies or by industry practices. So acceptable collection and use norms are still evolving. Notwithstanding the current entropy in the market, this is a natural form of evolution which should temper both expectations and desires to intervene prematurely.

Commercial models are also evolving on top of this ever-changing technological landscape. We often cannot predict what models the current technology will enable. Consider the models based on the cookie. Lou Montulli and John Giannandria, colleagues of mine at Netscape, developed the cookie to solve a very real technical problem—to store state and invent the notion of a “session” over several HTTP requests. It is safe to say they would have never imagined a whole industry built upon a technical construct like the cookie and the data practices it enables.

During this same period, the digital advertising business has grown, reaching a record-breaking \$36.6 billion in 2012³—so there is real money at stake. This means any change will be met with resistance by inherent incumbent interests. We have seen these arguments in this debate expressed as change is bad for competition or will decrease revenue. We should question whether protecting business models that lack transparency is “protecting or promoting competition”—particularly models

¹2012 Most Trusted Companies for Privacy, Ponemon Institute, January 28, 2013; <http://www.ponemon.org/local/upload/file/2012%20MTC%20Report%20FINAL.pdf>

²Techonomy Conference, Lake Tahoe, California, August 4, 2010; <http://techonomy.com/>

³IAB Internet Advertising Revenue Report, Interactive Advertising Bureau and PricewaterhouseCoopers, April 2013; http://www.iab.net/media/file/IAB_Internet_Advertising_Revenue_Report_FY_2012.pdf

that use data in ways that people do not understand or expect. Historically, there have been many profitable models that have challenged our norms, but the fact that they were profitable neither sanctioned them nor justified their preservation. It is worth pointing out that the widespread adoption of pop-up blocking by browsers, which Mozilla led many years ago and was initially labeled “bad for advertising,” has clearly done nothing to hinder the success or innovation of online marketers or the operation of websites.

At the same time, a new paradigm has developed that pits “what can be done” against “what should be done.” We face this challenge often at Mozilla. Although we employ privacy by design and use transparency, choice, and control as guiding principles, the application is not always easy. For example we internally debate whether the functionality and configuration for a new product or service provides enough informed choice, the right choices, which defaults make sense, and whether user experience is compromised. No doubt this body is no stranger to extended debate given the vast constituencies you represent. The point here is that the application of our values is still under development and that application changes based on context while the values do not. We all remain in search of that delicate balance that allows for aggressive innovation and competition, but that also respects user intent, expectations, and ultimately creates trust. This is part of the backdrop that should inform what we expect from business solutions, technical standards and self-regulatory programs.

Developments Since June 2012

It was nearly a year ago when Alex Fowler, my colleague and Chief Privacy Officer of Mozilla, sat at this table to report on the status of DNT. Since that time, the industry has not moved forward quickly enough, consumers have shown increased concern about online tracking and privacy, more users are sending DNT signals, and yet the efficacy of the Ad Choice program remains questionable.

Consumer concerns over online tracking persist and continue to grow. A study published by the prominent industry analyst group Ovum, found that 68 percent of the Internet users across 11 countries would select Do Not Track if easily available to them. The group also found that only 14 percent of respondents believe Internet companies are honest about their use of consumers’ personal data.⁴ Similarly, research at UC Berkeley’s Center for Law and Technology found that over 60 percent of users want DNT to prevent the collection of information about their online activities.⁵

Our own data continues to show strong user support for and steady adoption of DNT. We see this in actual adoption and consumer sentiment. DNT adoption in the U.S. Firefox user base is approximately 17 percent. Globally, the average is 11 percent. Statewide Firefox DNT adoption rates are outlined in the table below.⁶

⁴*Ovum predicts turbulence for the Internet economy, as more than two-thirds of consumers say ‘no’ to Internet tracking*, February 6, 2013; http://ovum.com/press_releases/ovum-predicts-turbulence-for-the-internet-economy-as-more-than-two-thirds-of-consumers-say-no-to-internet-tracking/

⁵*Privacy and Modern Advertising: Most U.S. Internet Users Want “Do Not Track” to Stop Collection of Data About their Online Activities*, Chris Jay Hoofnagle, Jennifer Urban and Su Li, Oct. 8, 2012; <http://www.law.berkeley.edu/privacysurvey.htm>

⁶Anyone with a website and access to a web server can start counting how many users are sending DNT:1, which is how the signal is expressed via HTTP requests.

Table: User Adoption Averages in the U.S. for Do Not Track in Firefox

Source: Mozilla, April 2013

Consumer concerns over online tracking and privacy are real. Surveys of our user base consistently show concern about online privacy. Only 13 percent of respondents believe their privacy is being respected online. More importantly, over 60 percent of those polled want DNT to cover both collection and use by companies online in either a first- or third-party context. At the same time, the prevalence of non-transparent online tracking continues to grow year over year. A recent Evidon study showed a 53 percent increase in trackers from the prior year.⁷ Even more alarming, only 45 percent of the tracking tags identified by Evidon were placed there by the publisher of the site.

The efficacy of the Digital Advertising Alliance (DAA) Ad Choices program, which is still only in beta after several years of development, remains low. Many stakeholders view this as an indicator of the inadequacy of the industry-led, self-regulatory program. Last year, according to one study, the number of users who viewed the icon was low: 0.0035 percent of users clicked, and only 1 in 20 of those actually opted out.⁸ Last month, the industry reported that more than a trillion ads per month include the Ad Choices icon—a blue triangular icon that when clicked, takes consumers to a page where they can learn about the ad, and opt out of receiving it. Only five million users have accessed the choice tool, and 1 million of those have opted out of all interest-based advertising.⁹ The claims that this low opt-out rate prove that consumers are “OK” with the tracking and collection practices associated with cookies clearly do not square with the overwhelming research that consistently finds that the majority of consumers are concerned with being tracked across the Web. They also do not square with the 11 percent of Firefox users who have turned on Do Not Track.¹⁰

⁷ Evidon, a firm that administers the ad industries’ Ad Choices program for more than \$2 billion of display media and e-commerce transactions annually, measured sites across the Internet and found 987 web-tracking tags from ad servers, analytics companies, audience-segmenting firms, social networks and sharing tools, which represented a 53 percent increase from the 645 unique trackers found in previous studies.

⁸ Leon, P. et al., *What Do Online Behavioral Advertising Disclosures Communicate to Users?* April 13, 2012; http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12008.pdf

⁹ “Opinion: Harnessing the power of digital advertising,” Lou Mastria, *Politico*, March 10, 2013; <http://www.politico.com/story/2013/03/harnessing-the-power-of-digital-advertising-88668.html#ixzz2QrUsIE1S>

¹⁰ A common practice would be to gather user data to test the impact of the program. The results of A/B testing and user group studies on the Ad Choices user experience may be helpful

Continued

Currently, DNT signals are largely ignored by ad networks. We estimate that approximately 45 million Firefox users send more than 135 million DNT signals every day—more than four trillion every month—that mostly go unanswered. As discussed at the last DNT hearing, Microsoft adopted DNT and made it a default setting in their latest versions of Internet Explorer (IE). The position from the ad industry's trade groups, paraphrasing of course, is that their members can ignore DNT signals sent by users of IE.¹¹ This was followed by a similar statement by Yahoo! that it intended to disregard DNT signals coming from IE users.¹² The rationale: DNT signals from IE do not represent a real user choice because it is on by default. So, in the interim, both Firefox users sending DNT signals every day and those IE users for whom the DNT signal represents their real choice are ignored. It does not have to be this way. The industry could incrementally respond in parallel while the standard is being finalized, and could always prompt an IE user to confirm his/her choice.

What to Expect from a Standards Process

Over the past year, we have been troubled by a trend to characterize the ongoing standardization work on DNT by the W3C as a part of industry self-regulation. First, the W3C is neither *the* industry, nor the proper vehicle on its own to establish a self-regulatory program. It is a technical standards group. The W3C's Tracking Protection Working Group¹³ is not an extension of the DAA's Ad Choices program. The W3C is a body that codifies technical standards for issues that are either well understood and agreed upon in advance, or problematic for a set of stakeholders who are motivated to find a common solution. The W3C, or any technical standards group for that matter, is not intended to develop mechanisms that replace regulation and enforcement. Most standards groups are intended to be voluntary with a focus on improving issues like interoperability, efficiency, performance and transparency. This drives competition toward quality of implementation (efficiency/performance) and away from fragmentation.

The group is currently in the drafting stage which is now co-chaired by Professor Peter Swire who testified at last year's DNT hearing. This will be followed by a period of testing at Internet scale. In fact, our discussions with members of the group reveal that we may be very close to signing off on the Tracking Preference Expression specification, which covers the client-server architecture for DNT.¹⁴ Stakeholders that are standing by, waiting for the W3C to "complete" its work are misguided. Technical standards are adopted only after drafting, testing, refining and finalizing. But nothing prohibits *de facto* adoption during this process. Thus, arguments that shift blame exclusively to the W3C are dubious. At the same time, regulatory groups in the U.S. and abroad should not hold back enforcement of its local laws in deference to the work happening within the W3C.

Ultimately, the question here is not about the standards process, but about responding to the tens of millions of consumers every day who are sending a DNT signal expressing a concern about their privacy and online tracking. There are many examples of how other markets react to guidance from their consumers. For example, car owners expressed preferences about the need for better gas mileage from their cars. They might not have immediately perceived that this could have an impact on the oil industry, influenced manufacturing, or that the solution was electric or hybrid cars, but the market did not ignore the signals. Rather, the market provided basic education and responded to the demand. Here, in the DNT context users are saying, "do not track me." They may not know *exactly* what it means in every detail or nuance, but they understand enough without the extensive explanation called for by some.

The DNT standard does not have to be final at the W3C before implementation begins. We would like to see more of the industry move forward and begin implementing DNT now. This is how Web standards are established—they must be iterative and user/developer-tested. It is how HTML5 was developed—some set of players adopt an approach that looks promising, they work out the kinks through use, and over time codify it. This practice is borne from the experience that if you wait to work out the perfect specification, you'll never get anything done.

to this Committee as it seeks to understand the effectiveness of the current self-regulatory effort.

¹¹DAA Statement on DNT Browser Settings, October 09, 2012; <http://www.businesswire.com/news/home/20121009005980/en/DAA-Statement-DNT-Browser-Settings>

¹²In Support of a Personalized User Experience, October 26, 2012; <http://www.ypolicyblog.com/policyblog/2012/10/26/dnt/>

¹³See <http://www.w3.org/2011/tracking-protection/>

¹⁴See <http://www.w3.org/2011/tracking-protection/drafts/tracking-dnt.html>

We are encouraged by some publishers, advertisers and other companies in the ecosystem who have put DNT into effect for their businesses. We applaud leading companies like Twitter, the Associated Press and Jumptap who have voluntarily implemented DNT and are trying to respond to the expression of user intent—all without waiting for a W3C pronouncement.¹⁵ We are also aware of many more companies across the advertising and publishing industries quietly supporting users who have enabled DNT, including DAA member companies. Apparently, it takes neither a law nor a finalized W3C specification to do the right thing.

What is at stake is not money, but trust. To date the debate has focused on the threat to those revenue models that are based on tracking. But, the loss of user trust is far more dangerous than potential lost revenues. Trust is the true currency that needs to be protected.

The lack of trust stems from users not understanding the value proposition of online tracking. Former IAB Chair, Jim Spanfeller, recently wrote in an op-ed, “[B]y doing unto others what we want done to us, we will enter into a more trusted ecosystem. Business, information exchange, spontaneous discovery and overall satisfaction will thrive in ways that have become increasingly difficult due to black hat activities perpetrated partly in the name of advertising efficiencies.”¹⁶ This trust gives rise to increased participation and will foster new jobs. Similarly, Pam Horan, the Online Publishers Association’s President, wrote in an op-ed, “Ultimately this is about fostering a healthy environment where consumers feel safe online. It is hard to dispute that without this baseline acknowledgement of consumers’ expectations, our entire ecosystem will be compromised.”¹⁷

This is where industry can really make a difference. If users do not understand what happens to their data, how it is used, or the trade-offs, they will inevitably seek more protective blocking options. Conversely, we may see the adoption of more invasive and even less transparent tracking methods. The impact is that efforts to protect the status quo further erode people’s trust in the ecosystem, thereby compromising future expansion of commerce and innovative growth of this ecosystem. Personalized content is good, however, the collective challenge we face is how to deliver that content transparently.

The future of a viable, innovative Web that continues to contribute jobs and drive social, educational and economic activity depends on consumer trust. To develop this trust, transparency, choice and control are essential. Real transparency of business and data sharing practices combined with meaningful user choice will engender the confidence users expect. With this as a baseline, I suspect survey results would be dramatically different and users may very well even opt-in to forms of tracking and data collection they understand and find valuable.

We saw a similar reaction in the early years of online commerce. People were afraid to use credit cards on the Internet until encryption was readily used and then users began to trust the practices that supported online electronic purchases. We believe it is in the industry’s own best interest to aggressively seek long-term, privacy-preserving and economically sound approaches to behavioral targeting and personalization that foster trust and greater participation and sharing of data. As the OPA’s Pam Horan observed, “Although change can be hard for any industry, it can also be a catalyst for better content services and privacy protections in the Internet ecosystem . . .”¹⁸

We want to help the advertising and publishing industries create a paradigm of trust that both respects users and supports commerce. We recognize that the current opt-out system is in many ways a significant achievement—it is no small task to achieve comprehensive industry behavioral change. We also recognize that legislating technology is challenging and risky—but we can articulate clear values. Given the low participation rates of the current voluntary opt-out system, the increasing concern of consumers, and the increasing volume of DNT signals that remain unanswered from users across the United States, it is clear that more is required—including continued congressional oversight. As we and industry thought leaders have observed, there is a better way to gain the user’s trust—through choice, control and transparency, and meaningful engagement with the user on the benefits and trade-offs of the current tracking practices.

¹⁵ See <http://www.donottrack.us/implementations>

¹⁶ “Firefox Cookie-Block Is The First Step Toward A Better Tomorrow,” Jim Spanfeller, *AdExchanger*, March 18, 2013; <http://www.adexchanger.com/the-sell-sider/firefox-cookie-block-is-the-first-step-toward-a-better-tomorrow/>

¹⁷ “Relax, Mozilla’s Move Will Not Break the Ad-Supported Internet,” Pam Horan, *Ad Age*, April 02, 2013; <http://adage.com/article/guest-columnists/mozilla-move-break-ad-supported-internet/240663/>

¹⁸ *Ibid.*

Thank you, again, Senator Rockefeller, Ranking Member Thune, and members of the Committee for the opportunity to join you today.

The CHAIRMAN. Thank you, Mr. Anderson, very much.
And now Mr. Mastria?

**STATEMENT OF LUIGI MASTRIA, CIPP, CISSP, MANAGING
DIRECTOR, DIGITAL ADVERTISING ALLIANCE**

Mr. MASTRIA. Chairman Rockefeller, Ranking Member Thune, and members of the Committee, thank you for the opportunity to testify today.

My name is Lou Mastria, and I am the Managing Director of the Digital Advertising Alliance.

The DAA is a nonprofit organization led by the leading advertising and marketing trade associations, representing more than 5,000 U.S. corporations. The DAA administers a comprehensive program of industry self-regulation for online data collection that provides enhanced consumer transparency and choice.

The DAA's Choice program also appropriately preserves consumers' strong preference for free, ad-supported content powered by relevant advertising, an approach that has helped sustain the astonishing growth and ever-expanding variety of Internet services and content. The DAA is the only program in the marketplace today that successfully provides an end-to-end system for controlling Web viewing data collected across unrelated sites.

This system is backed by strong and credible enforcement by the Council of Better Business Bureau and the DMA. The DAA provides enhanced transparency via the ubiquitous triangular blue icon from which consumers can access the DAA's universal, easy-to-use choice mechanism.

Since the program's launch, more than 23 million consumers have visited the DAA portal and education sites to learn about their choices. More than 8 million have visited the DAA opt-out tool, and nearly 2 million have taken action to exercise their choice.

I would like to emphasize five attributes of the DAA program that are frequently misrepresented by our critics. First, from its launch, the DAA has offered a simple, easy-to-use, one-button choice mechanism that works regardless of the type of browser used.

Second, the DAA principles apply to the collection of all Web viewing data across unrelated sites, not just data collected for advertising purposes.

Third, the DAA offers users persistent choice, that is to say choice that exists even after deletion of cookies.

Fourth, the DAA principles restrict both the collection and the use of data.

Fifth, the DAA's enforcement applies to all marketplace participants, regardless of whether they have enrolled in the DAA program.

At a highly publicized White House event last year announcing President Obama's framework for privacy, the then chairman of the Federal Trade Commission and the Secretary of Commerce, along with White House officials, publicly praised and endorsed the DAA's initiative. In fact, a senior White House official stated that

the DAA is “an example of the value of industry leadership as a critical part of privacy protection going forward.”

At this event, the DAA announced an agreement to honor the DAA principles through a browser signal when a consumer both receives meaningful information about the effect of that choice and affirmatively makes that choice themselves. Unfortunately, the DAA agreement at the White House was short-circuited, due to contrary approaches taken by both Microsoft and Mozilla.

Microsoft subsequently released its new version of IE 10 with what is “Do-Not-Track” turned on by default. This is in direct conflict with the agreement they helped develop at the White House.

In February this year, Mozilla announced that it will block third-party cookies. These actions do not advance consumer choice, and they will have a significant adverse effect on users’ Internet experience.

Cookies set by third parties play a vital role in the Internet ecosystem by facilitating consumer access to content and services. Blocking of third-party cookies would simply disrupt consumer’s online experience on the websites they use by reducing content personalization and the relevancy of ads that they receive.

This change would harm all Internet content services that use third-party technologies to understand and protect their audiences. In particular, it would disproportionately harm the numerous small publishers that are completely reliant on these technologies to operate and monetize their sites, thereby thwarting new job creation and chilling innovation.

For more than 4 years, the DAA has been responsive to the concerns of consumer advocates, regulators, and legislators. The DAA’s initial advertising principles met the FTC’s call for enhanced transparency. The DAA’s multisite data principles again met the call of regulators and consumer advocates to extend choice to all Web viewing data.

At the White House, again DAA, responding to regulators, agreed to honor its principles through a browser setting that would complement DAA’s existing choice mechanism. And soon the DAA will announce detailed guidance that provides transparency and control for the mobile Web applications and marketplace.

To be clear, the DAA is the solution provider here, not the problem. We are the only entity that actually delivered choice for consumers.

Today, the DAA calls on all stakeholders, including the FTC, the W3C, Microsoft, and Mozilla, to honor the terms of the White House announcement and remove impediments that are preventing implementation of browser-driven choice for consumers.

Thank you.

[The prepared statement of Mr. Mastria follows:]

PREPARED STATEMENT OF LUIGI MASTRIA, CIPP, CISSP, MANAGING DIRECTOR,
DIGITAL ADVERTISING ALLIANCE

Chairman Rockefeller, Ranking Member Thune, and Members of the Committee, good afternoon and thank you for the opportunity to speak at this important hearing.

My name is Lou Mastria. I am Managing Director of the Digital Advertising Alliance (“DAA”) and I am pleased to report to the Committee on the substantial progress of our Self-Regulatory Program.

The DAA is a non-profit organization led by the leading advertising and marketing trade associations including the Association of National Advertisers (“ANA”), the American Association of Advertising Agencies (“4As”), the Direct Marketing Association (“DMA”), the Interactive Advertising Bureau (“IAB”), the American Advertising Federation (“AAF”), and the Network Advertising Initiative (“NAI”) in consultation with the Council of Better Business Bureaus (“CBBB”). These organizations came together in 2008 to start developing the Self-Regulatory Principles for Online Behavioral Advertising, which were extended in 2011, beyond advertising, to cover the collection and use of Multi-Site Data across non-Affiliate sites over time. The DAA was formed to administer and promote these responsible comprehensive Self-Regulatory Principles for online data collection and use.

In response to the Chairman’s request for a status update on steps industry stakeholders have taken to fulfill their commitment to honor Do-Not-Track requests from consumers,¹ Since the fall of 2010, the DAA and its participants have been providing uniform choice to consumers. The DAA Program provides consumers with a one-button choice mechanism to stop the collection and use of web viewing data. This choice mechanism, which is consistent with the recommendations of the Federal Trade Commission (“FTC”) is being implemented: (1) to universally apply to all parties that collect web viewing data across nonaffiliated sites over time; (2) to be easy to find, understand, and use; (3) to make consumers’ choices persistent; (4) to be effective and enforceable; and (5) to apply beyond simply opting out of receiving interest-based tailored ads.² Furthermore, our program and choice tools share and meet the goals of the Chairman’s legislation—providing individuals with a simple and easy means to indicate their preference about the collection of such online viewing data. Unfortunately, some browser manufacturers have frustrated the DAA desire to extend the DAA program and tools to a browser setting. Nonetheless, the DAA and its participants today provide meaningful and effective consumer choice tools to consumers that with the click of one button provides consumers with the exact choice that a browser setting could provide. The DAA is the only system that provides an end to end system that captures all data viewing behavior, provides enhanced transparency in the form of an icon, and strong and credible enforcement to ensure compliance. The DAA stands committed to work with the Committee, these browsers and all organizations that are willing to join our efforts to provide meaningful choice while continuing to provide consumers with the Internet offerings that they cherish.

My testimony today will describe the commitment made by the DAA to extend its effective choice mechanisms to include browser-based signals, the threat to the Internet ecosystem posed by the actions of two browser manufacturers, and how the online advertising industry continues to successfully work to give consumers transparency and easy, uniform, and effective tools to control online data collection. Companies recognize that consumers have different preferences about online advertising and data collection and want to continue to build consumer trust in the online experience by ensuring that consumers have meaningful choices about how data is collected and used.

The DAA appreciates the Committee’s interest in exploring how consumer privacy concerns should co-exist with consumers’ desire for innovative products and services. Industry self-regulation coupled with consumer education effectively achieves this outcome. The DAA standards empower consumers to make choices about online data collection and use. Self-regulation is the appropriate approach because it is flexible and can adapt to rapid changes in technology and consumer expectations, whereas legislation and government regulation, particularly in such a rapidly-developing area, can stifle innovation, reduce competition, and add unnecessary costs.³ The

¹Hearing Notice: A Status Update on the Development of Voluntary Do-Not-Track Standards, available at http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=1cf8fb1a-fb0b-4bf1-958b-1ea3c443a73c.

²“FTC Report: Protecting Consumer Privacy in a, Era of Rapid Change—Recommendations for Businesses and Policymakers”, at 53 available at http://www.ftc.gov/os/2012/03/120326_privacyreport.pdf.

³See: http://cetucker.scripts.mit.edu/docs/law_summary_2011.pdf. In a congressional hearing on “Internet Privacy: The Impact and Burden of EU Regulation,” Professor Catherine Tucker of the MIT Sloan School of Management testified about the effect on advertising performance of the European Union’s e-Privacy Directive, which limits the ability of companies to collect and use behavioral data to deliver relevant advertising. Professor Tucker’s research study found that the e-Privacy Directive was associated with a 65 percent drop in advertising performance, measured as the percent of people expressing interest in purchasing an advertised product. The study also found that the adverse effect of such regulation was greatest for websites with content that did not relate obviously to any commercial product, such as general news websites. Professor Tucker cautions: “on the basis of this evidence, it is reasonable to say that privacy regulation

business community has a strong incentive to ensure broad, industry wide compliance with its self-regulatory principles and achieves this goal through the accountability that is built into our Self-Regulatory Program.

I. DAA's Commitment to Honor Browser-Based Opt-Out Mechanisms

For more than two years, the DAA has been offering an effective, one-button choice mechanism that empowers consumers to stop the collection of web viewing data for by third parties participating in the program. On February 23, 2012, at a White House event announcing President Obama's framework for privacy in the 21st Century, the Chairman of the Federal Trade Commission, the Secretary of Commerce, and White House officials publicly praised and endorsed the DAA's cross-industry initiative. In the words of one White House official, the DAA is "an example of the value of industry leadership as a critical part of privacy protection going forward."⁴ At this event, the DAA committed to developing a process to honor browser settings while providing consumers with the ability to make choices about the collection and use of web browsing data.

A. DAA Commitment to Honor a Users' Choices Through Browser-Based Tools

At the February 2012 White House event, the DAA committed to recognize browser-based header signals as a means of exercising the choices provided under the Self-Regulatory Principles. Specifically, at the event, the DAA read the following commitment reached with the DOC, FTC, and White House:

The DAA standard and corresponding enforcement of the standard will be applied where a consumer:

- (1) has been provided language that describes to consumers the effect of exercising such choice including that some data may still be collected and
- (2) has affirmatively chosen to exercise a uniform choice with the browser based tool.

The DAA standard will not apply in instances where (1) and (2) do not occur or where any entity or software or technology provider other than the user exercises such a choice.⁵

This framework is tied to an industry-consensus standard known as the *Self-Regulatory Principles for Multi-Site Data* that govern the collection and all uses of web viewing, including interest-based advertising.⁶ The framework also recognizes that consumers should be educated as to the effect of their choice, in particular they should be aware that if they exercise their choice: (1) they will still receive advertising but that ads may not be relevant to their interest; (2) consistent with the Self-Regulatory Principles, web viewing data may still be collected for narrow purposes including operational and system management purposes, fraud prevention and security, content delivery, market research, and product development; and (3) that data is vital to workings of the Internet ecosystem, and limiting collection can result in a reduced online experience.

The DAA committed to this standard because it provides consumer transparency, control, and education concerning the scope and effect of their choice while ensuring that a broad range of companies can continue to deliver products and services today and to innovate for tomorrow's marketplace.

B. Browsers' Subsequent Actions

Following the February 2012 White House event, the DAA set out to work toward implementing browser-based choice by the end of last year. The DAA efforts were short-circuited due to decisions by Microsoft and Mozilla. In particular, contrary to the agreement at the White House which Mozilla and Microsoft supported, they unilaterally chose to implement browser-based header signals, that they call "do not

could have sizable effects for the advertising-supported internet." Professor Tucker advises that "policymaking in the area of privacy regulation needs to be careful and fulfill the twin aims of protecting consumer privacy and ensuring that the advertising-supported Internet continues to thrive."

⁴ Speech by Danny Weitzner, *We Can't Wait: Obama Administration Calls for A Consumer Privacy Bill of Rights for the Digital Age* (February 23, 2012), available at <http://www.whitehouse.gov/blog/2012/02/23/we-can-t-wait-obama-administration-calls-consumer-privacy-bill-rights-digital-age> (last visited March 16, 2012).

⁵ DAA Position on Browser Based Choice Mechanism, available at https://www.aboutads.info/resource/download/DAA_Commitment.pdf.

⁶ DAA Self-Regulatory Principles for Multi-Site Data (November 2011), available at <http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf>.

track” signals, in a way inconsistent with the DAA commitment announced with the FTC, Department of Commerce, and White House.

Microsoft released its new version of Internet Explorer 10 (“IE10”) with a “do not track” tool turned “on” as a default setting in direct conflict with the commitment they supported at the White House that a user—and not the browser manufacturer—choose to exercise the choice mechanism in the browser setting. Machine-driven signals with the default on set by Microsoft do not represent user choice. The existing Microsoft system further compounds this problem by making it difficult in its settings for consumers to change the mandated default “on” setting. The DAA believes that a choice that prohibits data collection and use should not be made for the consumer by a browser or any other party. Allowing browser manufacturers to determine these choices for users limits the information and experience received by consumers, and consumers’ ability to enjoy the ad supported Internet provided by DAA participants and hundreds of thousands of other websites that consumers value. Most importantly, honoring the approach that Microsoft has elected to put in its browser was not part of the public commitment at the White House.

Mozilla has implemented what it refers to as a “do not track” tool in the current Firefox release also without following the White House agreement, for example by not describing for consumer the impact of their choice and creating inaccurate consumer expectations. Mozilla’s interface permits users to check a box to “Tell websites I do not want to be tracked.” Nothing more is provided to users; for example, consumers are not told that, by exercising such choice some data may still be collected. This implementation conflicts with the workable standard developed through industry consensus in 2012 and does not provide consumers with clear information about the effect of their choices.

The process for implementing the DAA’s commitment has been further delayed by the Worldwide Web Consortium (“W3C”), a technical standard-setting organization for web technologies, and its failure to reach any consensus after nearly two years of dialogue. Because the W3C is ill-equipped to address such public policy matters, its involvement has further complicated and protracted efforts to reach consensus on a standard and implementation for choice offered in the browser settings. This process is still ongoing and the DAA continues to participate in this forum.

C. DAA Offers a Universal Choice Mechanism

These browser implementations conflict with the DAA commitment, and are inconsistent with Chairman Rockefeller’s “Do Not Track Online Act” (S. 418). The Chairman’s bill calls for a standard by which “an individual can simply and easily indicate whether the individual prefers to have personal information collected.”⁷ This bill identifies the type of data subject to the tool and the effect of choice. The above-described browser implementations contain no standard for the types of data subject to the choice mechanism or the effect of exercising a choice. Without a standard governing when a browser-header signal is activated and what it means, a website or other entity receiving this signal will not know how to implement it. As a result, the signal could be ignored or, worse, treated differently by different signal recipients resulting in the consumer receiving no effect from the choice or receiving uneven results. This could cause confusion for consumers instead of comfort and security.

In contrast, we believe that the DAA’s current implementation is consistent with the Chairman’s bill and the recommendations set forth by the FTC. The DAA Principles, our Self-Regulatory Program, and our consumer choice tool enforced by credible accountability programs are the only mechanisms in the marketplace today that provide consumers with clear transparency, choice, and understanding about how their data will and will not be used. Through more than 1 trillion ad impressions served each month with the DAA’s Advertising Option Icon (“DAA Icon”), consumers can access the DAA’s universal, easy-to-use choice mechanism via www.aboutads.info/choices and www.youradchoices.com/control.aspx. This choice tool provides consumers with a single button to exercise choice against participating companies, either as a group or individually. When a consumer exercises choice—whether against all participants or a few—the affected participants stop collecting and using web viewing data from the user’s browser for interest-based advertising. Since the program’s launch in 2010, more than 23.5 million consumers have visited the DAA sites to learn about their advertising data choices, and, last year alone, more than a million consumers have taken action via DAA to exercise their choice about how advertisers will use their data.

⁷ S. 418, “Do Not Track Online Act, 113th Congress.

II. Mozilla's Technology Blocking Tool Could Harm Consumers and the Internet

In an act that is sure to further undercut consumer choice committed to at the White House and that will break critical Internet functionality, in February 2013, Mozilla announced that it will block cookies set by third parties in the upcoming release of its Firefox browser. Mozilla's decision to block technologies by certain types of companies will have a significant adverse impact on the Internet by reducing competition and diminishing the consumer's online experience.

A. Third Party Cookies are Vital to the Internet Ecosystem

Today's Internet is built around the technology of "cookies". Cookies are small text files that websites use to store information in order to make it easier for users to utilize and access web pages efficiently. For example, a website might use cookies to keep track of items a user has placed in a virtual "shopping cart." This well-established and very transparent technology enables the delivery of rich content, products, relevant advertising, and security and fraud prevention services. Recently, Mozilla has decided to selectively deny access to this technology, in effect picking winners and losers in the Internet ecosystem. The Internet, however, does not discriminate against technology based on its source. Affiliated companies operating differently branded domains could find their cookies blocked as third parties across these different domains. This blocking approach would also hurt a company's measures to provide security measures. Companies often implement security measures through third party domains or even their own differently branded domains. Mozilla would thwart these security efforts by preventing companies from setting cookies for security purposes in these multiple domains. This change harms not only third parties, but all companies that rely on integrated services, particularly the large number of small publishers that rely on service providers to operate and monetize their sites.

The Internet is a complex ecosystem comprised of a diverse set of actors including web publishers, content providers, ad networks, analytics firms, security and fraud prevention providers, exchanges, advertisers, plugin providers, and many other actors. These entities work seamlessly together to provide content and services to the benefit of consumers. Cookies set by third parties play a vital role in this ecosystem by facilitating consumer demand for content and services. Cookies are also vital to interest-based advertising ("IBA"). IBA provides consumers with a more relevant online experience by providing information about products and services that more likely relevant to their. Blocking third-party cookies will prevent third parties from fulfilling these roles, in turn disrupting consumer services, lessening online relevancy and security, and destroying many Internet business models.

B. Blocking Third Party Cookies Will Restrict Consumers' Access to Content and Services

Today, hundreds of thousands of publishers deliver mainstream and niche content for free or at low cost. Web publishers rely on third parties to help select, provide, and display relevant content to visitors to their publisher sites. On any given website, content such as news feeds, weather tools, social plugins, or emergency response and safety information (e.g., Amber alerts) are often provided by a third party integrated into the publisher's site for a seamless appearance and experience for the user. Third parties also enhance content quality, providing information relevant to the browser user's interests, and securing the user's safety when browsing or shopping on a site. All of these essential services are typically delivered through cookie technology. Mozilla's denial of the use of cookies would prevent third parties from providing these services resulting in blocked access to content, and a slower, less optimized, and less safe consumer experience online. In order to receive the Internet that works effectively and gives consumers the services they are used to receiving, it will be time for consumers to change their browser.

Mozilla's cookie-blocking approach will lead U.S. consumers down a path where a few large companies can control the amount and diversity of content made available online. Not that long ago, television was comprised of three networks that selected and delivered all programming to consumers. Through advances in technology and infrastructure, consumers may now access a rich diversity of television content. The Internet delivers an even more stunning array of content because of the low barriers to entry. Consumers value these choices, and should not have their online experience be forced back into a 1970s television construct where a few control the content that consumers can access. In short, Mozilla's actions could significantly hurt the Internet, consumer experience and choice to have robust content offerings.

C. Blocking Cookies Disadvantages Small Businesses

Advertising fuels the Internet economic engine. The support provided by online advertising is substantial and growing despite the difficult economic times we are facing. The online advertising industry is a beacon for innovation and job creation. In 2012, Internet advertising revenues reached a new high of \$36.6 billion, an impressive 15 percent higher than 2011's full-year number.⁸ Because of this advertising support, small and medium-size publishers can provide consumers with access to a wealth of online resources at low or no cost. Revenue from online advertising facilitates e-commerce and subsidizes the cost of content and services that consumers value, such as online newspapers, weather, Do-It-Yourself websites, blogs, social networking sites, mobile applications, e-mail, and phone services. According to a recent poll by Zogby Analytics, 92 percent of Americans think free content like news, weather and blogs is important to the overall value of the Internet.⁹

This model delights consumers and creates jobs across America, fostering a competitive marketplace that drives down prices for consumers and costs for businesses. The Internet is a tremendous engine of economic growth. It has become the focus and a symbol of the United States' famed innovation, ingenuity, inventiveness, and entrepreneurial spirit, as well as the venture funding that flows from these enormously productive and positive efforts. A 2009 study found that more than three million Americans in every U.S. state are employed due to the advertising-supported Internet, contributing an estimated \$300 billion, or approximately 2 percent, to our country's GDP.¹⁰ There is employment generated by this Internet activity in every single congressional district in every state across the United States.¹¹

Recently, more than 700 small publishers signed an open letter to Mozilla requesting that it reconsider its decision to block third-party cookies.¹² These small publishers rely on third party cookies for content delivery as well as the delivery of advertising that subsidizes their provision of online services, products, and content through their websites. Small-business website publishers that cannot afford to employ advertising personnel to sell their advertising space, and may not even be on the radar of large brand-name advertising campaigns, can increase their revenue by featuring advertising that is more relevant to their users. This is commonly done through third-party platforms, often offered on a self-serve basis, that allow publishers to add advertising to their sites efficiently and easily. In turn, advertising-supported resources help other small businesses to grow. Small businesses can use free or low-cost online tools, such as travel booking, long-distance calling, and networking services, to help them run their companies.

III. DAA Approach Is Successful

The DAA is a broad-based self-regulatory program established by the leading advertising and marketing industry associations. The program is led by the 4As, AAF, ANA, DMA, IAB, and the NAI. The DAA program unites these major trade associations representing thousands of online companies across the full spectrum of advertising services (including web publishers, advertisers, third-party ad networks, and exchanges). The DAA program is based on seven core Self-Regulatory Principles: education, transparency, consumer control, data security, controls with respect to material changes to policies and practices, heightened safeguards for sensitive data, and accountability. The DAA offers several interrelated mechanisms to deliver consumers enhanced transparency and a ubiquitous and easy-to-use choice mechanism as described below.

A. Consumer Disclosure through the Advertising Option Icon

The DAA program has developed a universal icon to give consumers transparency and control for interest-based ads. The icon provides consumers with notice that information about their online interests is being gathered to customize the web ads they see. Clicking the icon also allows consumers to choose whether to continue to allow this type of advertising.

⁸Interactive Advertising Bureau Press Release, "Internet Ad Revenues Again Hit Record-Breaking Double-Digit Annual Growth, Reaching Nearly \$37 Billion, a 15 percent Increase Over 2011's Landmark Numbers" (April 16, 2013) (reporting results of PricewaterhouseCoopers study).

⁹Interactive Survey of U.S. Adults commissioned by the DAA (April 2013), available at http://www.aboutads.info/resource/image/Poll/Zogby_DAA_Poll.pdf.

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

¹¹*Id.* at 53.

¹²Open Letter to Mozilla, available at http://www.iab.net/mozilla_petition/.

The icon is served over *one trillion times each month* on or next to Internet display ads on websites covered by the program. The DAA reached this milestone within a short 18 months from program launch. This achievement represents an unprecedented level of industry cooperation and adoption.

B. Consumer Control

At the *www.aboutads.info* website and accessible from the companion *www.youradchoices.com* website, the DAA program makes available a choice mechanism that unites the opt-out mechanisms provided by more than 114 different third-party advertisers participating in the program. We estimate that the DAA program coverage is approaching 100 percent participation of the interest based ads being delivered. The choice mechanism offers consumers a “one-click” option to request opt outs from all participants or allows a user to make choices about specific companies. Consumers are directed to *aboutads.info* not only from icon-based disclosures on or around ads, but from other forms of website disclosure. The site also contains other educational and informational materials about the DAA program and its participants. Since program launch, there have been more than 16 million page views of our choice portal. More than a year ago, the DAA also introduced a suite of browser plug-ins to help ensure the persistency of these choices.

In 2012, more than 5.2 million unique users accessed the resources provided at *www.aboutads.info*. Of those visitors, nearly one million unique users have exercised choice using the integrated opt out mechanism provided at that site; nearly two million unique visitors have opted out since the program launch. Many users visit the website, learn about their choices, and ultimately choose not to opt out. We believe that this shows that once consumers understand how online advertising works, many prefer to receive relevant ads over irrelevant ads. Research supports this proposition. A recent poll of U.S. consumers shows that 68 percent of Americans prefer to get at least some Internet ads directed at their interests with 40 percent of Americans prefer to get all their ads directed to their interests.¹³

C. Consumer Education

The DAA is deeply committed to consumer education. In 2012, the DAA launched a dedicated educational site at *www.YourAdChoices.com*. The site provides easy-to-understand messaging and informative videos explaining the choices available to consumers, the meaning of the Advertising Option icon, and the benefits they derive from online advertising.

In 2012, companies participating in the DAA program voluntarily donated more than four billion impressions to support an educational campaign for *www.YourAdChoices.com*. Since the campaign launch in late January 2012, more than 13.5 million unique users have visited the site, an average of about one million visitors each month. This site also provides access to the DAA’s user choice mechanism. The combination of the educational campaign and the ubiquitous availability of the Advertising Option Icon have significantly increased consumer usage of the DAA program tools. Indeed, the 5.2 million unique visitors to *www.aboutads.info* in 2012 are more than three times the 2011 figure.

D. Commitment to Accountability

For the past 40 years, the advertising industry has distinguished itself through its self-regulatory systems for independent oversight of compliance and public reporting of enforcement actions. In keeping with this tradition, a key feature of the DAA Self-Regulatory Program is accountability. All of DAA’s Self-Regulatory Principles are backed by the robust enforcement programs administered by the Council of Better Business Bureaus (“CBBB”) under the policy guidance of the Advertising Self-Regulatory Council (ASRC), and by the DMA under its Guidelines for Ethical Business Practice. In addition to the oversight provided by the CBBB and DMA compliance programs, the NAI also has a strong compliance program. The NAI compliance program includes pre-certification reviews, ongoing technical monitoring of member companies’ opt-out scripts, annual compliance reviews, mechanisms for accepting and investigating complaints alleging non-compliance, and annual reporting. The NAI’s compliance program, like the CBBB and DMA programs, helps members to comply with their self-regulatory obligations, and to hold them accountable.¹⁴

The CBBB Accountability Program builds on the successful track records of the other ASRC programs: the National Advertising Division, operating since 1971; the Children’s Advertising Review Unit, operating since 1974; and the Electronic Retail-

¹³Interactive Survey of U.S. Adults commissioned by the DAA (April 2013), available at <http://www.aboutads.info/DAA-Zogby-Poll>.

¹⁴NAI 2012 Compliance Report, available at http://www.networkadvertising.org/2012_NAI_Compliance_Report.pdf.

ing Self-Regulation Program, operating since 2004. These programs feature independent monitoring, public reporting of decisions and referral to government agencies, often to the Federal Trade Commission, of any uncorrected non-compliance. They have extremely high voluntary compliance rates. In fact, over 90 percent of companies voluntarily adopt the recommendations of these programs. Those companies that fail to comply or refuse to participate in the self-regulatory enforcement process are referred publicly to the appropriate government agency for further review.

The CBBB administers its Interest-Based Advertising Accountability Program under the ASRC self-regulatory policy guidance and procedures. Because of the highly complex, technical and interdependent nature of interest-based advertising, the Accountability Program receives a weekly privacy dashboard report based on independent data about more than 250 companies' compliance with various requirements of the Principles. The Accountability Program's technical staff analyzes these data and independently performs further research to determine whether there may be a violation of the Principles warranting formal inquiry. Like other ASRC programs administered by the CBBB, the CBBB Accountability Program also finds potential cases through its own staff monitoring and investigation, by analysis of consumer complaints and reviews of news stories and technical reports from academics and advocacy groups. Where there is a potential compliance issue, the CBBB initiates formal inquiries and works to ensure the company understands the Principles and voluntarily implements the requirements of the Principles. At the end of the process, the CBBB Accountability Program issues a public decision, which details the nature of the inquiry, the Accountability Program's conclusions, any recommendations for correction, and includes a statement from the company in question regarding its implementation of the recommendations. A press release is also issued.

The CBBB's Accountability Program has brought 19 cases since November 2011, and has a 100 percent track record of voluntary industry compliance with its recommendations. The CBBB Accountability Program has focused its inquiries on the key concepts of transparency and choice under the DAA's Self-Regulatory Principles. In its initial round of cases, the Accountability Program investigated whether companies were correctly and reliably providing consumers with an effective choice mechanism. Cases involved defective links to opt-out mechanisms and opt outs that failed to meet the OBA Principles' five-year minimum opt-out period.

The CBBB Accountability Program's recent decisions provided companies with guidance on a range of important compliance issues involving the DAA's Transparency and Consumer Control Principles. For example, in a case in which a newly-established company was unaware of the Principles and therefore out of compliance, the CBBB Accountability Program made clear that the Principles cover the entire advertising ecosystem and that all companies are expected to comply with these requirements. In other cases, the Accountability Program has demonstrated the flexibility of self-regulation by applying the Principles to diverse technologies and to evolving business models.

The DMA's enforcement program likewise builds on a long history of proactive and robust self-regulatory oversight. The DMA's longstanding *Guidelines for Ethical Business Practice* ("Guidelines") set out comprehensive standards for marketing practices, which all DMA members must follow as a condition of membership. The DAA Self-Regulatory Principles are incorporated into these Guidelines.

The DMA's Committee on Ethical Business Practice examines practices that may violate DMA Guidelines. To date, the DMA Guidelines have been applied to hundreds of marketing cases on a variety of issues such as deception, unfair business practices, personal information protection, and online behavioral advertising. In order to educate marketing professionals on acceptable marketing practices, a case report is regularly issued which summarizes questioned direct marketing promotions and how cases were administered. The report also is used to educate regulators and others interested in consumer protection issues about DMA Guidelines and how they are implemented.

The Committee on Ethical Business Practice works with both member and non-member companies to gain voluntary cooperation in adhering to the guidelines and to increase good business practices for direct marketers. The DMA Corporate Responsibility team and Ethics Committee receive matters for review in a number of ways: from consumers, member companies, non-members, or, sometimes, consumer protection agencies. Complaints are reviewed against the Guidelines and Committee members determine how to proceed. If a potential violation is found to exist, the company will be contacted and advised on how it can come into full compliance.

Most companies work with the Committees to cease or change the questioned practice. However, if a member company does not cooperate and the Committee be-

believes there are ongoing guidelines violations, the Committee can recommend that action be taken by the Board of Directors and can make case results public. Board action could include censure, suspension or expulsion from membership, and the Board may also make its actions public. If a non-member or a member company does not cooperate and the Committees believe violations of law may also have occurred, the case is referred to Federal and/or state law enforcement authorities for their review.

The CBBB and DMA programs demonstrate the success of self-regulation and its many benefits, including the ability for the regulatory apparatus to evolve to meet new challenges. Importantly, accountability under the Principles applies to all members of the advertising ecosystem, not merely “members” of the various organizations.

E. Application of Self-Regulatory Principles to Data Collected on Mobile Devices

Industry self-regulation is especially appropriate for the technology sector because it is nimble. The DAA Self-Regulatory Program is adapting over time and we expect this evolution to continue with changes in the marketplace driven by technological advancements and evolving consumer preferences. Currently, the DAA is finalizing new implementation guidance responding to the fact that companies operate across a variety of channels including mobile. The guidance will explain how the Self-Regulatory Principles apply to certain data practices that may occur on mobile or other devices.

Stakeholders representing all major elements of the mobile ecosystem participated in the development of this guidance. The guidance will clarify that the previously-issued Self-Regulatory Principles apply to the mobile web environment. In addition, the guidance will explain how the Transparency and Consumer Control Principles apply to “Cross-App” data—data collected from a device across non-affiliated applications over time. The DAA will build on the success of its existing web-based uniform choice mechanism by working with DAA stakeholders to develop and implement, or otherwise specify, a companion choice mechanism for Cross-App Data. This new tool will offer consumers an unprecedented level of control over third-party data collection across applications on a device.

The guidance will also ensure Transparency and Consumer Control for both Precise Location Data and Personal Directory Data, the term encompassing calendar, address book, phone and text logs, or photo and video data created by a consumer that is stored on or accessed through a device. Any entity engaged in the collection and use of Cross-App Data, Precise Location Data, or Personal Directory Data will be subject to the DAA accountability mechanisms. As discussed above, these robust accountability mechanisms can, and do, review an entity’s practices regardless of whether that company has announced its adherence to the DAA Self-Regulatory Principles.

F. Benefits of Industry Self-Regulation

The DAA’s commitment to self-regulation has put us at the forefront of new consumer protection initiatives. The DAA believes that self-regulation is the appropriate approach for addressing the interplay of online privacy and responsible data collection and use practices. We appreciate the positive recognition of the White House and the Federal Trade Commission for our efforts. Our approach has been successful in addressing consumer concerns while ensuring that the U.S. Internet economy remains vibrant. Self-regulation provides industry with a nimble way of responding to new challenges presented by the evolving Internet ecosystem. For our information-driven economy to thrive and continue as an engine of job creation, self-regulation led by industry codes of conduct is the ideal way to balance privacy and innovation. The DAA is also a global leader in self-regulation. The DAA Program has been implemented in close to 30 countries including throughout Europe soon to be launched elsewhere. The success means a standard consumer experience and universal standards for business operating around the world.

We believe that our commitment to and success in advancing industry self-regulation obviates the need for new legislation. We remain concerned that laws and regulations are inflexible and can quickly become outdated in the face of extraordinarily rapidly-evolving technologies. When this occurs, legislation thwarts innovation and hinders economic growth and can impede a competitive marketplace that offers a full range of choice to consumers. We believe, however, as we have noted that our DAA program furthers the goals of the legislation introduced by Chairman Rockefeller, while allowing for the more rapid and flexible response to marketplace developments that are so pronounced in the Internet and new media environment.

The DAA has championed a balanced approach to consumer control that both accommodates consumers’ privacy expectations and supports the ability of companies

to deliver services and continue innovating. This balance is essential to allow consumers to continue to receive and enjoy the diverse range of websites and services subsidized by relevant advertising.

Industry has invested tens of millions of dollars to develop the DAA program, which is one of the most successful and fastest-developing consumer choice systems in the world.

The CHAIRMAN. Thank you.

And now Mr. Justin Brookman, Project on Consumer Privacy.

**STATEMENT OF JUSTIN BROOKMAN, DIRECTOR, CONSUMER
PRIVACY, CENTER FOR DEMOCRACY & TECHNOLOGY**

Mr. BROOKMAN. Chairman Rockefeller, Ranking Member Thune, members of the Committee, thank you very much for the opportunity to testify here today.

I am Director of Consumer Privacy at the Center for Democracy and Technology. I am also an editor and a member of the W3C's working group working on Do-Not-Track.

And this issue of behavioral advertising obviously is one that we have wrestled with for over 15 years now. And Chairman, I share your frustration that it is one we haven't gotten right.

Today, people still don't understand—

The CHAIRMAN. Sir, can you bend that down just—there you go.

Mr. BROOKMAN. I can. Does that help?

All right. People don't understand they are being monitored online, and users feel less in control and more tracked than ever. I think people understand the tradeoff that they can view free content online in exchange for seeing ads. What I think they don't get and often would not accept is that they are getting content in exchange for the surveillance of their reading and browsing habits.

So for a number of years, some privacy advocates argue that we should have opt-in consent, opt-in consent for these companies we have no relationship with monitoring our activities to build up profiles to service ads. And in response, industry said, no, opt-out is good enough.

And over time, at least here in the U.S., industry won that fight. Calls for opt-in permission went unheeded, and legal challenges failed.

But if you are going to have a system based on opt-out rights, you need a global opt-out so users can opt out all at once, telling all parties on a site, "Hey, leave me alone. Don't track me." Users cannot reasonably be expected to track down every single company that is monitoring them and tell them to stop individually.

And industry in principle agrees with this, so, as Mr. Mastria described, the DAA has for a couple of years now offered a site you can go to, to opt out of behavioral advertising for member companies. Unfortunately, the system suffers from a number of fundamental flaws.

One, it is not universal. The choice only applies to DAA member companies. Companies that don't pay DAA for membership are not included and receive no indication that an individual user doesn't want to be tracked.

It is almost always based on cookies. So when you opt out, DAA member companies put tracking cookies in your device. If that gets

deleted, your opt-outs go away, and companies don't know that you don't want to be tracked.

And the program does not meaningfully address collection and retention. Opting out turns off behavioral advertising, but member companies can still monitor you and collect data about you for research or product improvement purposes with no data retention limits.

At the same time, behavioral tracking has expanded dramatically in the last couple of years. So sites that used to place one or two cookies on your device are now dropping hundreds from dozens from different companies.

A recently released study from Evidon shows the number of tracking companies and websites have gone up 53 percent in the last year alone. This led one longtime industry insider to conclude in an op-ed titled "Suicide by Cookies" self-regulation hadn't worked the way we promised Washington it would.

And so, it was before this committee 3 years ago that then-Chairman Leibowitz said that users need a reliable, easy to find, persistent global opt-out like Do-Not-Track. And to their credit, the browsers reacted pretty quickly. So, today, all major browsers can easily send Do-Not-Track signals. However, the advertising industry has been less willing to adapt.

Finally, as you mentioned, Chairman Rockefeller, in February 2012, four and a half years after advocates first called for Do-Not-Track and a year and a half after Chairman Leibowitz called for it here, the DAA said it would "begin work" on letting users use browser settings to express choice. And at that time, they said, "The DAA expects that such functionality will be implemented within 9 months."

Now it is 14 months later, and only a handful of DAA companies are responding to DAA headers at all. Efforts to come up with consensus meaning of Do-Not-Track in the World Wide Web Consortium have ground to a standstill, and for over a year now, the group has seen no movement on the key issues, such as whether cookies can be set when Do-Not-Track is turned on, whether companies can track for market research when Do-Not-Track is turned on, whether and how companies need to de-identify data they get, whether ad networks can reject DNT settings from browsers that turn on Do-Not-Track by default.

And data retention. I mean, if, at the end of the day, ad companies can still log and retain individual-level data for years and years and Do-Not-Track was turned on, what privacy have we really achieved?

But we are not even to that point yet. Mozilla has been sending out these signals for over 2 years now for users who go out of their way to turn on Do-Not-Track, and a few companies, like Yahoo! and BlueTie, treat it as an opt-out. But most just ignore it.

Google Chrome has a Do-Not-Track setting that meets every possible test DAA could want. It is not on by default. There is explanatory text. There is a link for more information. You can't just do it with one click, and companies are ignoring those, too.

I am personally still hopeful that a compromise can be worked out after all this time because if the industry, the advertising industry won't agree to a meaningful standard, the browsers have

shown they are going to fight back. So Mozilla has moved to disable cookies, at least in the short term, so that the browsers understand unfettered data collection and retention isn't necessary for the Net to work.

After all, Apple's Safari browser has blocked cookies for years and is far more restrictive than a negotiated DNT setting would be, and the Web works just fine on Apple devices. So much of the privacy debate in this country is focused on just this one narrow issue, and for years, we haven't had resolution.

Ultimately, we really need to fundamentally rework our privacy framework in America. Citizens deserve basic privacy rights over all commercial collection of data, and they need due process of law before Government access. Only then will consumers in this country have confidence their privacy is being protected.

Thank you very much for the opportunity to testify, and I look forward to responding to the Senators' questions.

[The prepared statement of Mr. Brookman follows:]

PREPARED STATEMENT OF JUSTIN BROOKMAN, DIRECTOR, CONSUMER PRIVACY,
CENTER FOR DEMOCRACY & TECHNOLOGY

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today. We applaud the leadership the Chairman has demonstrated in examining the challenges in developing a consensus Do Not Track standard and appreciate the opportunity to address the continued insufficiency of self-regulatory consumer privacy protections.

CDT is a non-profit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the decentralized Internet. I currently serve as the Director of CDT's Consumer Privacy Project. I am also an active participant in the Worldwide Web Consortium's Tracking Protection Working Group, where I serve as editor of the "Tracking Compliance and Scope" specification—the document that purports to define what Do Not Track should mean.

My testimony today will briefly describe the history of online behavioral advertising and the genesis of the Do Not Track initiative. I will then describe the current state of the World Wide Web Consortium's efforts to create Do Not Track standards and the challenges going forward to implement Do Not Track tools successfully. I will conclude with my thoughts on the future of Do Not Track, and why I believe that this protracted struggle demonstrates the need for the fundamental reform of our Nation's privacy protection framework for commercial and government collection and use of personal information.

The Rise of Behavioral Advertising

Online behavioral advertising has been a concern for regulators and privacy advocates for over fifteen years now. Behavioral advertising, or more specifically *cross-site* behavioral advertising, was originally made possible because of two core capabilities afforded by web browsers: cookies and referer headers. Cookies are small bits of code that the operator of a website can store locally on a user's computer—among other things, they can be used as unique IDs so that a website can recognize a particular user (or device) when the user returns to a particular website. Originally conceived as a means for first-party services to keep remember a user over time, soon advertising networks—the companies that websites often use to generate ads for them—began to place unique cookies' on web users' browsers as well. Because web browsers typically identify the referring site when it passes along a web request (the "referer header"), advertising networks were informed of the precise webpage they served a user a particular advertisement. Combining cookies and referer headers together, advertising networks were able to generate detailed logs of the various websites they encountered a particular user.

Eventually, these companies began analyzing this web history to help inform decisions about which ads to show particular users. When an advertiser has a presence on many sites a user may visit, it is able to develop a trail of past web surfing behavior consisting of a list of many individual actions a user has taken online. These trails are very unique in the sense that no two people do exactly the same things online, so advertisers are able to leverage this very rich, unique view of each user to make split-second decisions about what ads to show them that they will have the

highest likelihood of noticing and interacting with. In a nutshell, that's what behavioral advertising is—utilizing information about previous sites visited by a particular user to influence decisions about what ads to show in the future.

As the behavioral advertising industry took off, many privacy advocates complained that users did not understand that their cross-site behavior was being tracked by companies they had never heard of, and urged that users should have to affirmatively consent to the tracking of their web surfing habits. In 2000, a class action suit was filed against DoubleClick, a leading behavioral advertising company, arguing that the company's tracking users without consent across websites violated the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act. At the same time, the Federal Trade Commission investigated DoubleClick's behavioral advertising practices, and the allegations that DoubleClick intended to attach real names to behavioral profiles. Eventually, the *DoubleClick* lawsuit was dismissed,¹ and the FTC discontinued its investigation of the company, declining to allege that the company's tracking of users without explicit consent violated existing law.²

However, while advocates' call for *opt-in* consent for behavioral tracking went unheeded, industry has always acknowledged that users should at least have the right to *opt out* of behavioral advertising.³ Moreover, for years, there has been general recognition that there must to be a *global* way to opt out of *all* behavioral tracking at once—users cannot reasonably be expected to locate all potential tracking companies and one-by-one opt out of their tracking. Thus, already today, the Digital Advertising Alliance (DAA)—the umbrella self-regulatory group consisting of the Interactive Advertising Bureau, Network Advertising Initiative, Better Business Bureau and others—maintains a site through which users can globally opt out of behavioral advertising by its member companies.⁴

Unfortunately, there are several limitations to industry's current opt-out structure:

- It only applies to advertisers that are members of the DAA; companies that don't sign up and pay for membership are not included, and receive no indication that a user does not want to be tracked.
- The opt-out is almost always cookie-based. If a user deletes her cookies—or if they are routinely deleted by her anti-virus software, as is often the case—the opt-out disappears, and companies subsequently have no way of knowing that the user does not want to be tracked.
- The opt-out only prevents users from seeing targeted ads, which are based on information gathered from tracking. However, it does not prevent tracking itself. While the DAA's Multi-Site Principles in principle agree with the notion of collection limitation, in practice, the code's bases for collection are extremely broad, and any justification to understand “consumer preferences and behaviors [or] research about consumers, products, or services” could justify individualized data collection despite the user's opting out.⁵
- The interface through which users are presented their choices around tracking and opting out both through the AdChoices icon and on the DAA website are confusing.⁶

Coupled with the limitations of the industry's opt-out approach, industry self-regulation has failed to grapple with the dramatic expansion of the scope of tracking online. Websites that used to embed one or two tracking cookies now embed dozens. A *Wall Street Journal* report found that the top 50 websites placed over 3,000 tracking files on a test computer; IAC Interactive's Dictionary.com alone placed 223

¹*In re DoubleClick, Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

²Letter from the Federal Trade Commission to Christine Varney, January 22, 2001, Re: DoubleClick, Inc., <http://www.ftc.gov/os/closings/staff/doubleclick.pdf>.

³FTC Staff Report, Public Workshop on Consumer Privacy on the Global Information Infrastructure, December 1996, <http://www.ftc.gov/reports/privacy/Privacy1.shtm>, at I.I.C.2 (Consumer Choice).

⁴Digital Advertising Alliance, <http://www.aboutads.info/choices/>.

⁵Digital Advertising Alliance, Self-Regulatory Principles for Multi-Site Data, <http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf>.

⁶A. M. McDonald and Lorrie Faith Cranor, *Social Science Research Network*, “Beliefs and behaviors: Internet users' understanding of behavioral advertising,” October 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092; Pedro G. Leon *et al.*, *Carnegie Mellon University CyLab*, “Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising,” October 2011, http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html.

tracking files from a variety of third-party companies.⁷ In the past year alone, the number of web tracking tags on websites has gone up 53 percent, nearly half of which were embedded not by the first-party publisher, but by ad networks embedding their own tags to transmit data to still other companies.⁸ Moreover, tracking that used to be pseudonymous (profiles tied to a device, but not a name) are increasingly linked or easily linkable to real world identities.⁹ Last December, for example, the *Wall Street Journal* reported on a company named Dataium that tracked users by e-mail address, and sent descriptions of online surfing to offline companies with which users had shared that same e-mail address.¹⁰ Industry trade associations have failed to adapt to address new business models predicated on expanded and more personal tracking. As one long-time industry player summarized recently: “Self-regulation hasn’t worked the way we promised Washington it would.”¹¹

The Call for Do Not Track

Given the longstanding inadequacy of industry self-regulatory control options, in October 2007, CDT and other consumer advocacy organizations called on the Federal Trade Commission to create a Do Not Track list, similar to the successful “Do Not Call” list that allows users to opt out of telemarketing. Under the original formulation for Do Not Track, online advertisers would have to self-identify to the FTC, which would then compile a list of their domains that track consumers. Browsers that supported Do Not Track would then block any third-party communications to domains on the FTC’s block list.¹² Only ad networks that did not use unique identifiers to track users around the web would be able to serve advertisements. As a result, users who turned on Do Not Track would simply see ads that were not specialized for them, since advertisers would not have access to the consumers’ recent history on the Web to surmise their interests.¹³

Initially, advocates’ call for Do Not Track functionality went nowhere. In July of 2009, researcher Christopher Soghoian and Mozilla privacy engineer Sid Stamm created a prototype add-on for Firefox, which reformulated Do Not Track as a persistent HTTP header appended to all web requests. This would give consumers the option of sending out a digital signal each time the user visits a website, asking companies to stop tracking them from site to site. The Do Not Track header was in many ways an improvement over the original concept, as it did not rely on tracker self-identification, and did not require a centrally-hosted list of tracking domains. However, this approach was offered initially as a proof-of-concept, and was not implemented into the Mozilla Firefox browser.¹⁴

In July 2010, then-FTC Chairman Jon Leibowitz testifying before this Committee effectively resurrected the idea of Do Not Track, and called upon browser makers and ad networks to work together to implement this technology.¹⁵ The FTC formally recommended the development of Do Not Track in its 2010 draft privacy report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*.¹⁶

⁷ Julia Angwin, “The Web’s New Gold Mine: Your Secrets,” *The Wall Street Journal*, July 30, 2010, <http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html>.

⁸ George Simpson, “Suicide by Cookies,” *MediaPost*, February 22, 2013, <http://www.mediapost.com/publications/article/194073/suicide-by-cookies.html#axzz2REncGaSy>.

⁹ Justin Brookman, CDT blog, “Why Facebook Apps Story is Problem for Entire Web,” October 19, 2010, <https://www.cdt.org/blogs/justin-brookman/why-facebook-apps-story-problem-entire-web>.

¹⁰ Jennifer Valentino-Devries and Jeremy Singer-Vine, “They Know What You’re Shopping For,” *Wall Street Journal*, December 7, 2012, <http://online.wsj.com/article/SB10001424127887324784404578143144132736214.html>.

¹¹ George Simpson, “Suicide by Cookies,” *MediaPost*, February 22, 2013, <http://www.mediapost.com/publications/article/194073/suicide-by-cookies.html#axzz2REncGaSy>.

¹² *Tech Law Journal*, “CDT Proposes That FTC Create a Do Not Track List for Consumer Internet Use,” October 31, 2007, <http://www.techlawjournal.com/topstories/2007/20071031.asp>.

¹³ Louise Story, *The New York Times*, “Consumer Advocates Seek a ‘Do-Not-Track’ List,” October 31, 2007, http://www.nytimes.com/2007/10/31/technology/31cnd-privacy.html?_r=0.

¹⁴ Emil Protalinski, *The Next Web*, “Everything you need to know about Do Not Track: Mozilla vs Google & Microsoft,” November 25, 2012, <http://thenextweb.com/apps/2012/11/25/everything-you-need-to-know-about-do-not-track-currently-featuring-microsoft-vs-google-and-mozilla/>.

¹⁵ Jeffrey S. Edelstein and Linda A. Goldstein, *Lexology*, “Privacy Update: Senate bill and FTC ‘Do-Not-Track’ list?” August 12, 2010, <http://www.lexology.com/library/detail.aspx?g=5cf00693-fda7-4d91-a1b1-61a70f795565>.

¹⁶ Federal Trade Commission Report: Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework For Businesses and Policymakers, December 2010, <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>. This call was repeated in the final version of the report issued 16 months later. Federal Trade Commission Report: Protecting Consumer Pri-

In response to Chairman Leibowitz's call, browser makers moved surprisingly quickly to offer Do Not Track features. One week after the draft report was released, Microsoft announced that Internet Explorer 9 would include Tracking Protection Lists, which give consumers the option to block communications to all third-party domains listed on a specific blacklist.¹⁷ This approach mirrored the advocates' original 2007 conception of Do Not Track, which was predicated on blocking tracking domains. However, rather than rely on a centralized list of trackers, Microsoft encouraged others to create and publish their own list of trackers for users to download.

The next month, Mozilla announced it would implement the header approach to Do Not Track in its Firefox web browser, allowing users to send out a persistent header to all websites indicated a preference not to be tracked. Quickly, popular support within the privacy community coalesced around the notion that the header approach was the most viable way to implement Do Not Track, and within several months, all the major browsers offered users a means to append Do Not Track headers to all web requests.¹⁸

Perhaps most significantly, in February of 2012, at a White House event to announce President Obama's proposed comprehensive privacy protection framework, the DAA announced that it would begin work to allow users to opt out of behavioral advertising using browser based headers. At the time, the DAA stated that it would enforce its self-regulatory choice principles when a user had been provided information about "the effect of exercising such a choice," and when the user had affirmatively chosen to exercise her choice using the browser based header.¹⁹ The DAA stated in February of 2012, "The DAA is committed to making such choices work for all consumers. . . . The DAA expects that such functionality will be implemented within nine months."²⁰

Status of Do Not Track Today

However, despite industry's commitment from 14 months ago, today, only a handful of third-party companies acknowledge and respond to Do Not Track headers in any way.²¹

For some time, the delay in implementation was perhaps justified by a lack of agreement on what exactly the Do Not Track signal should mean. Much of this debate has taken place within the Tracking Protection Working Group of the World Wide Web Consortium (W3C). W3C is a voluntary web standards setting body made up of industry members, privacy advocates, and academic experts; historically they have promulgated standards for the Web on a wide range of matters, such as Web Design and Applications, Web Architecture, and the Semantic Web.²² The Tracking Protection Working Group was established originally in response to Microsoft's request to standardize Tracking Protection Lists, but was subsequently chartered to form a standard for a universal Do Not Track request tool.²³

However, this delay has become less defensible over time as the Tracking Protection Working Group has failed to come to consensus on a number of key issues. For well over a year now, the group has effectively stalled on how to address:

- *Cookies*: Privacy advocates have argued that parties honoring Do Not Track should be prohibited from using cookies or other unique identifiers, which would allow those companies to more easily recognize users across websites. In response, industry has argued that cookies should be available for limited pur-

vacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, March 2012, <http://www.ftc.gov/opa/2012/03/privacyframework.shtm>.

¹⁷ Josh Lowensohn, CNET, "Internet Explorer 9 to get tracking protection," December 7, 2010, http://news.cnet.com/8301-10805_3-20024864-75.html.

¹⁸ Crowd Science, "A Brief History of Do Not Track (DNT)," August 2012, <http://www.crowdscience.com/2012/08/a-brief-history-of-do-not-track-dnt/#!prettyPhoto>.

¹⁹ Digital Advertising Alliance, *DAA Position on Browser Based Choice Mechanism*, http://www.aboutads.info/resource/download/DAA_Commitment.pdf.

²⁰ *Id.*

²¹ Do Not Track, <http://donottrack.us/implementations>; Yahoo! Policy Blog, Shane Wiley, *Yahoo! Launches Global Support for Do Not Track*, March 29, 2012, <http://www.ypolicyblog.com/policyblog/2012/03/29/yahoo-launches-global-support-for-do-not-track/>. However, the ways in which these companies honor Do Not Track is not standardized and varies considerably. Moreover, not all Do Not Track headers are acknowledged: industry trade associations have excused members from adhering to Do Not Track instructions from Microsoft Internet Explorer 10 due to disagreement over whether those implementations reflect user choice. Katy Bachman, "Take That, Microsoft: Digital Ad Community's Final Word on Default Do Not Track," *Ad Week*, October 9, 2012, <http://www.adweek.com/news/technology/take-microsoft-digital-ad-communitys-final-word-default-do-not-track-144322>.

²² W3C, Standards, <http://www.w3.org/standards>.

²³ W3C, Tracking Protection Working Group, <http://www.w3.org/2011/tracking-protection/>.

poses (such as fraud prevention or ad frequency capping). This has been a point of contention within the group from the beginning, and indeed back to the original call for Do Not Track in 2007.²⁴

- *Market research and product improvement:* Apart from the question of *what* data can be collected despite a Do Not Track signal is the question of *why* data may be collected and retained despite a Do Not Track signal. All parties within the working group are generally in agreement that some data may be collected for basic operational purposes, such as ad delivery, security, frequency capping, and accounting. However, some working group participants have sought to allow the collection and use of data for broader purposes such as market research and product improvement. These purposes are certainly legitimate and societally worthwhile, but not necessarily essential to any particular website's functioning, and purposes for which a Do Not Track user might not necessarily expect her browsing history to be monitored and retained by third parties with which she has no relationship. Though the working group is agreed that research data could not be used to alter any individual's experience and will ultimately be used in the aggregate, it would be collected and retained on an individualized basis for a potentially extensive period of time (up to 53 weeks per one recent proposal, and longer in others). At one point, the working group had decided to exclude these purposes as a permitted use under the standard, but the idea has recently been reintroduced.²⁵
- *Deidentification:* All parties are in agreement that if data has been "deidentified," then it falls outside the scope of Do Not Track. That is, if a set of data has been stripped of identifiers and cannot be attributed to a person or device, Do Not Track should not apply to the data, and the company may use it as it pleases. However, there is debate over how robust deidentification must be. Advocates have argued for a test that largely mirrors the FTC's own test for deidentification: (1) you must have a reasonable belief that data could not be tied back to an individual or device, (2) you must promise not to try to reidentify the data, and (3) anyone you transfer the data to must also promise not to reidentify it. Some working group members have pushed back against this model, arguing that companies should be allowed to retain the technical ability to reidentify data so long as there are institutional controls in place to prevent reidentification. Under that approach, companies could continue to collect behavioral data for research and modeling purposes so long as the company had procedures in place to prohibit anyone within the company from singling out a particular user or device.²⁶
- *Browser presentation of Do Not Track options and consequences for non-compliant browsers:* The working group is generally agreed that a Do Not Track signal should represent the will of the user—browsers shouldn't send a Do Not Track signal without the user's understanding and consent. However, there is an open question over who should be able to evaluate the validity of a browser's presentation of Do Not Track choices to users. Some working group participants have argued that third parties should be able to reject Do Not Track signals from browsers that they believe do not adequately obtain consent to turn on Do Not Track from users. Other working group members have argued that third parties claiming compliance with Do Not Track should be required to honor syntactically correct signals and not second-guess a user's state of mind.²⁷
- *Data retention:* While all parties recognize the need for some level of data collection and retention by third parties when Do Not Track is turned on, there is disagreement on how long companies should be permitted to retain such data. Some working group members have argued that financial and auditing require-

²⁴ W3C Tracking Protection Working Group, Tracking Compliance and Scope, No Persistent Identifiers, <http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#no-persistent-identifiers>; CDT, "Consumer Rights and Protections in the Behavioral Advertising Sector," October 31, 2007, <https://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf>.

²⁵ W3C, Tracking Protection Working Group, Tracking Compliance and Scope, Audience Measurement, <http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#audience-measurement>.

²⁶ W3C, Tracking Protection Working Group, Tracking Compliance and Scope, Unlinkability, <http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#def-unlinkable>.

²⁷ W3C, Tracking Protection Working Group, Tracking Compliance and Scope, User Agent Compliance, <http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#user-agent-compliance>; W3C, Tracking Compliance Working Group, Tracking Compliance and Scope, Noncompliant User Agents, <http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#noncompliant-UA>.

ments dictate that data should (or must) be retained in individualized form for up to seven years. Other working group members have stated that such extensive retention is neither legally or logistically necessary, and that prolonged and individualized retention of cross-site data would run counter to a user's reasonable expectations in turning on Do Not Track.²⁸

Obviously, many of these issues are inter-dependent. Data retention matters more if companies can use unique cookies to log cross-site behavior. Companies may be more willing to adopt a robust deidentification standard if they are allowed to collect and retain data for market research and product improvement. For a bargain to be struck, these issues will all likely need to be decided as part of a comprehensive package.

However, to date, most industry working group participants have not been publicly willing to agree to move much beyond the current DAA principles for users who opt out of behavioral advertising, which regulators and advocates have criticized as insufficiently robust.²⁹ In some ways, industry proposals are even weaker than the rules currently in effect. For example, the DAA code arguably has a stronger definition of deidentification than has been proposed as an alternative within the Tracking Protection Working Group. Indeed, the DAA recently appears to have backtracked on the very notion that Do Not Track should even turn off behavioral advertising—the very purpose for which Do Not Track was originally proposed.³⁰

The Future of Do Not Track and Behavioral Advertising

Industry's failure to honor Do Not Track signals more than two years after they were first incorporated within Mozilla's Firefox browser is frustrating and perplexing. Despite disagreements over the precise contours of Do Not Track, self-regulatory groups could at least require members to treat Do Not Track as an opt-out under the DAA code, as Yahoo! and some other companies do today.³¹ Nor has there been any particular urgency within W3C (or elsewhere) to define a different standard for the treatment of Do Not Track users. Although trade association representatives have increasingly made chicken-little pronouncements on the effect that Do Not Track will have for the web,³² it is important to remember that they have long supported industry-wide opt-out rights for consumers online. Do Not Track is merely an improvement on industry opt-outs that have not proven sufficiently robust to address user concerns.

Moreover, it is important to note that Safari users have effectively had Do Not Track turned on *by default* for several years, ever since Apple made the decision to prevent third parties from setting cookies. Apple users can readily attest that apocalyptic predictions over the effects of Do Not Track have not come true for them, and that they enjoy the same wide variety of free Web content as users of other browsers, supported by (non-behaviorally targeted) advertisements.

Despite the lack of progress, CDT remains hopeful that ultimately the working group can agree on a strong Do Not Track standard that allows for some basic operational collection and retention of user data but limits behavioral retention and use to whatever is strictly necessary for the web to function. CDT originally proposed such a compromise approach in January 2011 just after the FTC formally called for the adoption of Do Not Track.³³ In April of 2012, we presented a similar compromise suggestion to the Tracking Protection Working Group at a face-to-face meeting in Washington, DC. Under our proposal, third parties would be allowed to use unique identifiers for narrow operational purposes, but not secondary purposes such as

²⁸ W3C, Tracking Protection Working Group, Tracking Compliance and Scope, Financial Logging and Auditing, <http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#financial-logging>.

²⁹ Federal Trade Commission Report: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, March 2012, <http://www.ftc.gov/opa/2012/03/privacyframework.shtm>.

³⁰ E-mail from Rachel Thomas to Tracking Protection Working, October 4, 2012, <http://lists.w3.org/Archives/Public/public-tracking/2012Oct/0115.html>.

³¹ Note however that Yahoo! does not honor Do Not Track requests from Internet Explorer 10, as the company alleges that the user flow for turning on Do Not Track does not sufficiently ensure that the signal represents a user's informed choice. Yahoo! Policy Blog, Shane Wiley, "In Support of a Personalized Experience," October 22, 2012, <http://www.yppolicyblog.com/policyblog/2012/10/26/dnt/>.

³² Leslie Harris, "The Bizarre, Belated Assault on Do Not Track," *Huffington Post*, October 4, 2012, <http://www.huffingtonpost.com/leslie-harris/the-bizarre-belated-assault-on-do-not-track-1935668.html>.

³³ CDT, "CDT Releases Draft Definition of 'Do Not Track,'" January 31, 2011, <https://www.cdt.org/blogs/erica-newland/cdt-releases-draft-definition-do-not-track>. CDT subsequently released a slightly revised version of this definition in April 2012, CDT, "What Does 'Do Not Track' Mean? A Scoping Proposal from the Center for Democracy & Technology, April 27, 2011 https://www.cdt.org/files/pdfs/20110447_DNT_v2.pdf.

market research. We support the robust deidentification standard as articulated by the FTC, but could be willing to allow third parties to reject certain Do Not Track signals—so long as the rejection is immediately signaled to the browser. However, to date, these proposals and other efforts to break the logjam have not gained significant traction.

One important development since Chairman Leibowitz called for Do Not Track in 2010 has been a stronger commitment to user privacy on the part of the browser makers. For years, browser vendors seemed more intent of preserving the business models of behavioral advertising than in satisfying the demands of their users. However, with increased focus on privacy issues by the press and by regulators, browser makers have listened to the demands of their clients—that is, their users—and have increasingly taken steps to protect users' privacy. As noted previously, all the major browser makers have implemented means for users to turn on Do Not Track and send Do Not Track headers to all websites. In June of last year, Microsoft announced that it would include Do Not Track options during the install flow for Windows 8 and Internet Explorer 10—with the recommended setting set to Do Not Track being on.³⁴ In February, Mozilla announced that it would join Apple in preventing third parties from setting cookies in its browser.³⁵

That browser makers are increasingly competing on privacy and responding to user's sentiments on behavioral advertising³⁶ is a welcome and important development. For years, privacy advocates have worried that in an arms race between users and ad networks, users, who by and large lack the sophistication and technical skills of the ad networks, were destined to lose. However, with the browsers increasingly acting in accordance with the desires of their user base, that result is no longer a foregone conclusion. Do Not Track was originally offered as a reasonable middle ground to avert an arms race—where ad networks could collect basic operational information and still serve (non-targeted) advertisements.³⁷ If trade associations continue to stick their heads in the sand and ignore consumer sentiment about their practices (instead of establishing a value proposition to users about behavioral advertising's benefits), moves like Mozilla's and Apple's to frustrate cross-site tracking will become the norm, and an inability to set cookies may be the least of their concerns.

Ultimately, the tortured Do Not Track saga is a stark demonstration of why consumers fundamentally need comprehensive privacy law. Unlike many areas of privacy, behavioral advertising has been under considerable regulatory and press scrutiny for over fifteen years (and intense scrutiny for at least the last five), and still despite all that effort and attention, practices have not meaningfully corrected and aligned with consumer expectations. In order to ensure that adequate consumer protections are in place for behavioral advertising—as well as considerably less examined industries with as least as extensive privacy implications—consumers deserve a strong but flexible horizontal privacy law governing all collection, use, and retention of personal information based on the Fair Information Practice Principles.

Finally, the ever-increasing stores of commercial databases of personal information about each and every one of us provides a compelling reason to revisit law enforcement privacy rules as well. For this reason, CDT has convened the Digital Due Process coalition to advocate for the reform of the Electronic Communications Privacy Act, to ensure that these databases are only accessed by the government under the due process of law.³⁸ Absent meaningful protections on potential government abuse, consumers have all the more reason to distrust commercial data collection and retention practices.

Conclusion

CDT would like to thank Senator Rockefeller and the Committee again for holding this important hearing on an issue that Americans are increasingly concerned about. We believe that Congress has a critical role to play in ensuring the privacy

³⁴Ed Bott, "Microsoft sticks to default Do Not Track settings in IE 10," *ZDNet*, August 7, 2012, <http://www.zdnet.com/microsoft-sticks-to-default-do-not-track-settings-in-ie-10-7000002289/>.

³⁵Justin Brookman, CDT blog, "Mozilla Says Enough is Enough," February 26, 2013, <https://www.cdt.org/blogs/justin-brookman/2602mozilla-says-enough-enough>.

³⁶Joseph Turow *et al.*, "Americans Reject Tailored Advertising and Three Activities that Enable It," September 29, 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214; Wendy Davis, "Zogby Poll: Web Users Troubled by Behavioral Advertising," *MediaPost*, June 8, 2010, <http://www.mediapost.com/publications/article/129753/#axzz2REncGaSy>.

³⁷Leslie Harris, "The Bizarre, Belated Assault on Do Not Track," *Huffington Post*, October 4, 2012, http://www.huffingtonpost.com/leslie-harris/the-bizarre-belated-assau_b_1935668.html.

³⁸Digital Due Process, <http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163>.

of consumers, through rigorous oversight of industry practices, and through the long overdue enactment of reasonable privacy legislation. CDT looks forward to working with the Members of the Committee as they pursue this and other privacy issues further.

The CHAIRMAN. Thank you, sir.

And then, finally, Mr. Adam Thierer, who is Senior Research Fellow at George Mason University.

**STATEMENT OF ADAM THIERER, SENIOR RESEARCH FELLOW,
MERCATUS CENTER, GEORGE MASON UNIVERSITY**

Mr. THIERER. Thank you, Mr. Chairman and members of the Committee, for inviting me here today to comment on the important issues of online privacy policy and data collection.

My name is Adam Thierer, and I am a Senior Research Fellow at the Mercatus Center at George Mason University, where I study Internet policy issues in the Mercatus Center's Technology Policy Program.

My message here today, which is condensed from two recent Law Review articles on these issues, boils down to three key points. First, no matter how well intentioned, restrictions on data collection could negatively impact the competitiveness of America's digital economy, as well as consumer choice.

Second, it is unwise to place too much faith in any one single silver bullet solution to online privacy, including Do-Not-Track, because such schemes are often easily evaded or defeated or fail to live up to their billing.

Finally, with those two points in mind, we should look to alternative and had less costly approaches to protecting privacy that rely on education, empowerment, and targeted enforcement of existing laws. Serious and lasting long-term privacy protection requires a layered, multifaceted approach incorporating many solutions.

Let us begin by being more specific about those costs associated with restrictions on data collection because they are important. Online advertising and data collection are the fuel that powers our information economy. Privacy-related mandates that curtail the use of data to better target ads or services could have several deleterious effects.

First, data restrictions could raise direct cost to consumers if walled gardens and pay walls are erected in response. As Senator Heller has already pointed out, something has to pay for all the wonderful free sites and services we enjoy today, and that is advertising and data.

Second, data restrictions could indirectly cost consumers by diminishing the abundance of content and culture now supported by data collection and advertising. In other words, even if prices and pay walls don't go up, overall quality or quantity could suffer if data collection is restricted.

Third, as Senator McCaskill and Senator Thune have already pointed out, data restrictions could hurt the competitiveness of domestic markets. While regulation raises the cost of doing business for all players in our economy, those costs will ultimately fall hardest on the small competitors or new start-ups.

For example, today's app economy has given countless small innovators a chance to compete on even footing with the biggest players. Burdensome data collection restrictions could short-circuit the engine that drives that sort of entrepreneurial innovation among mom-and-pop companies.

Fourth, data restrictions could undermine America's global competitive advantage in this space. We should ask ourselves how it is that America's Internet sector came to be the envy of the world and why it is so hard to name any major Internet company from Europe. Our more flexible, light-touch regulatory regime leaves more breathing room for competition and innovation compared to Europe's top-down approach.

Generally speaking, when it comes to privacy protection, therefore, we should avoid placing excessive faith in schemes like Do-Not-Track because they ultimately could fail, just as previous techno fixes failed to keep pace with fast-moving developments in this space.

Even if Do-Not-Track takes root and some consumers do turn it on, many will be incentivized by ad networks and publishers to opt right back out into tracking to retain access to the sites and services they desire. In doing so, they may actually end up sharing even more information than they do today. Moreover, that may drive still greater consolidation since larger players will be in a position to grant Internet-wide permissions or exceptions while smaller providers cannot.

In light of these trade-offs, we should subject new data restrictions to strict benefit/cost analysis to ensure we are not imposing unnecessary burdens on our data-driven economy. We should simultaneously consider how we might better spend our time and resources developing a richer mosaic of privacy-enhancing tools and educational strategies.

Luckily, an extensive array of tools and strategies exist today to help privacy, and that is made clear by an article that appeared just this morning on Lifehacker.com entitled, "The Best Browser Extensions That Protect Your Privacy," which ended with the following line. "You have some solid options. The tools are at your fingertips. It has never been easier to take the reins for yourself and make the Web an opt-in experience instead of an opt-out one."

Meanwhile, Web browsers continue to provide—or experiment with different privacy defaults, and while the W3C continues to pursue a single Do-Not-Track standard, innovators in the marketplace have already made private Do-Not-Track tools a reality. It is worth noting that almost all of these tools are available free of charge to consumers. So no barrier to widespread adoption exists.

As is the case with online safety concerns, citizens have access to many tools and methods to let them protect their privacy as they see fit, and evidence suggests they are already doing so.

Finally, where serious harms are documented, the FTC already possesses broad enforcement authority to police unfair and deceptive practices and has recently been using it more aggressively. Moreover, State law and class action lawsuits exist as a backstop and are often used aggressively following data breaches or privacy violations.

In closing, if we want America’s digital economy to remain open, innovative, and vibrantly competitive, then this sort of flexible bottom-up approach to privacy protection is the constructive path forward.

If our fear is that consumers lack enough information to make informed choices about their privacy, then let us work harder to educate them while pushing for greater transparency about online data collection practices.

Finally, we should remember that not everyone shares the same privacy sensitivities and that citizens also care about other values, such as cost, convenience, and choice. Moreover, we must take into account the very strong likelihood that citizens will adjust their privacy expectations in response to ongoing technological developments, just as they have many times before.

I thank the Committee for inviting me here today, and I would be happy to take questions.

[The prepared statement of Mr. Thierer follows:]

PREPARED STATEMENT OF ADAM D. THIERER, SENIOR RESEARCH FELLOW,
MERCATUS CENTER, GEORGE MASON UNIVERSITY

Mr. Chairman and members of the Committee, thank you for inviting me here today to comment on the important issues of online privacy policy and commercial data collection. My name is Adam Thierer and I am a senior research fellow at the Mercatus Center at George Mason University, where I study Internet policy issues in the Mercatus Center’s Technology Policy Program.

My message here today, condensed from two recent law review articles,¹ boils down to three points:

1. First, no matter how well-intentioned, *restrictions on data collection could negatively impact the competitiveness of America’s digital economy, as well as consumer choice.*
2. Second, *it is unwise to place too much faith in any single, silver-bullet solution to privacy*, including “Do Not Track,” because such schemes are easily evaded or defeated and often fail to live up to their billing.
3. Finally, with those two points in mind, *we should look to alternative and less costly approaches to protecting privacy* that rely on education, empowerment, and targeted enforcement of existing laws. Serious and lasting long-term privacy protection requires a layered, multifaceted approach incorporating many solutions.

Trade-offs Associated with Restrictions on Data Collection

Let’s be more specific about the potential costs of restrictions on data collection. Online advertising and data collection are the fuel that powers our information economy. Privacy-related mandates that curtail the use of data to better target ads or services could have several deleterious effects.²

First, *data restrictions could raise **direct** costs for consumers* if walled gardens and paywalls are erected in response. Something has to pay for all the wonderful free sites and services we enjoy today.

Second, *data restrictions could **indirectly** cost consumers by diminishing the abundance of content and culture now supported by data collection and advertising.*

¹Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 HARV. J. L. & PUB. POL. 409 (2013), papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680; Adam Thierer, *A Framework for Benefit-Cost Analysis in Digital Privacy Debates*, 20 GEO. MASON UNIV. L. REV., (forthcoming, Summer 2013).

²See generally Adam Thierer & Berin Szoka, *The Hidden Benefactor: How Advertising Informs, Educates & Benefits Consumers*, Progress & Freedom Foundation, PROGRESS SNAPSHOT, Feb. 2010; Berin Szoka & Adam Thierer, *Online Advertising & User Privacy: Principles to Guide the Debate*, Progress & Freedom Foundation, PROGRESS SNAPSHOT, Sept. 2008.

In other words, even if prices and paywalls don't go up, overall quantity or quality could suffer if data collection is restricted.³

Third, *data restrictions could hurt the competitiveness of domestic markets*. While regulation raises the costs of doing business for all online operators, those costs will fall hardest on smaller operators and new start-ups.⁴ For example, today's "app economy" has given countless small innovators a chance to compete on even footing with the biggest players.⁵ Burdensome data collection restrictions could short-circuit the engine that drives entrepreneurial innovation among mom-and-pop companies if ad dollars get consolidated in the hands of only the larger companies that can afford to comply with new rules.⁶

Fourth, *data restrictions could undermine America's global competitive advantage in this space*. We should ask ourselves how it is that America's Internet sector came to be the envy of the world and why it is so hard to name any major Internet company from Europe.⁷ Our more flexible, light-touch regulatory regime leaves more room for competition and innovation compared to Europe's top-down regime.⁸

Unintended Consequences of Do Not Track

Generally speaking, when it comes to privacy protection, *we should avoid placing excessive faith in schemes like Do Not Track* because they could fail, just as previous techno-fixes failed to keep pace with fast-moving developments in this space.

[See Appendix I: "Techno-'Silver-Bullet' Solutions Don't Work—Some Case Studies."]

³A 2010 study by Howard Beales, the former Director of the Bureau of Consumer Protection at the FTC, found that "the price of behaviorally targeted advertising in 2009 was 2.68 times the price of run of network advertising." That increased return on investment is important, Beales notes, because it creates "greater utility for consumers from more relevant advertisements and clear appeal for advertisers from increased ad conversion." Beales also noted that, "a majority of network advertising revenue is spent acquiring inventory from publishers, making behavioral targeting an important source of revenue for online content and services providers as well as third party ad networks." Howard Beales, Network Advertising Initiative, *The Value of Behavioral Targeting*, at 1 (March 2010), www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

⁴"In a setting where first-party advertising is allowable but third-party marketing is not, substantial advantages may be created for large incumbent firms," argue Professors Avi Goldfarb and Catherine Tucker. "For example, if a large website or online service were able to use its data to market and target advertising, it will be able to continue to improve and hone its advertising, while new entrants will find it difficult to challenge the incumbent's predominance by compiling other data or collecting their own data." Avi Goldfarb & Catherine Tucker, *Comments on 'Information Privacy and Innovation in the Internet Economy'*, Comments to the U.S. Department of Commerce, Jan. 24, 2011, at 4, http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/NTIA_comments_2011_01_24.pdf.

⁵"The App Economy now is responsible for roughly 466,000 jobs in the United States, up from zero in 2007 when the iPhone was introduced." Michael Mandel, *Where the Jobs Are: The App Economy*, (TechNet, Feb. 7, 2012) <http://www.technet.org/wp-content/uploads/2012/02/TechNet-App-Economy-Jobs-Study.pdf>.

⁶Apple's Safari browser already blocks third-party cookies and now Mozilla's Firefox browser will as well. This has led to concerns about how market structure and competition will be impacted. See: Tim Peterson, *The Demise of Third-Party Cookies Could Help Premium Publishers*, ADWEEK, Apr. 15, 2013, <http://www.adweek.com/news/technology/demise-third-party-cookies-could-help-premium-publishers-148573>; "First Safari and now Firefox are blocking third-party companies from dropping cookies on publishers' sites to protect users' privacy. Those moves hurt revenues of the smaller publishers that depend on third parties to sell ads. But, paradoxically, the winners could be premium publishers and large media companies, especially Facebook and Google, who will be able to prop up their proprietary audience data as the ideal alternative. Big traditional publishers whose ad revenue has shrunk as readers and advertisers shift online could recoup their losses by parlaying their first-party audience data into even higher ad rates"; Adam Lehman, *Don't Fear the Cookie Backlash*, DIGIDAY, Apr. 17, 2013, <http://www.digiday.com/platforms/dont-fear-the-cookie-backlash>; "Several people have already pointed out that the Mozilla [third-party cookie restriction] change will create even greater advantages for the largest players in digital media."

⁷Goldfarb and Tucker have also found that "after the [European Union's] Privacy Directive was passed [in 2002], advertising effectiveness decreased on average by around 65 percent in Europe relative to the rest of the world." They argue that because regulation decreases ad effectiveness, "this may change the number and types of businesses sustained by the advertising-supporting Internet." The European Union's experience makes it clear that regulation of online advertising and data collection can affect market structure, competitive rivalry, and the global competitiveness of online firms. This could also have antitrust implications that the FTC or other agencies would need to take into account when considering new privacy rules. Goldfarb & Tucker, *Comments on 'Information Privacy'*, 4.

⁸Adam Thierer, *A Better, Simpler Narrative for U.S. Privacy Policy*, TECHNOLOGY LIBERATION FRONT, Mar. 19, 2013, <http://techliberation.com/2013/03/19/a-better-simpler-narrative-for-u-s-privacy-policy>.

Even if Do Not Track takes root and some consumers turn it on, many will be incentivized by ad networks or publishers to opt right back in to “tracking” to retain access to sites and services they desire.⁹ In doing so, they may end up sharing even more information than they do today.¹⁰ Moreover, this may drive still greater consolidation since larger players will be in a position to grant Internet-wide opt-in exceptions, while smaller providers cannot.¹¹

Constructive Alternatives to Regulation

In light of these trade-offs, *we should subject new data restrictions to strict benefit-cost analysis* to ensure that we are not imposing unnecessary burdens on our data-driven economy.¹²

We should simultaneously consider how *we might better spend our time and resources developing a richer mosaic of privacy-enhancing tools and educational strategies*. Luckily, an extensive array of such tools and strategies already exists.¹³

[See Appendix II: “Digital Self-Help Tools.”]

Web browser providers continue to experiment with different privacy defaults,¹⁴ and while the World Wide Web Consortium (W3C) continues to pursue a single Do Not Track standard, innovators in the marketplace have already made private Do Not Track tools a reality.¹⁵

It is worth noting that *almost all of these tools are available free of charge*, and no barrier to widespread adoption exists.¹⁶ As is the case with online safety concerns,¹⁷ *citizens have access to many tools and methods that let them protect their privacy as they see fit*, and evidence suggests they already actively do so.¹⁸

Alternative Enforcement Approaches

Finally, where serious privacy harms are documented, *the Federal Trade Commission already possesses broad enforcement authority* to police unfair and deceptive

⁹Berin Szoka, *The Paradox of Privacy Empowerment: The Unintended Consequences of “Do Not Track,”* Position paper for W3C Workshop: Do Not Track and Beyond Berkeley, California, (Nov. 26–27, 2012), <http://www.w3.org/2012/dnt-ws/position-papers/5.pdf>.

¹⁰See Nicklas Lundblad & Betsy Masiello, *Opt-in Dystopias*, 7:1 SCRIPTed 155, (2010), <http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp>, noting that as a result of a push for stronger-opt-in regimes, “service providers may attempt to maximise data collection in every instance that they are forced to use an opt-in framework; once a user consents to data collection, why not collect as much as possible? And the increased transaction costs associated with opt-in will lead service providers to minimise the number of times they request opt-in consent. In combination these two behaviours are likely to lead to an excessive scope for opt-in agreements. In turn, users will face more complex decisions as they decide whether or not to participate.”

¹¹Szoka, *The Paradox of Privacy Empowerment*, 3.

¹²I have explained how to conduct such an analysis in my forthcoming article, Adam Thierer, *A Framework for Benefit-Cost Analysis in Digital Privacy Debates*, 20 GEO. MASON UNIV. L. REV., (forthcoming, Summer 2013).

¹³They include: ad preference managers, “private browsing” tools, ad-blocking technologies, cookie-blockers, web script blockers, encryption and web proxy tools, and reputation protection services.

¹⁴Megan Geuss, *Firefox 22 Will Block Third-Party Cookies*, Ars Technica, Feb. 23, 2013, <http://arstechnica.com/business/2013/02/firefox-22-will-block-third-party-cookies>; Alexis Santos, *Microsoft Sets ‘Do Not Track’ as Default on IE10, Ruffles Feathers*, ENGADGET, June 1, 2012, <http://www.engadget.com/2012/06/01/do-not-track-is-default-on-ie10>.

¹⁵Online privacy company Abine offers a “Do Not Track Plus,” which it claims blocks more than 600 trackers. See <http://www.abine.com/dntdetail.php>.

¹⁶The only serious objection to this bottom-up, user empowerment-based approach is that it could inconvenience users by making it more difficult to use some sites or slow down their browsing experience in some fashion. But it is no more an inconvenience than it is to use parental control tools so that your kids won’t see or download objectionable content.

¹⁷Adam Thierer, Progress & Freedom Foundation, *Parental Controls & Online Child Protection: A Survey of Tools*, Version 4.0, Summer 2009, <http://www.pff.org/parentalcontrols>.

¹⁸The Pew Research Center’s Internet & American Life Project has note that 88 percent of U.S. adults now own cell phones, and 43 percent say they download cell phone applications or “apps” to their phones. When surveyed, 54 percent of those app users said they had decided to not install a cell phone app when they discovered how much personal information they would need to share in order to use it and 30 percent of them had uninstalled an app that was already on their cell phone because they learned it was collecting personal information that they didn’t wish to share. “Taken together,” Pew notes, “57 percent of all app users have either uninstalled an app over concerns about having to share their personal information, or declined to install an app in the first place for similar reasons.” Jan Lauren Boyles, Aaron Smith, and Mary Madden, *Privacy and Data Management on Mobile Devices*, (Pew Research Center’s Internet & American Life Project, Sept. 5, 2012), <http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx>.

practices and has recently been using it more aggressively.¹⁹ Targeted Federal statutes already exist to address sensitive issues related to health,²⁰ financial,²¹ and children's privacy.²² Enforcement alternatives are also available through state courts, including torts,²³ contract law,²⁴ and state statutes.²⁵ Class action lawsuit activity is also remarkably intense following any major privacy violation or data breach.²⁶

Conclusion

In closing, if we want America's digital economy to remain open, innovative, and vibrantly competitive, then this flexible, bottom-up approach to privacy protection is the constructive path forward.

If our fear is that consumers lack enough information to make smart privacy choices, then let's work harder to educate them while pushing for greater transparency about online data collection practices.

Finally, we should remember that not everyone shares the same privacy sensitivities and that citizens also care about other values, such as cost, convenience, and choice.

Moreover, we must also take into account the strong likelihood that citizens will adjust their privacy expectations in response to ongoing technological change, just as they have many times before.²⁷

[See Appendix III: "Societal Adaptation, Evolving Cultural Norms & Privacy."]

I thank you again for inviting me here today and I would be happy to take any questions.

¹⁹In its March 2012 *Protecting Consumer Privacy in an Era of Rapid Change* report, the FTC noted that, using its Section 5 authority and other powers, the agency has carried out many privacy and data security-related actions just since December 2010. See Fed. Trade Comm'n, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012) at ii, <http://ftc.gov/os/2012/03/120326privacyreport.pdf>. The FTC brought several other privacy and data security-related cases using its Section 5 powers after the 2012 report was released. See: *FTC Finalizes Privacy Settlement with Myspace*, Fed. Trade Comm'n, (Sept. 11, 2012), <http://www.ftc.gov/opa/2012/09/myspace.shtm>; *FTC Halts Computer Spying*, Fed. Trade Comm'n, (Sept. 25, 2012), <http://www.ftc.gov/opa/2012/09/designware.shtm>; *Tracking Software Company Settles FTC Charges That it Deceived Consumers and Failed to Safeguard Sensitive Data it Collected*, Fed. Trade Comm'n, (Oct. 22, 2012), <http://www.ftc.gov/opa/2012/10/compete.shtm>.

²⁰See Health Breach Notification Rule (2009), 16 C.F.R. § 318.1 (2012).

²¹See Truth in Lending Act, 15 U.S.C. §§ 1601–1667(f) (2006); Fair Credit Billing Act, 15 U.S.C. §§ 1666–1666(j) (2006); Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681–1681(u) (2006).

²²See Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. § 6501 (2006).

²³See Jim Harper, *The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection* (2002), http://www.privacilla.org/releases/Torts_Report.html.

²⁴See Jim Harper, *Understanding Privacy—and the Real Threats to It*, Cato Policy Analysis, Aug. 4 2004, at 3, www.cato.org/pub_display.php?pub_id=1652: "Contract law, for example, allows consumers to enter into enforceable agreements that restrict the sharing of information involved in or derived from transactions. Thanks to contract, one person may buy foot powder from another and elicit as part of the deal an enforceable promise never to tell another soul about the purchase."

²⁵State governments and state attorneys general also continue to advance their own privacy policies, and those enforcement efforts are often more stringent than Federal law. Christopher Wolf, *Targeted Enforcement and Shared Lawmaking Authority as Catalysts for Data Protection*, at 3 (2010), http://www.justice.gov.il/NR/rdonlyres/8D438C53-82C8-4F25-99F8-E3039D40E4E4/26451/Consumer_WOLFDataProtectionandPrivacyCommissioners.pdf: "At the state level, legislatures have become the proving grounds for new statutory approaches to privacy regulation. Some of these developments include the enactment of data security breach notification laws . . . as well as highly detailed data security laws, enacted largely in response to data breaches. This partnership has resulted in a set of robust standards for the protection of personal data."

²⁶Peter Fleischer, *Privacy-litigation: get ready for an avalanche in Europe*, PETER FLEISCHER: PRIVACY? (Oct. 26, 2012), <http://peterfleischer.blogspot.com/2012/10/privacy-litigation-get-ready-for.html?m=1>: "Within hours of any newspaper headline (accurate or not) alleging any sort of privacy mistake, a race begins among privacy class action lawyers to find a plaintiff and file a class action. Most of these class actions are soon dismissed, or settled as nuisance suits, because most of them fail to be able to demonstrate any 'harm' from the alleged privacy breach. But a small percentage of privacy class actions do result in large transfers of money, first and foremost to the class action lawyers themselves, which is enough to keep the wheels of the litigation-machine turning."

²⁷See Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J. L. SCI. & TECH. 309, 364–73, (2013).

Appendix I: Techno-“Silver-Bullet” Solutions Don’t Work—Some Case Studies

Seeking a simple solution to a complex problem such as online privacy protection is quixotic. In this sense, the Do Not Track falls into a long line of proposed silver-bullet or “universal” solutions to complicated technological problems. When it comes to such information control efforts, there are not many good examples of simple fixes or silver-bullet solutions that have been effective, at least not for very long.

- *Online Pornography*: Consider the elusive search for a universal solution to controlling access to online pornography. The experience of the W3C’s Platform for Internet Content Selection (PICS)²⁸ and the Internet Content Rating Association (ICRA)²⁹ is instructive in this regard. Around the turn of the century, there was hope that voluntary metadata tagging and content labeling could be used to screen objectionable content on the Internet,³⁰ but the sheer volume of material to be dealt with made that task almost impossible.³¹ The effort was eventually abandoned.³² Of course, the effort did not have a government mandate behind it to encourage more widespread adoption, but even if it had, it is hard to believe that all pornography or other objectionable content would have properly been labeled and screened.
- *Spam*: In a similar way, the CAN-SPAM Act³³ aimed to curtail the flow of unsolicited e-mail across digital systems, yet failed to do so. Private filtering efforts have helped stem the flow to some extent, but have not eliminated the problem altogether. Royal Pingdom estimates that in 2010, 89.1 percent of all e-mails were spam.³⁴ “Spam pages” are also a growing concern.³⁵ In January 2011, Blekko, a new search engine provider, created a “Spam Clock” to track new spam pages and found one million new spam pages were being created every hour.³⁶
- *Privacy*: Technical silver-bullet solutions have also been tried on the privacy front before Do Not Track. The Platform for Privacy Preferences (P3P) is an earlier W3C project that began in the 1990s and attempted to make the use of privacy policies easier for consumers to understand. It sought to do so by encoding those privacy policies in a standard machine-readable format. The hope was that this would allow sites “to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily” by users and then allow users “to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit.”³⁷ In theory, “such a privacy disclosure format could also allow the FTC to automate enforcement of its existing authority to punish unfair or deceptive trade practices.”³⁸ Unfortunately, the P3P project has not been successful. Even though the process got underway in the mid-1990s and the W3C had a formal process in place to guide its development by 1997, the project was suspended

²⁸ PICS Frequently Asked Questions (FAQ), WORLD WIDE WEB CONSORTIUM, <http://www.w3.org/2000/03/PICS-FAQ>, (last visited Jan. 30, 2013).

²⁹ About ICRA, FAMILY ONLINE SAFETY INST., <http://www.fosi.org/icra>, (last visited Jan. 30, 2013).

³⁰ See, e.g., Joris Evers, *Net labels mean choice, not censorship*, PC ADVISOR, Oct. 23, 2001, <http://www.pcadvisor.co.uk/news/desktop-pc/1646/net-labels-mean-choice-not-censorship/>.

³¹ See PHIL ARCHER, ICRAFAIL: A LESSON FOR THE FUTURE 9 (2009), philarcher.org/icra/ICRAfail.pdf; “The problem with a safety system that has a label at one end and a filter at the other is that unlabelled sites can only be treated as a single group, i.e., you either block them all or allow them all. Since the number of labelled sites was very small, blocking all unlabelled sites would effectively shut off most of the Web.”

³² FAMILY ONLINE SAFETY INST., <http://www.icra.org>, (last visited Nov. 30, 2012).

³³ Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified at various sections of 15 and 18 U.S.C.).

³⁴ *Internet 2010 in Numbers*, ROYAL PINGDOM, Jan. 12, 2011, <http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers>.

³⁵ Spam pages are “useless pages that contain only a nugget of relevancy to your query and are slathered in ads.” Caleb Johnson, *Spam Clock Claims 1 Million Spam Pages are Created Every Hour*, Jan. 10, 2011, SWITCHED.COM, <http://switched.com/2011/01/10/blekko-spam-clock-1-million-pages-an-hour>.

³⁶ SPAMCLOCK, [HTTP://WWW.SPAMCLOCK.COM](http://www.spamclock.com), (last visited Jan. 30, 2013); see also Danny Sullivan, *Blekko Launches Spam Clock To Keep Pressure On Google*, SEARCH ENGINE LAND.COM, Jan. 7, 2011, <http://searchengineland.com/blekko-launches-spam-clock-to-keep-pressure-on-google-60634>.

³⁷ W3C, Platform for Privacy Preferences (P3P) Project, <http://www.w3.org/P3P> (last accessed Apr. 21, 2013).

³⁸ Adam Thierer & Berin Szoka, The Progress & Freedom Foundation, *Chairman Leibowitz’s Disconnect on Privacy Regulation & the Future of News* at 7, (Jan. 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1619470.

in 2007.³⁹ A 2009 survey of privacy technologies by analysts at the UC Berkeley School of Information found that “to date, the adoption rate of P3P has been fairly low. Our analysis of the top 100 websites for this project revealed that only 27 of them provided a P3P policy, and only a subset of those were valid according to the P3P standard.”⁴⁰

Similar problems likely await the Do Not Track mechanism.⁴¹ Also, Do Not Track “does not address mobile or app data, nor any data created outside a traditional web browser,” notes Michael Fertik, CEO of Reputation.com.⁴² “At the same time, the growth in technology and understanding can render current solutions inadequate. A privacy rule to limit behavioral advertising today might not work in the future when more data is available and there are more powerful algorithms to process it,” he says.⁴³ “There is no reliable way of ensuring this technology is being used,” adds Sidney Hill of *Tech News World*.⁴⁴ “Ensuring compliance with antitracking rules will become even more difficult as more users turn to mobile devices as their primary means of connecting to the Web.”⁴⁵

Importantly, Do Not Track would not slow the “arms race” in this arena as some have suggested.⁴⁶ If anything, a Do Not Track mandate will speed up that arms race and have many other unintended consequences.⁴⁷ Complex definitional questions also remain unanswered, such as how to define and then limit “tracking” in various contexts.⁴⁸

In sum, in light of the global, borderless nature of online rapid data flows, the Do Not Track scheme likely will not be effective.⁴⁹ The regulatory experience with spam, objectionable content, and copyrighted content suggests serious challenges lie ahead for top-down regulatory efforts.

Appendix II: Digital Self-Help Tools/Privacy-Enhancing Technologies

The market for digital “self-help” tools and privacy enhancing technologies (PET) continues to expand rapidly to meet new challenges. These tools can help users block or limit various types of advertising and data collection and also ensure a

³⁹ Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. ON TELECOMM. & HIGH TECH. L. 273, 279–82 (2012).

⁴⁰ Joshua Gomez, Travis Pinnick & Ashkan Soltani, UC Berkeley, School of Information, *Know Privacy*, at 12 (June 1, 2009).

⁴¹ Steve DelBianco & Braden Cox, *NetChoice Reply Comments on Department of Commerce Green Paper* (Jan. 28, 2011), available at <http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=1EA98542-23A4-4822-BECD-143CD23BB5E9>, (“It’s a single response to an overly-simplified set of choices we encounter on the web.”).

⁴² Michael Fertik, *Comments of Reputation.com, Inc. to the U.S. Department of Commerce* (Jan. 28, 2011), available at <http://www.reputation.com/blog/2011/01/31/reputation-com-comments-commerce-department-privacy-green-paper>.

⁴³ *Id.*

⁴⁴ Sidney Hill, *Internet Tracking May Not Be Worth the Headaches*, TECH NEWS WORLD, Dec. 29, 2010, <http://www.technewsworld.com/story/Internet-Tracking-May-Not-Be-Worth-the-Headaches-71543.html>.

⁴⁵ *Id.*

⁴⁶ See Rainey Reitman, *Mozilla Leads the Way on Do Not Track*, ELEC. FRONTIER FUND, Jan. 24, 2011, <https://www.eff.org/deeplinks/2011/01/mozilla-leads-the-way-on-do-not-track>; “the header-based Do Not Track system appeals because it calls for an armistice in the arms race of online tracking”; Christopher Soghoian, *What the U.S. government can do to encourage Do Not Track*, SLIGHT PARANOIA, Jan. 27, 2011, <http://paranoia.dubfire.net/2011/01/what-us-government-can-do-to-encourage.html>; “opt out mechanisms . . . [could] finally free us from this cycle of arms races, in which advertising networks innovate around the latest browser privacy control.”

⁴⁷ “Too often, well-intentioned efforts to regulate technology are far worse than the imagined evils they were intended to prevent.” HAL ABELSON *et al.*, *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion* 159 (2008).

⁴⁸ Lauren Weinstein, *Risks in Mozilla’s Proposed Firefox “Do Not Track” Header Thingy*, LAUREN WEINSTEIN’S BLOG (Jan. 24, 2010, 12:09 AM), <http://lauren.vortex.com/archive/000803.html>.

⁴⁹ “Many behavioral targeting companies are based outside the U.S.—making legislation ineffective,” says Doug Wolfram, CEO of IntelliProtect, an online privacy management company. Tony Bradley, *Why Browser ‘Do Not Track’ Features Will Not Work*, COMPUTERWORLD, Feb. 10, 2011, <http://news.idg.no/cw/art.cfm?id=ACE91A0E-1A64-6A71-CE2572C981C0204A>; DANIEL CASTRO, POLICYMAKERS SHOULD OPT OUT OF “DO NOT TRACK” 1, 3 (2010), www.itif.org/files/2010-do-not-track.pdf; “Another problem with Do Not Track is that it does not scale well on the global Internet. . . . To be effective, the proposal would require a Federal mandate calling for substantive modifications to networking protocols, web browsers, software applications and other Internet devices. Besides raising costs for consumers, it is unclear how effective such a mandate would be outside of the U.S. borders or how well the proposal would be received by international standard bodies.”

more anonymous browsing experience. What follows is a brief inventory of the PETs and consumer information already available on the market today:

- The major online search and advertising providers offer “ad preference managers” to help users manage their advertising preferences. Google,⁵⁰ Microsoft,⁵¹ and Yahoo!⁵² all offer easy-to-use opt-out tools and educational webpages that clearly explain to consumers how digital advertising works.⁵³ Meanwhile, a relatively new search engine, DuckDuckGo, offers an alternative search experience that blocks data collection altogether.⁵⁴
- Major browser providers also offer variations of a “private browsing” mode, which allows users to turn on a stealth browsing mode to avoid data collection and other forms of tracking. This functionality is available as a menu option in Microsoft’s Internet Explorer (“InPrivate Browsing”),⁵⁵ Google’s Chrome (“Incognito”)⁵⁶ and Mozilla’s Firefox (“Private Browsing”).⁵⁷ Firefox also has many add-ons available that provide additional privacy-enhancing functionality.⁵⁸ “With just a little effort,” notes Dennis O’Reilly of *CNET News.com*, “you can set Mozilla Firefox, Microsoft Internet Explorer, and Google Chrome to clear out and block the cookies most online ad networks and other Web trackers rely on to build their valuable user profiles.”⁵⁹
- There are also many supplemental tools and add-ons that users can take advantage of to better protect their privacy online by managing cookies, blocking web scripts, and so on. Like the marketplace for parental control technologies, a remarkable amount of innovation continues in the market for privacy empowerment tools, so much so that it is impossible to document all of them here. However, some of the more notable privacy-enhancing tools and services include: Ghostery,⁶⁰ NoScript,⁶¹ Cookie Monster,⁶² Better Privacy,⁶³ Track Me Not,⁶⁴ Collusion,⁶⁵ and the Targeted Advertising Cookie Opt-Out or “TACO”⁶⁶ (all for

⁵⁰*Ads Preferences*, GOOGLE, <http://www.google.com/ads/preferences> (last visited Jan. 30, 2013).

⁵¹*Ad Choices*, MICROSOFT, <http://choice.live.com/Default.aspx> and (last visited Jan. 30, 2013); *Personalized Advertising*, MICROSOFT, <https://choice.live.com/AdvertisementChoice/Default.aspx> (last visited Jan. 30, 2013).

⁵²*Ad Interest Manager*, YAHOO!, http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html (last visited Jan. 30, 2013).

⁵³*Privacy*, MICROSOFT, <http://www.microsoft.com/privacy/default.aspx>; (last visited Jan. 30, 2013); *Yahoo! Privacy Center*, YAHOO!, <http://info.yahoo.com/privacy/us/yahoo/> (last visited Jan. 30, 2013); *Privacy Policy*, GOOGLE, <http://www.google.com/privacy/ads> (last visited Jan. 30, 2013).

⁵⁴*Privacy*, DUCKDUCKGO, <http://duckduckgo.com/privacy.html> (last visited Jan. 30, 2013); see also, Jennifer Valentino-DeVries, *Can Search Engines Compete on Privacy?*, WALL ST. J. DIGITS BLOG (Jan. 25, 2011, 4:02 PM), <http://blogs.wsj.com/digits/2011/01/25/can-search-engines-compete-on-privacy>.

⁵⁵*InPrivate Browsing*, MICROSOFT, <http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/features/in-private> (last visited Jan. 30, 2013).

⁵⁶*Incognito mode (browse in private)*, GOOGLE, <http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95464> (last visited Jan. 30, 2013).

⁵⁷*Private Browsing—Browse the web without saving information about the sites you visit*, MOZILLA, <http://support.mozilla.com/en-US/kb/Private%20Browsing> (last visited Jan. 30, 2013).

⁵⁸*Add-Ons*, MOZILLA, <https://addons.mozilla.org/en-US/firefox/tag/incognito> (last visited Jan. 30, 2013).

⁵⁹Dennis O’Reilly, *Add ‘do not track’ to Firefox, IE, Google Chrome*, CNETNEWS.COM, Dec. 7, 2010, http://news.cnet.com/8301-13880_3-20024815-68.html.

⁶⁰*Ghostery Add-On*, MOZILLA, <https://addons.mozilla.org/en-US/firefox/addon/ghostery> (last visited Jan. 30, 2013).

⁶¹*No Script Add-On*, MOZILLA, <https://addons.mozilla.org/en-US/firefox/addon/noscript> (last visited Jan. 30, 2013).

⁶²*Cookie Monster Add-On*, MOZILLA, <https://addons.mozilla.org/en-US/firefox/addon/cookie-monster> (last visited Jan. 30, 2013).

⁶³*BetterPrivacy Add-On*, MOZILLA, <https://addons.mozilla.org/en-US/firefox/addon/better-privacy> (last visited Jan. 30, 2013).

⁶⁴*TrackMeNot Add-On*, MOZILLA, <https://addons.mozilla.org/en-US/firefox/addon/trackme-not> (last visited Jan. 30, 2013).

⁶⁵*Collusion Add-On*, MOZILLA, <http://www.mozilla.org/en-US/collusion> (last visited Jan. 30, 2013).

⁶⁶*Targeted Advertising Cookie Opt-Out (TACO) Add-On*, MOZILLA, <https://addons.mozilla.org/en-US/firefox/addon/targeted-advertising-cookie-op/> (last visited Jan. 30, 2013).

Firefox); No More Cookies⁶⁷ (for Internet Explorer); Disconnect (for Chrome);⁶⁸ AdSweep (for Chrome and Opera);⁶⁹ CCleaner⁷⁰ (for PCs); and Flush⁷¹ (for Mac). New empowerment solutions are constantly turning up.⁷² Many of these tools build around the Do Not Track notion and functionality that the FTC has been encouraging. For example, Reputation.com's new "MyPrivacy" service lets users remove their information from various sites and helps them create the equivalent of a Do Not Track list for over 100 online networks.⁷³ New tools from Priveazy⁷⁴ and Privacyfix⁷⁵ offer similar functionality and allow users to adjust privacy settings for several sites and services at once. Finally, online privacy company Abine offers a "Do Not Track Plus," which it claims blocks more than 600 trackers.⁷⁶ Abine also sells a "PrivacyWatch" service, which alerts Facebook users to privacy policy changes on the site,⁷⁷ as well as a "DeleteMe" service that helps users erase personal information from various other online sites and services.⁷⁸

- The success of one particular tool, AdblockPlus, deserves special mention. AdblockPlus, which lets users block advertising on most websites, is the most-downloaded add-on for both the Firefox and Chrome web browsers.⁷⁹ As of October 2012, roughly 175 million people had downloaded the Adblock Plus add-on for the Firefox web browser.⁸⁰ Incidentally, both Adblock Plus and NoScript, another of the most popular privacy-enhancing downloads for Firefox, support the Do Not Track protocol.⁸¹
- Finally, pressured by policymakers and privacy advocates, all three of those browser makers (Microsoft,⁸² Google,⁸³ and Mozilla⁸⁴) have now agreed to include some variant of a Do Not Track mechanism or an opt-out registry in their browsers to complement the cookie controls they had already offered. Microsoft has even decided to turn on Do Not Track by default, although it has been a controversial move.⁸⁵ These developments build on industry-wide efforts by the Network Advertising Initiative and the "Self-Regulatory Program for Online Be-

⁶⁷ No More Cookies, CNET.COM, http://download.cnet.com/No-More-Cookies/3000-2144_4-10449885.html (last visited Jan. 30, 2013).

⁶⁸ DISCONNECT, <https://disconnect.me> (last visited Jan. 30, 2013).

⁶⁹ AdSweep Add-On, OPERA, <https://addons.opera.com/addons/extensions/details/adsweep/2.0.3-3/?display=en> (last visited Jan. 30, 2013).

⁷⁰ CCleaner, PIRIFORM, <http://www.piriform.com/ccleaner> (last visited Jan. 30, 2013).

⁷¹ Flush, MACUPDATE, <http://www.macupdate.com/app/mac/32994/flush> (last visited Jan. 30, 2013).

⁷² David Gorodiansky, *Web Privacy: Consumers Have More Control Than They Think*, HUFFINGTON POST, Dec. 30, 2010, http://www.huffingtonpost.com/david-gorodiansky/web-privacy-consumers-have-b_799881.html.

⁷³ My Privacy, REPUTATION.COM, <http://www.reputation.com/myprivacy> (last visited Jan. 30, 2013).

⁷⁴ PRIVEAZY, <https://www.priveazy.com> (last visited Jan. 30, 2013).

⁷⁵ PRIVACYFIX, <https://privacyfix.com> (last visited Jan. 30, 2013).

⁷⁶ Do Not Track Plus, ABINE, <http://www.abine.com/dntdetail.php> (last visited Jan. 30, 2013).

⁷⁷ PrivacyWatch, ABINE, <http://www.abine.com/privacywatchdetail.php> (last visited Jan. 30, 2013).

⁷⁸ DeleteMe, ABINE, <http://www.abine.com/marketing/landing/index.php> (last visited Jan. 30, 2013).

⁷⁹ AdblockPlus, <https://adblockplus.org/en> (last visited Jan. 30, 2013).

⁸⁰ Statistics for Adblock Plus Add-On, MOZILLA, <https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/statistics/?last=30> (last visited Jan. 30, 2013).

⁸¹ X-Do-Not-Track support in NoScript, HACKADEMIX, <http://hackademix.net/2010/12/28/x-do-not-track-support-in-noscript> (Dec. 28, 2010, 5:31 PM).

⁸² Dean Hachamovitch, *IE9 and Privacy: Introducing Tracking Protection*, MICROSOFT IE BLOG (Dec. 7, 2010, 1:10 PM), <http://blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx>; Dean Hachamovitch, *Update: Effectively Protecting Consumers from Online Tracking*, MICROSOFT IE BLOG (Jan. 25, 2011, 2:43 PM), <http://blogs.msdn.com/b/ie/archive/2011/01/25/update-effectively-protecting-consumers-from-online-tracking.aspx>.

⁸³ Peter Bright, *Do Not Track support added to Chrome, arriving by the end of the year*, ARS TECHNICA, Sept. 14, 2012, <http://arstechnica.com/information-technology/2012/09/do-not-track-support-added-to-chrome-arriving-by-the-end-of-the-year>; Sean Harvey & Rajas Moonka, *Keeping your opt-outs*, GOOGLE PUB. POLY BLOG (Jan. 24, 2010, 12:00 PM), <http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html>.

⁸⁴ See Julia Angwin, *Web Tool On Firefox To Deter Tracking*, WALL ST. J., Jan. 24, 2011, <http://online.wsj.com/article/SB10001424052748704213404576100441609997236.html>; Stephen Shankland, *Mozilla offers do-not-track tool to thwart ads*, CNET NEWS DEEP TECH, Jan. 24, 2011, http://news.cnet.com/8301-30685_3-20029284-264.html.

⁸⁵ Natasha Singer, *Do Not Track? Advertisers Say 'Don't Tread on Us'*, N.Y. TIMES, Oct. 13, 2012, http://www.nytimes.com/2012/10/14/technology/do-not-track-movement-is-drawing-advertisers-fire.html?_r=1&.

havioral Advertising”⁸⁶ to make opting out of targeted advertising simpler. The resulting Digital Advertising Alliance is a collaboration among the leading trade associations in the field, including: American Association of Advertising Agencies, American Advertising Federation, Association of National Advertisers, Better Business Bureau, Digital Marketing Association, Interactive Advertising Bureau, and Network Advertising Initiative.⁸⁷ Their program uses an “Advertising Option Icon” to highlight a company’s use of targeted advertising and gives consumers an easy-to-use opt-out option.⁸⁸ It was accompanied by an educational initiative, www.AboutAds.info, which offers consumers information about online advertising.⁸⁹ The independent Council of Better Business Bureaus will enforce compliance with the system.⁹⁰ Self-regulatory efforts such as these have the added advantage of being more flexible than government regulation, which tends to lock in sub-optimal policies and stifle ongoing innovation.

Again, this survey only scratches the surface of what is available to privacy-sensitive web surfers today.⁹¹ Importantly, this inventory does not include the many different types of digital security tools that exist today.⁹²

What these tools and efforts illustrate is a well-functioning marketplace that is constantly evolving to offer consumers greater control over their privacy without upending online markets through onerous top-down regulatory schemes. Policymakers would be hard-pressed to claim any sort of “market failure” exists when such a robust marketplace of empowerment tools exists to serve the needs of privacy-sensitive web surfers.

Importantly, it is vital to realize that most consumers will never take advantage of these empowerment tools, just as the vast majority of parental control technologies go untapped by most families.⁹³ This is due to a number of factors, most notably that not every individual or household will have the same needs and values as they pertain to either online safety and digital privacy.

Therefore, the fact that not every individual or household uses empowerment tools should not be used as determination of “market failure” or the need for government regulation. Nor should the effort or inconvenience associated with using such tools be viewed as a market failure.⁹⁴ What matters is that these tools exist for those who wish to use them, not the actual uptake or usage of those tools or the inconvenience they might pose to daily online activities.

Government officials can take steps to encourage the use of PETs, but it is even more essential that they do not block or discourage their use.⁹⁵ For example, limitations on encryption technologies or mandates requiring that web surfers use online

⁸⁶ *Self-Regulatory Program for Online Behavioral Advertising*, DIGITAL ADVERTISING ALLIANCE, <http://www.aboutads.info> (last visited Jan. 30, 2013).

⁸⁷ Press Release, Network Advertising Initiative, 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) [hereinafter Major Marketing], www.networkadvertising.org/pdfs/Associations104release.pdf.

⁸⁸ *Id.*

⁸⁹ *Self-Regulatory Principles*, DIGITAL ADVERTISING ALLIANCE, <http://www.aboutads.info/principles> (last visited Jan. 30, 2013).

⁹⁰ Major Marketing, *supra* note 180, at 2.

⁹¹ There are many other mundane steps that users can take to protect their privacy. See, e.g., Kashmir Hill, *10 Incredibly Simple Things You Should Be Doing To Protect Your Privacy*, FORBES, Aug. 23, 2012, <http://www.forbes.com/sites/kashmirhill/2012/08/23/10-incredibly-simple-things-you-should-be-doing-to-protect-your-privacy>.

⁹² Online security and digital privacy are related, but are also distinct in some ways. For example, technically speaking, anti-virus and other anti-malware technologies are considered security tools, but they can also help protect a user’s privacy by guarding information she wishes to keep private.

⁹³ Adam Thierer, *Who Needs Parental Controls? Assessing the Relevant Market for Parental Control Technologies*, PROGRESS ON POINT, Feb. 2009, at 4–6, <http://www.pff.org/issuespubs/pops/2009/pop16.5parentalcontrolsmarket.pdf>.

⁹⁴ The Supreme Court has held as much in the context of child safety. See *United States v. Playboy Entm’t Grp.*, 529 U.S. 803, 824 (2000): “It is no response that voluntary blocking requires a consumer to take action, or may be inconvenient, or may not go perfectly every time. A court should not assume a plausible, less restrictive alternative would be ineffective; and a court should not presume parents, given full information, will fail to act.”

⁹⁵ A. Michael Froomkin, *The Death of Privacy*, STAN. L. REV. 1461, 1506, 1529 (2000): “Sometimes overlooked, however, are the ways in which existing law can impose obstacles to PETs. Laws and regulations designed to discourage the spread of cryptography are only the most obvious examples of impediments to privacy-enhancing technology.”

age verification or identify authentication technologies would undermine user efforts to shield their privacy.⁹⁶

Appendix III: Societal Adaptation, Evolving Cultural Norms & Privacy

Many technologies or types of media that are originally viewed as culturally offensive or privacy-invasive very quickly come to be assimilated into our lives, despite initial resistance.⁹⁷ A cycle of initial *resistance*, gradual *adaptation*, and then eventual *assimilation* is well-established in the context of popular entertainment.⁹⁸ For example, the emergence of dime novels, comic books, movies, rock-and-roll music, video games, and social networking services all lead to “moral panics”⁹⁹ or “technopanics.”¹⁰⁰ Over time, however, society generally came to accept and then even embrace these new forms of media or communications technologies.¹⁰¹

The same cycle of resistance, adaptation, and assimilation has played out countless times on the privacy front as well and “after the initial panic, we almost always embrace the service that once violated our visceral sense of privacy.”¹⁰² The introduction and evolution of photography provides a good example of just how rapidly privacy norms adjust. The emergence of the camera as a socially disruptive force was central to the most important essay ever written on privacy law, Samuel D. Warren and Louis D. Brandeis’s famous 1890 *Harvard Law Review* essay on “The Right to Privacy.”¹⁰³ Brandeis and Warren claimed “modern enterprise and invention have, through invasions upon his privacy, subjected [man] to mental pain and distress, far greater than could be inflicted by mere bodily injury.”¹⁰⁴ In particular, “instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life,” they claimed, “and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’”¹⁰⁵

The initial revulsion that many citizens felt toward this new technology was a logical reaction to the way it disrupted well-established social norms.¹⁰⁶ But personal norms and cultural attitudes toward cameras and public photography evolved quite rapidly. Eventually, cameras became a widely embraced part of the human experience and social norms evolved to both accommodate their place in society but also scold those who would use them in inappropriate, privacy-invasive ways.

That same sort of societal adaptation was on display more recently following the introduction of Google’s “Gmail” e-mail service in 2004. Gmail was greeted initially with hostility by many privacy advocates and some policymakers, some of whom wanted the service prohibited or tightly regulated.¹⁰⁷ A bill was floated in California that would have banned the service.¹⁰⁸ Some privacy advocates worried that Google’s contextually targeted advertisements, which were based on keywords that appeared in their e-mail messages, were tantamount to reading users’ e-mail and

⁹⁶ Adam Thierer, *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions*, PROGRESS ON POINT, Mar. 2007, at 3, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=976936.

⁹⁷ Doug Aamoth, *A Bunch of Tech Things People Have Threatened to Quit Recently*, TIME/TECH, Dec. 18, 2012, <http://techland.time.com/2012/12/18/a-bunch-of-tech-things-people-have-threatened-to-quit-recently>.

⁹⁸ Adam Thierer, *Why Do We Always Sell the Next Generation Short?*, FORBES, Jan. 8, 2012, <http://www.forbes.com/sites/adamthierer/2012/01/08/why-do-we-always-sell-the-next-generation-short>. (“many historians, psychologists, sociologists, and other scholars have documented this seemingly never-ending cycle of generational clashes.”)

⁹⁹ Robert Corn-Revere, *Moral Panics, the First Amendment, and the Limits of Social Science*, 28 COMMUNICATIONS LAWYER (2011).

¹⁰⁰ Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J. L. SCI. & TECH. 309, 364–73, (2013).

¹⁰¹ *Id.* at 364–8.

¹⁰² Larry Downes, Cato Institute, *A Rational Response to the Privacy “Crisis,”* Policy Analysis, 10, Jan. 7, 2013, <http://www.cato.org/publications/policy-analysis/rational-response-privacy-crisis>.

¹⁰³ Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

¹⁰⁴ *Id.* at 196.

¹⁰⁵ *Id.* at 195.

¹⁰⁶ Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295 (2010): “the rapid adoption of the portable camera had begun to make people uneasy about its ability to record daily life away from the seclusion of the photo studio. Old norms of deference and respect seemed under assault, and there was great anxiety among elites keen on protecting their status, authority, and privacy.”

¹⁰⁷ Adam Thierer, *Lessons from the Gmail Privacy Scare of 2004*, TECH. LIBERATION FRONT, Mar. 25, 2011, <http://techliberation.com/2011/03/25/lessons-from-the-gmail-privacy-scare-of-2004>.

¹⁰⁸ See Eric Goldman, *A Coasean Analysis of Marketing*, WISC. L. REV. 1151, 1212 (2006) (“California’s reaction to Gmail provides a textbook example of regulator antitechnology opportunism.”)

constituted a massive privacy violation.¹⁰⁹ Users quickly adapted their privacy expectations to accommodate this new service, however, and the service grew rapidly.¹¹⁰ By the summer of 2012, Google announced that 425 million people were actively using Gmail.¹¹¹

Sometimes companies push too aggressively against established privacy norms, however, and users push back. This was true for Instagram in late 2012. On December 17, 2012, the popular online photo sharing service, which is owned by Facebook, announced changes to its terms of service and privacy policy that would have allowed it to more easily share user information and even their photographs with Facebook and advertisers.¹¹² Within hours of announcing the changes, Instagram found itself embroiled in a consumer and media firestorm.¹¹³ The uproar also “helped a number of [competing] photo-sharing applications garner unprecedented amounts of traffic and new users.”¹¹⁴ One rival called EyeEm reported that daily sign-ups had increased a thousand percent by the morning after the Instagram announcement.¹¹⁵ According to some estimates, Instagram “may have shed nearly a quarter of its daily active users in the wake of the debacle.”¹¹⁶

Instagram’s experience serves as an example of how consumers often “vote with their feet” and respond to privacy violations by moving to other services, or at least threatening to do so unless changes are made by the offending company.¹¹⁷ Just three days after announcing those changes, Instagram relented and revised its privacy policy.¹¹⁸ In an apology posted on its corporate blog, Instagram co-founder Kevin Systrom noted that “we respect that your photos are your photos. Period.”¹¹⁹ Despite the rapid reversal, a class action lawsuit was filed less than a week later.¹²⁰ Although experts agreed the lawsuit was unlikely to succeed, such legal threats can have a profound impact on current and future corporate behavior.¹²¹

These episodes show how, time and time again, humans have proven to be resilient in the face of rapid technological change by using a variety of adaptation and coping mechanisms to gradually assimilate new technologies and business practices into their lives.¹²² Other times they push back against firms that disrupt establish privacy norms and encourage companies to take a more gradual approach to technological change.

¹⁰⁹ See Chris Jay Hoofnagle *et al.*, *Letter to California Attorney General Lockyer*, Electronic Privacy Information Center, May 3, 2004, <http://epic.org/privacy/gmail/agltr5.3.04.html>.

¹¹⁰ Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 984–5 (2013), (noting that the Gmail case study, “serves as a reminder of the limits of privacy law, because sometimes the consuming public, faced with truthful full disclosure about a service’s privacy choices, will nevertheless choose the bad option for privacy, at which point there is often little left for privacy advocates and regulators to do.”)

¹¹¹ Dante D’Orazio, *Gmail Now Has 425 Million Total Users*, THE VERGE, June 28, 2012, <http://www.theverge.com/2012/6/28/3123643/gmail-425-million-total-users>.

¹¹² Jenna Wortham & Nick Bilton, *What Instagram’s New Terms of Service Mean for You*, N.Y. TIMES BITS, Dec. 17, 2012, <http://bits.blogs.nytimes.com/2012/12/17/what-instagrams-new-terms-of-service-mean-for-you>.

¹¹³ Joshua Brustein, *Anger at Changes on Instagram*, N.Y. TIMES BITS, Dec. 17, 2012, <http://bits.blogs.nytimes.com/2012/12/18/anger-at-changes-on-instagram>.

¹¹⁴ Nicole Perlroth & Jenna Wortham, *Instagram’s Loss Is a Gain for Its Rivals*, N.Y. TIMES BITS, Dec. 20, 2012, <http://bits.blogs.nytimes.com/2012/12/20/instagram-loss-is-other-apps-gain/?smid=tw-nytimesbits&seid=auto>.

¹¹⁵ *Id.*

¹¹⁶ Garrett Sloane, *Rage Against Rules*, N.Y. POST, Dec. 27, 2012, http://www.nypost.com/p/news/business/rage_against_Dh05rPifiXBtJRE1rCOyML.

¹¹⁷ Downes, *A Rational Response*, 11: “Often the more efficient solution is for consumers to vote with their feet, or these days with their Twitter protests. As social networking technology is coopted for use in such campaigns, consumers have proven increasingly able to leverage and enforce their preferences.”

¹¹⁸ Declan McCullagh & Donna Tam, *Instagram Apologizes to Users: We Won’t Sell Your Photos*, CNET NEWS, Dec. 18, 2012, http://news.cnet.com/8301-1023_3-57559890-93/instagram-apologizes-to-users-we-wont-sell-your-photos.

¹¹⁹ Instagram, *Thank You, and We’re Listening*, INSTAGRAM BLOG, Dec. 18, 2012, <http://blog.instagram.com/post/38252135408/thank-you-and-were-listening>.

¹²⁰ Zach Epstein, *Instagram Slapped with Class Action Lawsuit over Terms of Service Fiasco*, BGR.COM, Dec. 25, 2012, http://bgr.com/2012/12/25/instagram-slapped-with-class-action-law-suit-over-terms-of-service-fiasco-267480/?utm_source=dlvr.it&utm_medium=twitter.

¹²¹ Jeff John Roberts, *Instagram Privacy Lawsuit is Nonsense Say Experts*, GIGAOM, Dec. 26, 2012, <http://gigaom.com/2012/12/26/instagram-privacy-lawsuit-is-nonsense-say-experts>.

¹²² Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J. L. SCI. & TECH. 309, 364–73, (2013).

Appendix IV: Why America's Privacy Regime is Worth Defending:

A BETTER, SIMPLER NARRATIVE FOR U.S. PRIVACY POLICY

by Adam Thierer [originally published on the *Technology Liberation Front* blog, March 19, 2013]

Last week on his personal blog, Peter Fleischer, Global Privacy Counsel for Google, posted an interesting essay titled, "We Need a Better, Simpler Narrative of U.S. Privacy Laws."¹²³ Fleischer says that Europe has done a better job marketing its privacy regime to the world than the United States and argues that "the U.S. has to figure out how to explain its privacy laws on the global stage" since "Europe is convincing many countries around the world to implement privacy laws that follow the European model." He notes that "in the last year alone, a dozen countries in Latin America and Asia have adopted euro-style privacy laws [while] not a single country, anywhere, has followed the U.S. model." Fleischer argues that this has ramifications for long-term trade policy and global Internet regulation more generally.

I found this essay very interesting because I deal with some of these issues in my latest law review article, "The Pursuit of Privacy in a World Where Information Control is Failing."¹²⁴ In the article, I suggest that the United States *does* have a unique privacy regime and it is one that is very similar in character to the regime that governs online child safety issues. Whether we are talking about online safety or digital privacy, the defining characteristics of the U.S. regime are that it is bottom-up, evolutionary, education-based, empowerment-focused, and resiliency-centered. It focuses on responding to safety and privacy harms after exhausting other alternatives, including market responses and the evolution of societal norms.

The EU regime, by contrast, is more top-down in character and takes a more static, inflexible view of privacy rights. It tries to impose a one-size-fits-all model on a diverse citizenry and it attempts to do so through heavy-handed data directives and ongoing "agency threats." It is a regime that makes more sweeping pronouncements about rights and harms and generally recommends a "precautionary principle"¹²⁵ approach to technological change in which digital innovation is more "permissioned."¹²⁶

Put simply, the U.S. regime is *reactive* in character while the EU regime is more *preemptive*. The U.S. system focuses on responding to safety and privacy problems using a more diverse toolbox of solutions, some of which are governmental in character while others are based on evolving social and market norms and responses. To be clear, law *does* enter the picture here in the United States, but it does so in a very different way than it does in the European Union. Fleischer actually explains that point quite nicely in his essay:

What is the U.S. model? People in the privacy profession know that the U.S. has a dense "patchwork" model of privacy laws: every individual U.S. State has numerous privacy laws, the Federal government has numerous sectoral laws, and numerous other "non-privacy" laws, like consumer protection laws, are regularly invoked in privacy matters. Regulators in many corners of government, ranging from State attorneys general, to the Federal Trade Commission, and armies of class action lawyers inspect every privacy issue for possible actions.¹²⁷

Indeed, in my new law review article, I summarize the litany of cases the FTC has brought recently on the data security and privacy front using its authority under Section 5 of the Federal Trade Commission Act to police "unfair and deceptive" practices. State AGs are active on this front as well, and there is plenty of class action activity every time there's a privacy or data security screw-up.

Meanwhile, public officials continue to work collaboratively with privacy advocates, corporations, and educators to develop better education and awareness-building efforts, including "best practices" on safety, security, and privacy issues.

For more details on this U.S. model, please consult pages 436–454 of my article, in which I provide a comprehensive overview of what I refer to as America's "3–

¹²³ Peter Fleischer, *We Need a Better, Simpler Narrative of U.S. Privacy Laws*, Mar. 12, 2013, <http://peterfleischer.blogspot.com/2013/03/we-need-better-simpler-narrative-of-us.html>.

¹²⁴ Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 Harv. J. L. & Pub. Pol. 409 (2013), papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680.

¹²⁵ Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J. L. SCI. & TECH. 309 (2013).

¹²⁶ Adam Thierer, *Who Really Believes in "Permissionless Innovation"?* TECHNOLOGY LIBERATION FRONT, Mar. 4, 2013, <http://techliberation.com/2013/03/04/who-really-believes-in-permissionless-innovation>.

¹²⁷ Fleischer.

E Approach” to dealing with online safety and digital privacy concerns. The “3-Es” refer to *education*, *empowerment*, and targeted *enforcement* of existing legal standards. As I note in the article:

[America’s “3-E Approach”] does not imagine it is possible to craft a single, universal solution to online safety or privacy concerns. It aims instead to create a flexible framework that can help individuals cope with a world of rapidly evolving technological change and constantly shifting social and market norms as they pertain to information sharing.¹²⁸

But what frustrates Fleischer is that the U.S. model still doesn’t translate into a simple narrative for international audiences:

How on earth do you explain U.S. privacy laws to an international audience? How do you explain the role of class action litigation to people in countries where it doesn’t even exist? The U.S. privacy law narrative is convoluted. That’s a pity, since almost all of the global privacy professionals with whom I’ve discussed this issue agree with me that the sum of all the individual parts of U.S. privacy laws amounts to a robust legal framework to protect privacy. (I didn’t say “perfect”, since laws never are, and I’m not grading them either.) By contrast, Europe’s privacy narrative is simple and appealing. Its laws are very general, aspirational, horizontal and concise. Critics could say they’re also inevitably vague, as any high-level law would have to be. But, like the U.S. Bill of Rights, they have a sort of simple and profound universality that has inspired people around the world. And they are enforced (at least, on paper) by a single, identifiable, specialist regulator.¹²⁹

I understand the frustration Fleischer is expressing here regarding how to frame the U.S. model for broader audiences. But the crucial point here is that, as he correctly notes, “the sum of all the individual parts of U.S. privacy laws amounts to a robust legal framework to protect privacy,” even if it is the case that we will never achieve anything near perfection when it comes to online privacy (or online safety for that matter). But it is unfortunate that Fleischer ignores the many other moving pieces at work here that are important to the U.S. system, especially the diverse array of educational and awareness-building efforts, as well as the astonishing array of empowerment tools that currently exist to help user protect their privacy to the degree they desire.

Of course, it should also be obvious that the U.S. regime is never going to appeal to a global audience as much as Europe’s privacy regime for the same reason that many other U.S. policy regimes don’t appeal to certain countries or their leaders: our systems aren’t regulatory enough in character for them! But while those top-down, centralized, preemptive regulatory regimes will almost always be more “aspirational, horizontal and concise”—and, therefore, have greater appeal to activist-minded lawmakers and regulators—that also means those regimes will likely leave less breathing room for social evolution (*i.e.*, evolving norms about safety and privacy) and economic innovation (new digital goods and services that potentially disrupt those regulatory expectations). That has real consequences for long-term growth and overall consumer welfare.

Regardless, to the extent we need “a better, simpler narrative for U.S. privacy policy” as Fleischer suggests, I believe we can boil it down to a few words: *bottom-up*, *evolutionary*, *flexible*, and *reactive*. What this means for public policy is clear: *We need diverse tools and solutions for a diverse citizenry, while leaving plenty of breathing room for ongoing innovation and the evolution of social norms and market responses.* Whether it’s online safety or digital privacy, public policy should take into account the extraordinary diversity of citizen needs and tastes and leave the ultimate decision about acceptable online content and interactions to them. We should look to educate and empower citizens so that they can make decisions about their online safety and privacy for themselves so that policymakers are not constantly trying to make decisions on their behalf.

This is a model worth defending, even if it is sometimes hard to delineate its contours. Please read my *Harvard Journal of Law & Public Policy* article for a fuller exploration of that model and a defense of it.

The CHAIRMAN. And I will have one in just a moment.

This is to each witness to answer briefly. The online advertising industry, as has been pointed out, stood at the White House last

¹²⁸ Thierer, *The Pursuit of Privacy*, at 437.

¹²⁹ Fleischer.

February and made a promise to honor Do-Not-Track requests from consumers by the end of the year. And yet, as I sit here today, these promises have been broken.

Do-Not-Track is still just an idea, not a reality, and I have heard a lot of finger pointing in the press. So my question is, but now I have you all here, and I would like each of you to tell me what exactly is the hold-up. Can you come to the table at the W3C and make good on your word to implement Do-Not-Track?

Starting with you, Mr. Anderson.

Mr. ANDERSON. Thank you, Chairman.

Yes, we will come to the table and make good on our commitment to honor Do-Not-Track. We have.

The DAA said some things just now that I think are actually specious. The notion that they can't implement Do-Not-Track because Firefox announced that it was going to explore, test third-party cookie blocking is—is just—it is offensive, actually.

The DAA already was not responding to Do-Not-Track. When IE announced that they were going to turn Do-Not-Track on by default, they told their members don't respond to it. We are not doing Do-Not-Track. That was last year. Last year.

This just happened. The third-party cookie thing was in February. And no, we didn't say—it hasn't happened. We said we were going to test it. I have spent days meeting with members, DAA members, members of the ad ecosystem to understand how third-party cookie blocking would affect them.

By the way, what they have told us is some say, depending on where they are in the industry, they will have different answers. Most have said they think the impact would be negligible. Some, who rely on it purely like the retargeting folks—retargeting, which is different than BT, behavior targeting—are extremely concerned.

There is also the sentiment, at least among publishers and many of the ad ecosystem people, that behavioral targeting, the effectiveness itself is questionable. This is not to say that they don't get more money for it, but whether it is actually effective, it is unclear. At least from that sector, that is what they have told us.

So you could speak directly when I am done. So, anyway, that is the answer to my question—to your question.

The CHAIRMAN. Very good. Please.

Mr. MASTRIA. Senator Rockefeller, thank you.

We stand—we sit here today ready to sit and work through the agreement that we made with the White House. So we encourage—as we did in our testimony, we encourage Microsoft, Mozilla, FTC, all the other parties, to sit with us and work through that for a standard that would meet those conditions.

But let me go back to something you mentioned at your opening, if I might?

The CHAIRMAN. Could you go back to answering my question?

Mr. MASTRIA. I thought that was your question, Senator.

The CHAIRMAN. Why isn't it working?

Mr. MASTRIA. That, in fact, we stand ready today to work toward the implementation of the White House agreement for Do-Not-Track.

The CHAIRMAN. Go ahead.

Mr. MASTRIA. I would like to go back to a point that you raised, which was that consumers should make that choice. We agree. We wholeheartedly agree.

What is happening with Mozilla and with Microsoft is that the browsers are making that choice, not the consumer. And that is a completely different dynamic.

Perhaps there are competitive reasons. Perhaps there are other reasons. We don't know. But we know for sure one thing, that user choice is not being satisfied, and that is something that we—we deliver on, we promised to deliver on, and we do on—on a routine basis every single day.

And so, the other point that Mr. Anderson raised that interest-based advertising is somehow some sort of fringe or immaterial thing, I would submit that 2X publishers are willing to pay twice as much for interest-based advertising, and consumers click through those ads twice as often, which means that they find it twice as convenient, twice as relevant, speaks volume for how innovative the product is.

The fact is that there may be other reasons why companies choose to invest in different parts of privacy, but that is not what is going on here. We are the ones who are delivering consumer choice day in and day out. What is being delivered by the browsers right now is not consumer choice. In fact, it is browser choice.

The CHAIRMAN. Mr. Brookman?

Mr. BROOKMAN. I think it is a good question. I can't answer why they haven't turned it on or responded to it.

As I mentioned during my testimony, Google Chrome's Do-Not-Track implementation meets every test they could possibly want. Those signals are going out from users who go out of their way to find that setting and turn it on. Industry is not responding.

Apple Safari, you have to go out of your way to turn it on. Industry is not responding. There is nothing in the White House agreement about cookies. Apple hasn't allowed cookies for 10 years. So I am not entirely sure how that is relevant.

CDT has proposed a reasonable middle ground going forward. Back in January 2011, we have consistently tried to bring both sides to the table to agree. I think it is in industry's interest to agree because if they keep taking a hard line in the sand, it won't be cookies being blocked. It is going to be ads being blocked, and that is the kind of tools Adam was talking about.

Those aren't Do-Not-Track tools. They are ad-blocking tools, which I think are a bad way to go for everybody.

Mr. THIERER. So, Senator, to answer your question, I think there are many reasons why this process has slowed down, but I think one of them is a simple truism that setting technical standards is really hard. And what W3C is doing here is trying to negotiate something for a very complex and fast-evolving ecosystem.

I should point out as well, as I pointed out in an appendix to my testimony, we have sort of been here before with the W3C. W3C has instituted the Platform for Internet Content Selection, or PICS, for online objectionable content. It also tried on privacy—a Platform for Privacy Preferences, or P3P.

These are both good faith efforts to deal with serious issues of online child safety content, privacy issues. Ultimately, they did not

work so well. And this is what leads to my skepticism about trying to use these sort of technical silver bullet schemes, as I call them, to solve these complex problems, as opposed to a multilayered approach to get at the issue.

The CHAIRMAN. Senator Thune?

Senator THUNE. Thank you, Mr. Chairman.

I would direct this to all the witnesses and just ask a general question, and that is do you believe that a multi-stakeholder process, whether it is the ongoing W3C effort, which has been discussed at some length, or a future effort, is a better way to reach an enduring and broad solution than a regulatory approach that would be—come down mandated from the Government?

Mr. ANDERSON. Go ahead, Justin.

Mr. BROOKMAN. So we have heard a lot about this. I mean, it is like the approach that we like is a basic comprehensive privacy law that allows for safe harbor programs like a self-regulatory model like DAA, like a multi-stakeholder approach that gets together and comes up with a code and says, hey, for our industry, if we do this negotiated code, does that mean we are in compliance with existing law?

I think that is the model that we have advocated. We have seen it proposed in President Obama's consumer privacy bill of rights. We have seen it in other legislation. I think that is a good way to get people into the room to agree to reasonable standards.

Without a baseline of saying you have to respect users' privacy, there is not enough incentive, I think, for any individual company to take the right steps in a lot of cases.

Mr. MASTRIA. So I would submit that we run a self-regulatory program. Our program provides meaningful consumer choice every single day. Consumers do take advantage of it. It is in prime real estate. We made sure of that.

And so, I think that our program is far superior, much more nimble than any regulatory mandate. Even today, as we speak, we are getting ready to launch what would be the guiding principles for data collection inside the mobile and applications environment. That is a huge leap forward.

And that is on top of already producing two codes of conduct and multiple technologies to help consumers manage their online privacy. We think that we are more nimble, but we don't take a stance on regulation or legislation.

Senator THUNE. There is another question. This, again, can be open and whoever would care to answer this.

But are there specific and identifiable harms being witnessed in the marketplace today because of behavioral and interest-based advertising?

Mr. THIERER. Privacy is an highly subjective condition, Senator, and obviously, people have different feelings about it, the same way they do about what is optimal safety or security. So it is tricky.

But to the extent that there are actual harms that can be identified, we have many remedies that exist, as I noted in my testimony, whether they be FTC remedies, unfair and deceptive practices, targeted laws dealing with very sensitive privacy issues, such as health, financial, or children issues. And then we also have State laws as a backdrop, along with class action activity.

Where there are harms, they are pursued. The FTC has been incredibly aggressive in recent years and has addressed these things with consent decrees with some of the biggest players in the online economy, which sends a pretty powerful message to other players, I believe.

But for the most part when people talk about these harms, they usually say things like online advertising or targeted advertising is “creepy.” But it is hard for me to find a real harm with creepiness. I think a lot of my neighbors are creepy, but I don’t think they are harmful.

So I would say that we need to identify more concrete harm than creepiness. And we also need to acknowledge the benefits on the other side of that equation.

Mr. MASTRIA. I would submit—oh, was that just—

Senator THUNE. No, go ahead. So, hopefully, his neighbors aren’t watching this.

[Laughter.]

Mr. MASTRIA. Senators, I have been at FTC hearings and workshops where this very issue was addressed, and I have heard staff ask many times, “Where is the harm?” And there hasn’t been any that has been demonstrated.

As Adam suggested, there have been issues of creepiness. And to be sure, that there are folks who would like to have control over their privacy experience online, and that is what we built our tools for, and that is what we see. We see the same kind of response to those tools that we—that the industry has seen in preference management tools for a decade.

A lot of consumers come to the tool. Just knowing that the tool is available oftentimes makes the consumer feel comfortable. But if there is a consumer who feels that much more dedicated to exercising a choice, the tool is there, and 2 million folks, nearly 2 million folks with us have, in fact, exercised that choice.

So I think that that is really the answer to the question. I think from our perspective, as we talk to consumers, when we asked them about what is top of mind in terms of privacy for them, what we hear is viruses, malware, identity theft. Interest-based advertising is not the top of that list.

Mr. ANDERSON. Senator Thune, if I could just—I think you are asking the right question about the harm. It is tough because the harm in this case potentially is if you undermine confidence in the ecosystem, then people don’t engage and participate.

And we saw that with online commerce initially. Remember, people were afraid to put their credit cards on the Web, and that really held back commerce at first until people started to rely on the notion of encryption. Whether they knew what it meant or not exactly or how it worked, they gained more trust. And now we see a booming online commerce, actual transactions online.

But there is something else here that we have talked about choice. It really helps people. The 45 million people on Firefox that I talked about that have turned on Do-Not-Track, we didn’t set that. The users went into the preference and set turn Do-Not-Track on themselves.

So that is 45 million people pored through the menus to turn that on at 17 percent rate of our user base in the U.S.

Mr. BROOKMAN. I think this is really more about consumer choice and consumer preferences rather than harm. I mean, if a couple walks into a restaurant and says, "Hey, can I have a private booth?" The maitre d' doesn't turn around and shout, "What is the harm?" They try to accommodate them. They try to them out. They say, "Yes, OK, you are my customer. I want to help you out."

That is what I think the browsers are doing here. They have heard over and over and over from consumers again that they don't like this. You can judge them for not thinking through the harm very well, but they have made a statement, and they want privacy protection in browsers.

And so, we are seeing the browsers respond to that either by turning off cookies. Some of them offering ad block add-ons. Or what we are trying to do is have a middle ground approach of Do-Not-Track, which is a signal to the company saying, "Hey, you can still get some information about me, but don't retain it, don't build a profile about me."

And that way, I get the advertising, but I don't get you knowing a whole lot about me. That is what we are trying to achieve here. And I think that is what Do-Not-Track is supposed to do.

Mr. MASTRIA. If I may answer one question on the point that Mr. Anderson raised regarding track——

The CHAIRMAN. I am sorry. Your time is up. The Senator's time is up.

You have talked a good deal. The Senator's time is up. I want to go on to Senator Heller.

Senator HELLER. Senator McCaskill?

The CHAIRMAN. She looks nervous.

Senator MCCASKILL. I don't know what to say.

The CHAIRMAN. Senator McCaskill?

Senator MCCASKILL. You may go first.

Senator HELLER. It is fine. It is fine.

Senator MCCASKILL. We are going to get along very well on our subcommittee, Mr. Chairman.

The CHAIRMAN. This is according to who got here first.

Senator MCCASKILL. Oh, OK. Well, go ahead. I am staying so——

Senator HELLER. I am happy to move forward. Thank you, Mr. Chairman. Thanks for giving me a couple minutes.

And I want to thank again for those who are testifying, for being here today and taking time out of a busy schedule.

Mr. Brookman, I have some specific questions. Some of the things I understand, if I go online and I purchase an item, I know I am going to be tracked. I know that.

After today's vote, I guess, on the Senate floor, I am also going to be taxed. But that is a different discussion for another time.

I also know that third-party advertising companies puts cookies on my computer. I know that. Let me ask you, do you believe that the general public understands this?

Mr. BROOKMAN. I don't. I think the ad industry has done a noble job in trying to move forward with the icon project to put some notice on all the ads that you can click through and get information.

Unfortunately, as I have gone around and talked at events where people come and want to hear about privacy, very, very, very few understand what that is or have interacted with it or know what

is going on. Talking with people outside of my industry when I describe what online behavioral advertising is, they say, "What?"

I think as targeting is getting better, I think people are starting to see very targeted ads. So they are seeing more and more retargeting. So when my wife looks for shoes online, as I am surfing later, those shoes follow me around the Internet.

I went to the Venetian site once, and the Venetian followed me around for 6 months. And so, I think people are starting to become aware something is happening, but I don't think they understand how it works.

And you see polls after poll after poll is when it is described to them, a lot of them don't like it. I just want to give them some choice around it.

Senator HELLER. Yes, if you have follow-up?

Mr. MASTRIA. Yes, specific to the polls. So we asked consumers not in any inflammatory terms, we asked them simply what is your preferred online experience? How do you like getting free content? What do you like about advertising?

And you know what we heard back? What we heard back is that the preferred online experience is free content with relevant advertising. Consumers acknowledge that they are going to get advertising. It might as well be for something that they are interested in.

I don't like to golf particularly, but I do like to bike ride. Why not, it would make a lot more sense for me to get that bicycling ad.

I want to make one last point about the point that Mr. Anderson raised. The Do-Not-Track that is being set inside the Mozilla browser does not mean anything. Consumers are being told Do-Not-Track. Does that mean zero data collection? As you acknowledged, Chairman, the reality is that there has to be some data collection for the Internet to work properly.

In the case of Mozilla, in fact, we know 60 percent of folks would like to have no tracking even on first-party sites. So does that mean that no first party, if you are looking at somebody's site, that they cannot collect data on you? What does it mean?

And I think that that is really one of the challenges here is that there is no standard definition for what that means, and therefore, answering that signal, as it has been so simply put, has been something of a challenge. And so, what we are looking for is to sit down, go through the White House commitment that we all agreed to, and map that out, understand what it means. We have a definition. We have a standard, and we would be willing to abide by it.

Senator HELLER. Let me go back to you, Mr. Brookman—and thank you for your comments.

There are some that believe that first-party tracking online tracking is better than third-party tracking, obviously because of the online introduction. Is that an accurate assumption?

Mr. BROOKMAN. I think it is more intuitive, right? I mean, if I go to Amazon.com, I buy a bunch of stuff. Later on, Amazon says here are the power drills. You asked for that last time. I kind of get I have a relationship with Amazon. They are showing me things that I liked before.

Later on, if I read stories about the New York Giants on *Newyorktimes.com*, and some company I don't know reads that and gathers it, and then later, I am at *Foxnews.com*, and I start getting Giants ads, I am like, "Who knows this? Who is this?" I mean, does Fox News know this? Does some company I never heard of know this?

So I think that relationship and that contextual intuitiveness does make first-party tracking a little more understandable for most users.

Senator HELLER. Very good. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator.

Senator McCaskill?

Senator MCCASKILL. So this is really hard because we have browsers versus advertisers. We have first party versus third party. We have big versus little. And the browsers are all pretty big.

I mean, I know my friend from Mozilla, and I visited there, and I have a lot of respect for what they are doing. And I get what Microsoft has done. But a lot of this is about competing with Google. And Google hasn't been talked about a whole lot today, and obviously, they are the huge, giant thing in the room because they are first party, and they have a lot.

So my first question is how did we get to the point that W3C is deciding all this stuff? I mean, it seems weird to me.

I mean, I am running around here, and we have so many people worried about the sovereignty of our country and who is deciding our economic future, and we have all this stuff. I mean, we have got people in the Senate that actually believe the United Nations is something that we can't be a party to anymore, that they are threatening us.

And now the biggest part of our economic growth in this country, that sector of our economy, we are all saying we are going to turn it over to W3C. And they have done technical before, but I don't recall them making huge policy decisions like this.

And I will be honest with you, I know we are bad at this. You know, trying to get this done and reconciling browsers versus advertisers, first party versus third party and big versus little. But I am a little uncomfortable that all of us seem to have agreed in the room that we are ceding the authority to set this policy to some organization I am not even sure who is in charge of this organization.

Who do they answer to? Who are they, and how did we get to this point?

Mr. MASTRIA. Senator, I can tell you based on where the DAA has been, and I mentioned earlier in my testimony the White House agreement, which we still hold, the browsers brought W3C into this.

We sit at the table. We are parties to the negotiation. We try to be constructive when we can, even to the point of trying to be educational on things like businesses need to have their customer data bases. There is no way around that. Right? We had to make that point.

But browsers brought them in. Again, we are willing to sit down to make the White House agreement a reality.

Senator McCASKILL. OK. Your turn, Mr. Anderson.

Mr. ANDERSON. Thank you, Senator. That is a good question.

So, as you recall, when DNT was initially launched, the reason why people couldn't respond to it was because trade said, well, we don't know what it means. So we said how about a multi-stakeholder process? Let us use the W3C. They are a standards body. They are used to doing it and defining it. So we all agreed let us go there and define it.

Senator McCASKILL. But had they done policy before, or had they just done tech?

Mr. ANDERSON. No, no. Yes, policy—and I would agree with you. They don't do policy. They do technical standards.

Senator McCASKILL. But isn't this policy?

Mr. ANDERSON. That is what I have said here, that they had should be focused on the technical side, but not the self-regulatory part. The W3C is not a self-regulatory body. At best it will do is codify an agreement of people that want to create a common agreement.

Senator McCASKILL. So what you are basically saying is this is just a place to go to try to see if all of you guys can agree? Couldn't we just set a room somewhere and all of you get there and try to decide and see if you all agree?

Mr. ANDERSON. Yes. Well, that is how HTML 5 was set up. So W3C didn't work for HTML 5. The browser makers got together and informally created the standard, and once it was sufficiently understood, you know, 70, 80 percent done, it sort of got turned over to W3C.

Senator McCASKILL. Are we setting the precedent if this comes from W3C? Are they going to be the policymaking body for the Internet sector for time immemorial?

Mr. MASTRIA. I think this is going down——

Senator McCASKILL. Let me hear from down here.

Mr. THIERER. I just want to say one brief thing in defense of the W3C here because I have been critical of some of the things they have done, including in this process. But no matter what one thinks of the W3C or this process, I think most people in the Internet community would agree that it is better positioned to deal with technical standard-setting processes than the FTC or other regulatory agencies if for no other reason that it is a more evolutionary body. It can go with the flow. It can change.

We might not even have cookies in 5 to 10 years. It might be something totally different. The W3C process could maybe evolve to deal with that problem.

So I think it is wrong—it is not a shadowy group that we need to worry about. They actually do some really good work.

Senator McCASKILL. Can you say that about the U.N.? Can we not worry about the U.N. anymore?

Mr. THIERER. If it was dealing with the Internet, I might be a little bit concerned. I don't know. But in this process, I don't think we need to worry too much about this. But I think, again, it is better that we evolve it through that process than through a top-down process.

Senator McCASKILL. Than through Government?

Mr. THIERER. Than through an FTC process.

Mr. BROOKMAN. Just one thing to point out, the W3C is a voluntary coalition of—mostly it is a bunch of companies, right? And the people in the room are Google and Yahoo! and Microsoft and Adobe and AT&T. I mean, CDT is a member. EFF is a member. Stanford is a member. But other than that, it is mostly just large companies trying to get together to talk through decisions about how the Internet actually functionally works.

Senator MCCASKILL. OK. Well, I just want to make sure—and I have had this discussion with several of the folks that have been mentioned today. I want to make sure that we are not shutting down something after the big guys have all gotten the cows out of the barn, and they have got this, and now it is going to get shut down so all the little ones that can grow and become the big ones of tomorrow have less of an opportunity to access the richness that is online commerce. And that is a concern.

And I know that all of you share it, and we have got to keep working at this because this is harder than it looks.

Senator THUNE. Mr. Chairman, I would say that on behalf of a number of colleagues on my side that we would be really worried if W3C is run by the U.N.

[Laughter.]

Senator MCCASKILL. I gathered that. We will probably have a vote tomorrow. And next we will say that they are sending out drones.

[Laughter.]

The CHAIRMAN. I think the point here is that W3C, or whatever it is, it doesn't really make any difference. It has no authority whatsoever, absolutely none whatsoever. And I think that some of you have used it as a takeoff place to talk about it rather than about the questions that we are really here to solve, and that is how do you protect the vast number of people who use the Internet and who use through the browsers of the Web, and they have no idea what is going on?

I will give you an example. This morning, I was with somebody. We were talking about this. And he said that is funny. Just last night, I was trying to—I wanted to find out about something, and I went on. And I began to get an answer, but then it referred me to the down below part. And the down below part was all this tiny print, which we on the Commerce Committee are so familiar with through health insurance companies and the cruise lines.

I don't want to compare you to the cruise lines. You really don't want me to compare you to the cruise lines, I promise. Because what they do, for example, is if you buy a ticket, you have to buy the ticket. They have a distinguished record, as you know. And then after you have bought the ticket, you sort of peel down the part of the ticket, and you discover that you just ceded all your rights to bring any class action suits against the cruise line, this kind of stuff.

There is a similarity in the ignorance of a lot of consumers, not because they are dumb, but just because they don't have the time to do all of this. And I think probably a tremendous percentage of those who go onto the Internet with the idea of buying or whatever, it is situational. I want to read about France, and so then they start getting ads about the cheapest flights to France. That is fine.

Others are behavioral. That gets a little bit more serious because that covers a much broader area of activity, and what people write on blogs and all kinds of things. And people really do get to know you very, very well.

But they don't know, the great majority of the people who use the Internet, which is just so young—Al Gore did such a good job—and such a good job that today it is the number one national security threat to the United States of America through cybersecurity. And we are all trying to figure out in 20 years, how does something like this happen, or 25 years, whatever it is.

But the point is they don't know. That is the harm that you are talking about. You are not talking about harm or creepiness or your neighbors, whatever. The harm is that people don't know what they are getting into. They don't know whether or not because they can't find it. It is in small print.

I think it is all of this is rather easy, Senator McCaskill, not very hard. I just think it is a question of do people want to say, as a matter of general principle, that minus the cybersecurity and fraud and stuff that we have built in to make sure that there is that there, that they want to be left alone.

They want to do—they want to transact their business. They don't want to be followed around. They don't want to be followed up on, and they have no way of doing that. Plus, no matter what kind of WC3, or whatever it is, W3C—is that it?

Senator McCASKILL. It is W3C.

The CHAIRMAN. I don't really care. But no matter what, it is not enforceable, and you can't enforce it. And you don't enforce it. So you can talk about "our Do-Not-Track policy." You don't have one that you can enforce. Correct? Correct?

Mr. MASTRIA. Senator, if I might—

The CHAIRMAN. No, I am just asking, am I correct?

Mr. MASTRIA. No, you are not, Senator.

The CHAIRMAN. OK. Well, then you tell me all about that.

Mr. MASTRIA. Yes, absolutely. Our self-regulatory program actually tracks very closely to the principles that you lay out in your own bill, number one. Number two, in terms of compliance, the counsel of Better Business Bureau has brought 19—to date, 19 compliance cases against both members of DAA and nonmembers, covering the entire marketplace of participants.

We think that we do offer a single one-button choice to consumers who choose not to receive relevant advertising and have their data either collected or used. That is what the DAA does.

In terms of making it available and education, we are completely with you, Senator. And in fact, we are so much with you that we place our icon—we have removed this piece outside of the traditional privacy policy, and we put it in prime real estate on top of every ad creative, a trillion times a month. And this isn't on small ads and little ads that are buried. This is at the top of many—

The CHAIRMAN. The symbol is.

Mr. MASTRIA. That is right, the symbol is. And if you click on the symbol, you get a choice to opt out. It is as simple as that.

I think we have delivered what basically in principle you have laid out in your bill. We are certainly open to making modifications where necessary. I know Justin is working on one with us right

now in terms of narrowing the research description, and we are happy to continue down that path.

But the reality is that we made an agreement last year at the White House to include browser-based choices as complements to our system. We still stand by that deal. We still stand by that agreement. We ask that everybody else who was in that room also stand by that deal. We think that is fair.

The CHAIRMAN. I see it differently, and my time is running out. I see that the reason that you don't like Mozilla and Microsoft, et cetera, is that they have gone—they have made it even easier for the consumer.

We are about consumers here. We are not about how much money you make. We are into how much money you make, provided it doesn't harm consumers or take advantage of consumers or overload them with stuff they don't want.

It is the right of an American to not want to have—you know, I buy DVDs because I like DVDs, OK? And so, I expect to get, about a week after I have gotten a slug of DVDs, a magazine about more DVDs, and I welcome that. Otherwise, I just don't get much reaction from it. I like that.

I don't want to be tracked. I don't want to be tracked contextually. I don't want to be tracked behaviorally. And you do both. And you make—that is the way you have to make your money. But how do you make your money? You make your money by selling ads.

What are we talking about here? We are talking about making it more difficult for you to sell your ads because consumers would be able to say, "I don't want this. I want this turned off. I just simply don't want it. I don't want to be philosophical about it. I don't want to get in the details of it. I just don't want it. I want privacy."

That is a pretty basic American instinct.

Senator Thune?

Senator THUNE. Mr. Chairman, if I might, and I would like to direct this to Mr. Brookman. You mentioned in your prepared testimony that you believe these ongoing negotiations on Do-Not-Track technical standards demonstrate, and I quote, "a need for fundamental reform of our Nation's privacy protection framework."

However, the approach we are currently discussing, both in the W3C process and in the Chairman's legislation, contemplates reforms that focus squarely on the activities of third parties. Do you think that approach that favors the ability of first parties to collect consumer data raises additional competition concerns in the marketplace?

Mr. BROOKMAN. I am not a competition lawyer. I do think comprehensive law should address first-party data collection.

I think the framework we have seen in some of the bills that have been introduced are that for first-party data collection, which is more intuitive, I understand I have a relationship with Amazon. They collect some stuff about me. I may be able to opt out from that marketing, but not on a global basis. I can do it on a one-by-one basis.

Whereas for third parties who I don't have a relationship with, I think the relationship is different. I think the rules have to be a little bit more stringent for third parties.

I think from an average consumer's experience, they get Amazon. They don't get a company like the Rubicon Project because they just don't know who they are. They are not a bad company. It is just they don't have a relationship with them. It is harder for them to track them down and say, "Sorry, leave me alone."

Mr. MASTRIA. Just, Senator, if I may? So Justin earlier mentioned that only the folks inside the DAA program would be affected by the one-button opt-out. Let me just clarify that a little bit.

The folks inside the DAA program are 90 to 97 percent of the entire Internet ecosystem. We encompass almost the entire digital advertising ecosystem. And so, a one-stop button for that is, in fact, what we provide, and we think that we have developed a system that both provides the preferred user experience while giving consumers privacy choices they can act on.

Earlier today, I had soup at lunch. It was Virginia—West Virginian ramp soup. I had never heard of it. I immediately searched for it online. Will I get some advertising related to West Virginia? I probably will.

If it is more to my liking, perhaps it involves biking, I might take an action on it twice as much as if I didn't get it. So that is the color that I want to add to Justin's remarks.

Senator THUNE. This one will be for Mr. Thierer. It appears that privacy and consumer tools are increasingly being used as competitive differentiators in the online market to earn new users. It also appears, however, that certain tools described as consumer empowering can also be used to more firmly establish market power.

Can you speak to the notion of online privacy being used to both enhance and even perhaps diminish competition?

Mr. THIERER. Well, on the enhancing competition point, it was just last night I saw the first Microsoft ad that mentioned Do-Not-Track by name. And Microsoft has been running a series of ads, basically trying to counter Google in many ways and differentiate it from Google based on privacy and security. That is a healthy form of competition in the marketplace that we are seeing.

Likewise, Mozilla, what they have been doing is doing the same thing. You may have heard of a very small start-up search engine called "DuckDuckGo" that competes on privacy and has been putting up billboards in Silicon Valley about how they don't collect any information when you search on their site.

I am not sure what their business model is. We will see. But good luck to them. That is great that we have that sort of competition. The more of that, the better.

In terms of how it could adversely affect the marketplace, I am not too worried so as long as the marketplace continues to evolve dynamically and freely and that we are not locking in any one standard that others may choose.

If it is the case that what Mozilla has chosen to do with third-party cookies or Microsoft has chosen to do with setting the default for Do-Not-Track to on, if consumers flock to it, so be it. They still have other options, and that is good. If they don't like it, it could end up that that tips the balance in favor of Google and Chrome because people just don't want to be bothered with interstitial pop-ups that basically say you have got to allow us to track you. You

have got to allow us to set a cookie, whatever else, and they just say, “Forget this, I am going somewhere else.”

Mr. MASTRIA. If I may? We have a letter here from 700 small publishers that have written to Google—written to Mozilla, apologies, who basically said that the third-party blocking—which I am hopeful is, in fact, just a test and not a real thing—would, in fact, impact their business and their ability to grow.

Senator THUNE. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Thune.

Would Mountain View, California, like to respond to that?

Mr. ANDERSON. Yes, thank you.

Relative to the third-party cookie blocking proposal, you know, there is—they sought to create a petition, and you have 700 people sign up that is right on your homepage. There you go—700, 500, a couple hundred people.

The former Chairman of IAB, we asked him what he thought about this, and the Online Publishers Association, we asked them what they thought about the third-party cookie blocking. And both organizations, they thought that there is a real problem here, fundamentally, and that is one way to address it. They didn’t have the same concerns. They didn’t feel that it was as disastrous as it has been portended here.

But I think even the discussion of the third-party cookie piece conflates Do-Not-Track. So it is almost as if we were saying if there was no proposal for third-party cookie blocking, just take it off the table because we are just evaluating it, why aren’t we responding to Do-Not-Track now from the Firefox users who opt in today? Why doesn’t that happen?

Mr. MASTRIA. If I may? I already answered that. The word “track” means nothing inside the Mozilla browser. That is just the way it is.

And as far as the former chairman of the IAB and the OPA, I would point out this. That the IAB today does not support the Mozilla standard and, in fact, the former chairman does not speak for the IAB. The IAB is the leading trade association for online publishers. It is a founding member of the DAA.

As far as the OPA goes, we have had a conversation with their chief executive, and she assures us that, in fact, there is a problem with the third-party blocking prospect that Mozilla is talking about.

Senator HELLER. Is it my turn?

The CHAIRMAN. Yes, I just apologize.

Senator HELLER. Thank you, Mr. Chairman. I know this issue—

The CHAIRMAN. You have got a great sense of humor. You know that? I love that Las Vegas line.

Senator HELLER. Do you?

The CHAIRMAN. Yes, you were on a roll there.

Senator HELLER. Yes, I will keep it going if you want me to.

The CHAIRMAN. No, actually—

[Laughter.]

Senator HELLER. Thank you, Mr. Chairman.

I know this issue is important to you, and obviously, it is important to all of us up here as we are asking these questions. And clearly, those that are listening to the testimony are as interested.

And I think you are right. I think you are right. People don't know. People just don't know. And I think if they knew, they might care. But we don't know because they don't know.

Mr. Thierer, you talked about some of the members of the industry advertising, getting billboards out. In fact I noticed on a Lakers game, I think it was Microsoft came out and said we are concerned about your privacy, during an NBA playoff game. So, clearly, industry is understanding, boy, it is time to get this information out there because more people are becoming concerned, and I think they have a right to be concerned about the amount of information that is being collected.

So I think I would like to ask about what information is collected today and by whom. And to Mr. Mastria, I would like to direct some of my questions toward you.

Is it a correct statement that third-party advertising companies who are regulated by Network Advertising Initiative do not intentionally collect information used or intended to be used to identify a particular individual, including name, address, telephone number, e-mail address, financial account, or Government-issued identifiers?

Mr. MASTRIA. So the NAI is a founding member of the DAA. I can't speak for them directly, but it is my understanding that is correct.

Senator HELLER. Are there online advertising companies that do collect and use such information about their users?

Mr. MASTRIA. Not that I am aware of for behavioral advertising or interest-based advertising.

Senator HELLER. OK. Mr. Brookman?

Mr. BROOKMAN. May I just interrupt? First of all, I think the NAI code does not actually prevent the use of PII in that way. It allows for—it requires opt-in consent for a retrospective pending PII, but it allow, I think, for using PII and in collecting behavioral data going forward.

The Wall Street Journal reported end of last year about a company called Dataium that would track you by e-mail address. And then I can't remember exactly how it went, but if you were online looking at cars, they could e-mail back to the car dealerships you had previously gone to and said, "Hey, Justin is in the market for that BMW again. Do you want to give him a call?"

So, I mean, there has been reporting. And I believe the code allows for tracking by real name online.

Senator HELLER. Let me follow up.

Mr. MASTRIA. Senator, if I may?

Senator HELLER. Go ahead.

Mr. MASTRIA. Just to clarify, so you asked about the NAI, but the DAA code actually does prohibit what you described.

Senator HELLER. Just to follow up, would you agree that my name, what I bought, my address, and other very identifiable pieces of information are collected elsewhere on the Internet, mostly by first-party and not by most third-party advertising companies?

Mr. MASTRIA. Typically, yes.

Senator HELLER. Mr. Brookman?

Mr. BROOKMAN. Yes, absolutely. They are the ones who have a relationship, and they are the ones that you tell. So, yes.

Senator HELLER. Any other comments?

[No response.]

Senator HELLER. Mr. Chairman, thank you.

The CHAIRMAN. Thank you, Senator Heller.

Mr. Anderson, Mozilla did announce that the newest version of your popular Web browser Firefox would automatically block most third-party cookies. The move was hailed by many as a necessary step to protect consumer privacy, particularly in light of the continued stalemate at W3C.

Will you just tell us why you decided to provide Firefox users with this protection?

Mr. ANDERSON. Thank you for the question.

First, the current third-party cookie proposal is under evaluation. The behavior that would block third-party cookies when a user goes to a site, unless they interact with them, and which also grandfathered in existing cookies, which means we are using that as a proxy for a prior relationship, is under evaluation right now.

It is in what is called an Aurora build. So about 200,000 users have it, and so we are testing it to see if it works and at what it breaks. The next step is that it would move into what is called a Beta build. So there will be several million users that we would test it on to see if it—how it responds.

But the genesis came from a contributor. So Mozilla is an open source project. Contributors propose patches and changes to the Firefox behavior. So this came from a contributor, a volunteer, earlier this year.

From a technical perspective, it seemed to make sense. It had a—it was a promising idea. And the goal, as I understand and as I think about it, is that it creates a Web that reflects a user's expectations.

Users don't expect that when they go to a site hundreds of cookies are placed on them. They just don't expect that. We may find that it is the right way to go. We may find that it is not the right way to go. I am not sure yet.

And so, we are still gathering information. That is why we have been spending a bunch of time talking to folks in the ad and publishing business to understand how it will actually affect them.

The CHAIRMAN. Mr. Mastria, the industry that you represent was obviously not happy about that development. One representative called it a "nuclear first strike." I have heard rumblings that this is the beginning of—this is the phrase that you all use—technological war between your member companies and browser developers like Mozilla.

Will your companies thwart Mozilla's privacy initiative by using other more invasive technologies to collect information on consumers? Second, if companies like Mozilla respond and develop other privacy tools—this is sort of like cyber war—will your companies attempt to get around these tools?

In other words, will your member companies do everything they can at all costs to subvert default privacy protections on Web browsers?

Mr. MASTRIA. Senator, so our members provide transparency and choice as a way to create trust for interest-based advertising. That is what we do. Interest-based advertising is one of the uses that emanates from the use of third-party cookies. There are hundreds of other uses.

There are third-party cookies on and third-party technologies on——

The CHAIRMAN. Are you going to answer my question?

Mr. MASTRIA. Yes. No, our commitment is to provide transparency and choice to consumers, regardless of technology, whether it is cookie based or any other technology that might come along. It is technology neutral.

The CHAIRMAN. So let me ask again. You will—you will——

Mr. MASTRIA. We will continue to provide transparency and choice——

The CHAIRMAN.—to rise above whatever technology he may bring at you. And if he goes up, then you will go up, too.

Mr. MASTRIA. I don't know what he is bringing. He is saying that——

The CHAIRMAN. Neither does he.

Mr. MASTRIA. Yes. So, I mean, you are asking me to speculate. The reality is——

The CHAIRMAN. You are going to win this, right?

Mr. MASTRIA. I am sorry. What?

The CHAIRMAN. You are going to win this. You are going to prevail.

Mr. MASTRIA. We think that transparency and choice, as has been discussed here, is, in fact, the appropriate solution to educate consumers about what is going on online with data. The reality is that third-party cookies are used, as I said, for a whole host of reasons—data protection, security, shopping carts, widgets, et cetera, et cetera. I can go down the line.

The fact that there are many, few, is no indication of anything other than a Website using multiple—multiple third-party services to deliver its content. There are no necessarily nefarious purposes assigned to the cookies simply because they are there. And that is an unfortunate——

The CHAIRMAN. Thank you.

I want to ask Mr. Brookman a question. My time is about to run out.

One of the things that really disturbs me in privacy, or the lack of it, is the way that data brokers can go in and buy all your health records, your financial records—they can get it one way or another—academic record. I mean, all kinds of things, what is of you they can have. And then from that, they—other people make a lot of money out of trying to send them stuff.

Why is it that I find that—and I know lots of people can do that. But we are talking about a very, very large industry here which can decide to do that and which is doing that. Why is that so repulsive to me?

Mr. BROOKMAN. I will speculate——

[Laughter.]

Mr. BROOKMAN.—that it is deemed on sensitive personal information by companies with which you have never heard of and have no relationship and no idea and no control over. Because if you wanted to right now go find out which data brokers are selling data about you, you could assign five interns for it, and you won't be able to do it.

One thing the FTC has actually done—has planned to do, and I think it is a really good idea, is that they are going to try to host a potential repository. So any data broker entity would have to register on the FTC site, and then you can go through and find out what companies are selling about you.

Again, it is going to be voluntary because we don't have privacy law in this country. The rest of the free world has privacy law. The United States and Turkey do not.

I think there should be obligations for companies to tell you what they have about you. And if it is wrong and it can be used for important purposes, I think you should have a right to access and correct it.

The CHAIRMAN. So legislation—I keep getting these little notes. They are not helping me as much as the writers of the notes are. So that is what legislation would do?

Mr. BROOKMAN. Yes. That is one piece of what legislation would do, which is why we spent so much time focusing on behavioral advertising. I mean, there are worse things out there, and it does fly under the radar.

I mean, data brokers have been around for——

The CHAIRMAN. That is the magic, isn't it? Nobody knows it is out there.

Mr. BROOKMAN. Yes. Yes, there is just no way to find out.

The CHAIRMAN. Senator Richard Blumenthal is a distinguished new member of our committee and was, for 28 years, attorney general in Connecticut and has a knack of getting to the point.

Senator Blumenthal?

**STATEMENT OF HON. RICHARD BLUMENTHAL,
U.S. SENATOR FROM CONNECTICUT**

Senator BLUMENTHAL. I am a member of this committee. Thank you, Mr. Chairman.

I don't know about distinguished, but I am a member of this committee who has proudly co-sponsored the bill that you have introduced to establish standards for implementation of the Do-Not-Track mechanism, very simply a mechanism that consumers can trust. And I am disappointed that the self-regulatory agreements that were committed to be done 5 months ago are overdue, and I would like to ask Mr. Mastria how long Congress should wait before moving on this legislation?

We have waited for voluntary agreements. How much longer should we wait?

Mr. MASTRIA. Senator, we are willing to move today. In fact, we are still engaged in the W3C process to move forward. There have been some actions of two browser companies in particular, which have frustrated those efforts, but we continue to abide by the White House agreement that we made in February 2012.

I would also want to go back and touch on the point that the chairman made when he asked about will the advertising industry win? Senator, really, the consumers will win, I think, at the end of the day, because we would give them their preferred user experience—free, ad-supported content with relevant advertising.

And I would submit that they would win partly because the program that we have in place matches very closely to the program that you and Senator Blumenthal are co-sponsoring.

Senator BLUMENTHAL. Let me bring you back to my question, if I may, Mr. Mastria?

Mr. MASTRIA. Sure.

Senator BLUMENTHAL. And I realize that in good faith, maybe you can't answer it. But I am asking you, whatever the reason why the commitment hasn't been met, really can we wait much longer? Isn't it appropriate for Congress to act now, given that, again, for whatever reason the voluntary agreements don't seem to be forthcoming?

Mr. MASTRIA. I think that—I think that we are hopeful that an agreement can be reached.

Senator BLUMENTHAL. How soon?

Mr. MASTRIA. I don't think that I could tell you.

Senator BLUMENTHAL. You don't know.

Mr. MASTRIA. I don't know an exact time.

Senator BLUMENTHAL. That is a fair answer. That is a fair answer.

Mr. MASTRIA. But I would also say, I would color that answer with this does take a little bit of time, and the reality is that we are working at it and that legislative or technological fiats are not necessarily what the Internet needs. It is still growing. It is still evolving.

And we think that a nimble self-regulatory approach, much like ours, which is about to provide guidance in mobile and the app environment, is exactly the kind of thing that helps foster consumer trust while protecting privacy.

Senator BLUMENTHAL. And I would find that answer satisfactory. And I am not challenging the good faith in providing that answer, except we are living in a revolutionary world. We are in the midst of a revolution.

We are debating right now on the floor of the United States Senate the Marketplace Fairness Act, which takes as a given that we have \$150 billion in Internet sales, a number that would have been unimaginable maybe just a year ago. And we all have friends. Some have more friends than others. Many of our friends don't know as much about us as the people who do business on the Internet, about our tastes in music or design or fashion or whatever.

And so, I think consumers have a right to ask whether we can trust the commitments, the commitment that was made months ago as part of the President's program, of whether we can trust that commitment when no one seems to know when the voluntary standards will be completed.

Mr. MASTRIA. We can commit to you that we are continuing to work on it. To put a specific date on it would not be fair. But I can commit to you that we are working on it.

Senator BLUMENTHAL. Is there something that either Congress or the FTC can provide to you that would make those voluntary standards or agreements easier to reach?

Mr. MASTRIA. Yes, well, as I said in my testimony and I think I repeated a number of times, the reality is that there are two browsers that are contravening that agreement right now. So as soon as we can get some agreement around that, then we can move forward much more quickly. But the reality is that we are at the table and willing to move forward.

Senator BLUMENTHAL. And really the only thing that can force compliance is a law, at the end of the day. Isn't that what you are telling this committee?

Mr. MASTRIA. No.

Senator BLUMENTHAL. Well, if those browsers are refusing to abide by voluntary standards or refusing to be part of an agreement, isn't a law necessary? Isn't that sort of the classic—

Mr. MASTRIA. No, we have an agreement, Senator. I mean, we just want them to live up to it. That is it. It is as simple as that.

Senator BLUMENTHAL. Well, when voluntary agreements fail to provide for compliance, it seems to me that is the classic instance, assuming that the public interest is involved, where a law is appropriate.

Mr. MASTRIA. I would submit, Senator, our program today delivers the very mechanisms that you and Chairman Rockefeller have proposed in your bill.

Senator BLUMENTHAL. OK.

The CHAIRMAN. Senator Blumenthal, I would just interrupt to say that what he is talking about, his standards are totally unenforceable, and he knows it.

Senator BLUMENTHAL. Thank you.

Well, Chairman Rockefeller, I think, has made the point more succinctly and clearly than I could. But I think that, unfortunately, is the thrust of what I am hearing at this committee hearing.

Thank you very much, Mr. Chairman.

The CHAIRMAN. You just arrived recently. Do you want to ask another question?

Senator BLUMENTHAL. I am done. Thank you.

The CHAIRMAN. You are done.

Senator BLUMENTHAL. Yes.

The CHAIRMAN. Just done. OK. I am going to close this by going back to what I think, Mr. Anderson, you started with. And that is that in the long run, most things that work in America of a commercial nature or which intersect with people's lives in a personal way—both personal and commercial, therefore—are where things are trusted.

And that the future of the Internet and its various transactions, as it weaves in and out of what it gets to know behaviorally or conceptually about individuals and then uses that so people can go make money off of it, that the American people are smart, and the statistics of the number of people who use the Internet are staggering. The 12 to 17 group is the highest percentage of users, but it is all staggering. It is all 85, 90 percent stuff.

So that all those people who are not aware of the practices of some because it is under the radar are gradually going to become

aware that this is a process. The Internet is very new. As I said before, I am stunned by the fact that, you know, this basically—the Internet went usable generally, what, in the mid 1990s, about then? And since then it has done nothing but grow exponentially.

Then you get Facebook, which actually is interesting because Facebook is all closed off. Nobody can penetrate them. It is rather good, I think. You come up with some ideas. Microsoft comes up with some ideas, actually different from my bill. I am just thinking maybe they are better than my bill.

Because I think that—well, I don't commit myself to anything on that, but it seems to me the more we do to make the consumer's life easier, his right to privacy or her right to privacy easier, whether you opt out, opt in, whether you do it by default, which is what you do, which sort of makes them, allows them to come back and say, "No, no, I want to be able to do this." But it protects them from the beginning.

And as they want not to be protected, they can make those adjustments. That ultimately is the kind of thing which builds the trust, or things of that nature within some radius of what you are talking about are what ultimately build the trust in this country toward the Internet that it is going to need.

Popular as it might be, it is stunning how much harm in real terms through blogging, through bullying, through stuff that leads to suicides and all that. It is commonly talked about now. It was not even a subject, obviously, 10 years ago when I went around West Virginia. It is commonly talked about. I have lots of round-table and town meetings on that.

So the American people are smart. They are going to figure this out. And as they figure it out, they better like what they see if the Internet wants to prosper.

And with that, the hearing is adjourned.

[Whereupon, at 4:19 p.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO HARVEY ANDERSON

Question 1. Do you believe that the DAA's self-regulatory program and choice mechanism, in their current form, are sufficient for consumers? Why or why not?

Answer. No, we do not believe the DAA's program in its current form is sufficient for consumers. As we outlined in our written testimony, the efficacy of the Digital Advertising Alliance (DAA) Ad Choices program remains an open question. Last year, according to one study, the number of users who viewed the icon was low: 0.0035 percent of users clicked on the icon, and only 1 in 20 of those actually opted out. The DAA itself reported that more than a trillion ads per month include the Ad Choices icon—a blue triangular icon that when clicked, takes consumers to a page where they can learn about the ad, and opt out of receiving it. Only five million users have accessed the choice tool, and reportedly a total of two million of those have opted out of all interest-based advertising since the program began. Over a three-month period this equates to an effective rate less than .0000006 percent.

This low opt-out rate seems inconsistent with the 11 percent of Firefox users who have turned on Do Not Track without prompting or any conspicuous visual clues in the Firefox user interface (see <https://dnt-dashboard.mozilla.org/>). The argument that the current low participation rate means that consumers are “OK” with the current tracking and collection practices is contradicted by the ample survey research indicating otherwise.

The user experience for the opt-out and the user education could be substantially improved. The icon could be more visible, contain less text, and require fewer clicks—it could be more user-friendly. Still, even though we believe improvement is warranted, we recognize that the DAA scheme represents significant effort, coordination, and investment that overtime can improve through iteration and feedback.

Question 2. Can the DAA's existing self-regulatory scheme be narrowed or changed in some way as to place reasonable, meaningful limits on the collection of consumer's information? How?

Answer. Mozilla only has access to the information that is publicly available concerning the DAA's program and, beyond our comments above, we do not have sufficient information to provide a detailed response to this question.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BARBARA BOXER TO HARVEY ANDERSON

Question 1. How do Firefox users find out about the Do Not Track feature?

Answer. Currently, we believe most Firefox users find out about the Do Not Track feature by exploring the Firefox preferences. Users may also learn about the feature through popular media, which has widely covered development of the feature, and from consumer advocacy groups. We have also provided users with some information about Do Not Track through our own blogs, marketing materials and support pages.

To enable Do Not Track in Firefox, a user must first select “Preferences” in the menu options, and then select the “Privacy” menu shown below to enable Do Not Track.



We do not promote the feature in the product or provide the user with visual prompts in the main user interface. This is primarily because Do Not Track is still under development and we need widespread industry adoption of the system and the signals for it to provide meaningful choice and control to users.

Question 2. To what do you attribute the growth in the number of Firefox users who have turned enabled Do Not Track?

Answer. We attribute the growth in the number of Firefox users who have enabled Do Not Track to a broad user sentiment that they want more control in their digital transactions. There are very few easy options available, and users perceive they are tracked across their web browsing activities and don't understand how/whether they receive benefits or direct value from this tracking. Those users who don't want this to occur or don't understand what's happening with their data set their browsers to tell sites "not to track" them. We expect that adoption will stabilize over time and we don't necessarily believe the growth rates will organically continue if adoption remains consistent with historical patterns. We also believe that the adoption rate may be affected by how well industry recipients respect Do Not Track signals.

Question 3. Why did Mozilla make the decision to block third-party cookies by default?

Answer. We continue to evaluate the "third party cookie patch" that is currently available in the Aurora build (a special testing build used by a small number of users) for Firefox. This patch would create a default setting that blocks third party cookies. Our primary motivation for considering the patch is to make enhancements to cookie policies that will help to create the Web experience users expect. The current feature set matches Apple Safari's third party cookie policy. We are still gathering feedback on the current proposal and iterating on other ideas and potential modifications. The new default cookie policy will remain in our test builds of Firefox until evaluation and development is complete.

Question 4. How do the expectations of Firefox users differ with respect to first-party and third-party cookies?

Answer. We believe that Firefox users are more likely to expect tracking and collection from parties with whom they have intentionally engaged. This is because users have a better understanding of the value proposition and the benefits to them. This is often called a first-party. For example, when you log into Amazon, users expect the service to remember your name, past history, and to offer experiences based on information they have collected about you through your interactions with the service. Conversely, users don't generally expect that parties with whom they do not have a relationship to collect or track information about them. The converse is also not necessarily true, all first parties are not necessarily "good" and all third parties are not necessarily "bad" or surprising to users. For example, some websites engage third parties by contract restricting their collection and tracking practices, others use third parties for analytics in ways that would be perfectly acceptable to users, and even other third parties operate and comply with the laws of the relevant jurisdictions with strict regulatory prohibitions on profiling without user consent.

Question 5. How does blocking third-party cookies change a user's browsing experience?

Answer. Through our testing we continue to learn more about what happens when third party cookies are blocked, but we our review process is still ongoing. For the most part, blocking third party cookies will have little overall impact to a user's browsing experience. Users will still be able to consume content from those websites that have enabled third party cookies even though those cookies cannot be read—ads will continue to be displayed, but the user may not be shown targeted ads based on cookie data. It's also possible that a site may prevent a user from accessing some content or services without enabling the use of third party cookies for that site. It is worth pointing out that in mobile web browsing, fewer sites and apps rely on third party cookies, so disabling third party cookies by a mobile OS provider has even less impact on a user's browsing experience.

Question 6. How have users, advertisers, and other stakeholders responded to Mozilla's announcement regarding its new third-party cookie policy?

Answer. The response to the proposal has differed widely depending on the respondent's role in the digital ecosystem. Users have largely been silent (maybe because the change and impact is not well understood outside of the ecosystem), yet comments posted to various social sites and media outlets demonstrate strong support coming from some segments of our user base. Publishers have expressed concerns about frequency capping and conversion management, functionality offered by cookies. Ad tech entities that don't have a direct relationship with the user or who provide re-targeting services have articulated concern that this may directly impact

their current businesses. Some stakeholders in the ad tech industry have expressed concern that the proposed change gives first parties an unfair advantage that may make their inventory more valuable over time. The brands have not articulated specific concerns, but generally tell us they don't want to be associated with non-transparent practices and are concerned about the extent to which third parties are tracking users outside their stated privacy policies. Consumer groups have been very supportive of the proposed change because it increases transparency and user control, reduces emergence of data inequalities, and the sale of secondary purposes outside of the user's control and benefit.

There also seems to be a general sentiment among stakeholders that the current practices of using cookies for collection and tracking are not long lived and new technological approaches are on the horizon. Thus, while stakeholders we've met with know change is inevitable with regard to cookies, there is inherent resistance until a better alternative is available.

Question 7. Do you anticipate other browser companies following suit in blocking third-party cookies by default?

Answer. Apple's Safari browser already has implemented a third party cookie policy that blocks most third party cookies by default, including on its iOS platform devices like iPhones and iPads. We are unable to predict what Google and Microsoft will do relative to third party cookies.

Question 8. How prevalent is the use of digital fingerprinting and other non-cookie tracking among websites encountered by Firefox users?

Answer. We know various forms of digital fingerprinting are in practice today, however, we do not have sufficient information to quantify the extent of the current practices.

Question 9. What does Mozilla do to address the use of these alternative tracking methods?

Answer. Our primary proposal to address all forms of tracking has been our work on Do Not Track. We still believe a simple, user-enabled Do Not Track signal is the best method for providing users and sites a simple, persistent, automated and effective signal to opt-out of tracking regardless of whether a site or app is using cookies, unique IDs, fingerprinting or other tracking methods. We also are continuing to work to minimize the Firefox user agent string fingerprint where possible.

Question 10. What role do alternative tracking methods play in the ongoing World Wide Web Consortium discussions regarding a Do Not Track standard?

Answer. To date, the scope of the W3C discussions have been focused on a Do Not Track signal that would be technology-agnostic on the form of tracking method being deployed by a third party. Barring some change in the coming weeks, the W3C specification would apply to any type of third party tracking.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO HARVEY ANDERSON

Question 1. A 2010 *Wall Street Journal* series on online privacy illustrated the extent to which individuals are being tracked and how the invasive practice can cause real harm. A recent high-school graduate, who had been identified by advertisers as concerned about her weight, told the paper she sees weight-loss ads every time she goes on the Internet. She said, "I'm self-conscious about my weight. I try not to think about it . . . then [the ads] make me start thinking about it." Do you believe this qualifies as a real harm?

Answer. We cannot judge how the ad placements may have impacted the individual interviewed in the *WSJ* series. Traditionally, legal harm that results in remedies and legislative action requires a cognizable and quantifiable loss or injury. The *WSJ* series demonstrates the real need for education, transparency and greater trust in advertising data practices.

Question 2. Many believe the lack of transparency—particularly with regard to 3rd party cookies—and an individual's inability to know what personal information is actually being collected can cause real harm because consumers don't have the ability to understand how to protect themselves from invasive tracking. Do you agree that this is a harm?

Answer. Harms in this case are difficult to quantify in a traditional sense because the real harm is a lost opportunity to accelerate commerce and more meaningful digital transactions. As stated in our written testimony before this Committee, we believe that more education, greater transparency and direct control around these advertising practices creates trust and demonstrates value to the user which would ultimately create a better, stronger ecosystem:

"If users do not understand what happens to their data, how it is used, or the trade-offs, they will inevitably seek more protective blocking options. Conversely, we may see the adoption of more invasive and even less transparent tracking methods. The impact is that efforts to protect the status quo further erode people's trust in the ecosystem, thereby compromising future expansion of commerce and innovative growth of this ecosystem. Personalized content is good, however, the collective challenge we face is how to deliver that content transparently.

The future of a viable, innovative Web that continues to contribute jobs and drive social, educational and economic activity depends on consumer trust. To develop this trust, transparency, choice and control are essential. Real transparency of business and data sharing practices combined with meaningful user choice will engender the confidence users expect."

Question 3. Do you believe that consumers have a basic right to privacy online?

Answer. Certainly some states like California, and many countries around the world, have provided constitutional protections for privacy. To the extent these rights extend to digital environments, we act consistently with the applicable law. We also believe users have a right to make choices—that don't punish them—about their information, habits, relationships, interests, activities, and preferences. This value is reflected in our product design in ways that users efficiently and easily navigate the web.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. AMY KLOBUCHAR TO
HARVEY ANDERSON

Question. It now appears that Mozilla, Apple, and Microsoft are competing on consumer privacy. Both the FTC and White House reports on privacy released last year mention the possibility of privacy practices, including online tracking options, becoming a consideration for consumers deciding between devices and services. Have you seen data suggesting consumers already chose services, particularly online, based on privacy practices? Is this impacting the competition between browsers and services?

Answer. Privacy practices by the major browser providers are emerging as a major factor but do not appear to be the driving factor in product selection. In most markets, privacy is important as a feature area for browsers, but our research indicates that it still ranks behind other factors like performance, stability and security.

Part of the challenge for browsers is that privacy is not a mature area of feature development. Most of the privacy tools and settings available in browsers are still in early phases of development and generally are not used by the mainstream user. If more browser technology existed that was privacy forward, intuitive, and added value to a user's online experience, more users would seek it out and avail themselves of it.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BRIAN SCHATZ TO
HARVEY ANDERSON

Question. I agree with the point that you made in your testimony that it is important to protect the trust of consumers. I am concerned that, right now, consumers lack even the most basic tools to understand, let alone trust, the information collecting activities of advertisers on the websites they visit. When a consumer is browsing on the internet, is there any way for that consumer to know on any given website (1) who is collecting information about that person, (2) for what purpose that data is being used, and (3) who else might have access to that data?

Answer. For over a decade, the primary basis for consumers to learn about any given site's data handling practices has been its posted privacy policy. Numerous studies have been done over the years showing that the vast majority of top commercial websites have privacy policies (see TRUSTe Privacy Index 2011; <http://tctechcrunch2011.files.wordpress.com/2011/11/truste-privacy-index-2011-websites.pdf>). Some state governments, such as California, have legislated that websites are required to post a policy that covers the three points you outlined in your question. The Federal Trade Commission has also brought a number of deceptive/unfair practice actions against sites that have wavered from stated data practices.

While there is research showing that consumers don't regularly read or make sense of these policies, privacy policies are noteworthy sign posts used to provide information about sites' data practices (see "The Cost of Reading Privacy Policies," A. McDonald & L. Faith Cranor, *I/S: A Journal Of Law And Policy For The Infor-*

mation Society, 2012; http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf).

As it relates to third party tracking, the current paradigm of relying on posted privacy policies creates challenges as it becomes more difficult to describe in detail within these policies how consumer websites employ third party services, widgets and advertising. Moreover, because of the need for more transparency about the current practices in the digital ad tech sector, consumer expectations of what is occurring on these websites are not being matched.

One of our stated objectives in developing a Do Not Track specification is to help evolve the notice and choice model to one where a user states his/her preference and the website is able to communicate back its relevant tracking practices all without the consumer needing to read the privacy policy.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. RON JOHNSON TO
HARVEY ANDERSON

Question. What are the harms that are actually occurring to consumers through anonymous cookie-based “tracking?” As indicated in Mr. Mastria’s testimony, the primary privacy concerns for most consumers online have to do with identity theft, viruses and malware, and government surveillance. So, what harms are occurring that the FTC doesn’t currently already have the authority to address?

Answer. The question of harms associated with online tracking is a complicated one to answer, as we stated above in our responses to Senator Lautenberg. We need to look beyond legal distinctions or classes of harms to look at the erosion of trust in the ecosystem resulting from non-transparent tracking of consumers online. Mr. Mastria’s testimony points to some of the privacy concerns of consumers today. However, we know consumers care about intrusions into their private lives, not just from hackers or governmental entities, but also from commercial entities.

To consumers, many types of personal information can be important to them, including elements that are uniquely identifiable or not, including de-identified data, that might be characterized as “anonymous” meaning not including a person’s name or SSN, for example.

Meaningful distinctions between personally identifiable information (PII) and non-PII are breaking down.

To a certain extent, much of the data collected from or about a consumer online could be reasonably considered “personal” by that person. In the context of cookies, calling data associated with a cookie “anonymous” because it doesn’t include a person’s name, home address or other PII doesn’t mean that there aren’t privacy considerations. Whether data is uniquely identifiable or becomes subsequently identifiable in combination with other data, or whether future, novel uses of that data create new contexts with privacy properties, people can have legitimate interests in wanting to understand and have a say in a company’s data handling practices. For example, a database generated by a third party company in the ad ecosystem that is able to associate a consumer’s online browsing history down to a specific product, interest or purchasing intent and then for that data to cross multiple companies’ systems to use that data across the web to personalize display ads, content or recommendations can feel personal to that user despite not including any PII.

On a technical level, there are many, real world examples of so-called anonymous data being later re-identified. In 2006, AOL released a large data set for research purposes of 650,000 users’ search queries that it anonymized before posting online. Using a phone book listing, *The New York Times* was able to identify individuals from the data. Since then, a number of researchers have demonstrated that by combining datasets from public sources with anonymized datasets, it is possible to re-identify actual individuals sometimes to dramatic effect in some cases where the once-anonymized dataset includes financial or health related data.

We shouldn’t accept comments made by those trying to minimize concerns associated with anonymized datasets about users’ online activities, purchases, communications and relationships because the business interest is only to personalize a display advertisement today. We have to think more broadly about the future of this data once its collected, whether it might be compromised by a hacker, resold to other businesses whose practices may not always be in the consumer’s interest (*e.g.*, employment decisions) or swept up in a government subpoena. We believe all players in the industry need to recognize the long-term ramifications and implications of any data being collected online and establish best practices and technical measures to provide users greater transparency, choice and control.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV
TO LUIGI MASTRIA

Question 1. Much of the hearing focused on the DAA's promises at the February 2012 White House event to honor Do-Not-Track browser-based header signals. In your testimony, you stated that the DAA committed to honor a Do-Not-Track header "where a consumer (1) has been provided language that describes to consumers the effect of exercising such choice including that some data may still be collected and (2) has affirmatively chosen to exercise a uniform choice with the browser based tool. The DAA standard will not apply in instances where (1) and (2) do not occur or where any entity or software or technology provider other than the user exercises such a choice." Some browsers, such as Google's Chrome, appear to currently meet these requirements, yet few DAA members honor such Do-Not-Track signals. Why do your members not currently honor Do-Not-Track header signals that meet the very standards you outlined in your testimony?

Answer. The DAA administers a comprehensive program of industry self-regulation for the collection and use of web viewing data that provides enhanced consumer transparency and control. The DAA's Principles call on companies to provide consumers with choice with respect to the collection and use of web viewing data. To help companies implement the Principle of Consumer Control, the DAA developed, implemented, and maintains a consumer choice page through which consumers can set their preferences. Since the program's launch, eight million users visited this choice page with more than two million exercising their choice. This tool provides meaningful and effective choice in the marketplace.

The DAA seeks to develop universal standards that deliver a consistent user experience. For instance, DAA developed principles for transparency that enumerates the elements of notice and the means by which such notice is provided. Specifically, DAA calls on companies to provide transparency outside the privacy policy via the DAA Icon. With each icon served—at a rate of more than one trillion ad impressions per month across the Internet—consumers can link to notice concerning a company's data practices and access a choice mechanism. This approach provides a consistent user experience for consumers; *i.e.*, when a consumer clicks on the Icon, the consumer can expect a certain result—notice of data practices and access to a choice tool.

The DAA seeks similar consistency for consumers with respect to browser-based choice mechanisms.

In February 2012, the DAA announced an agreement to honor the DAA Principles through a browser signal when consumers both (1) receive meaningful information about the effect of that choice, and (2) affirmatively makes that choice themselves. The DAA standard will not apply in instances where (1) and (2) do not occur or where any entity or software or technology provider other than the user exercises such a choice.

Unfortunately, this agreement has been short-circuited due to contrary approaches taken by Microsoft and Mozilla. Microsoft subsequently released its new version of IE 10 with "do not track" turned "on" as a default setting, in direct conflict with the agreement they helped develop with the White House.

Mozilla has implemented what it refers to as a "do not track" tool in the current Firefox release also without following the White House agreement, for example by not describing for consumer the impact of their choice and creating inaccurate consumer expectations. Mozilla's interface permits users to check a box to "Tell websites I do not want to be tracked." Nothing more is provided to users; for example, consumers are not told that, by exercising such choice some data may still be collected. This implementation conflicts with the workable standard developed through industry consensus in 2012 and does not provide consumers with clear information about the effect of their choices.

Until there is a universal meaning and implementation consistent with the Agreement at the White House across all browsers, DAA will continue to call for companies to provide choice via DAA's effective choice tools and not require companies to adhere to tools that promote confusion for consumers and do not meet the DAA's consensus standard for consumer control.

Question 2. I am very concerned that in the absence of a comprehensive Do-Not-Track agreement, your member companies will respond to default consumer privacy measures recently considered by Mozilla, the nonprofit organization behind the popular Web browser Firefox, and other browser developers. I worry that such a game of one-upmanship could have a detrimental impact on how consumers experience the Internet. Will your members thwart default settings that block third-party cookies by using other, more invasive technologies—such as browser fingerprinting—to collect information from consumers?

Answer. The DAA's Principles and Program are technology neutral. The DAA's Principles consist of seven principles: education, transparency, consumer control, data security, controls with respect to material changes to policies and practices, heightened safeguards for sensitive data, and accountability. The principles set standards designed to provide a consistent user experience. The DAA does not mandate the use of specific technologies by companies in satisfying these Principles or in delivering their services, but instead calls for companies to provide transparency and control with respect to their practices.

Question 3. If browser companies like Mozilla respond and develop other privacy tools for consumers that actively prevent the collection of information, will your members attempt to get around those tools and subvert default privacy protections on Web browsers?

Answer. It is my understanding that Mozilla has chosen to delay its plans to block third-party cookies to reassess the impact blocking would have on the Internet ecosystem. Cookie blocking does not advance consumer choice and would have a significant adverse effect on users' Internet experience.

Cookies set by third parties play a vital role in the Internet ecosystem by facilitating consumer access to content and services. Blocking of third-party cookies would disrupt consumers' online experience on the websites they use by reducing content personalization and the relevancy of advertising they receive—and these moves could even impact shopping cart and other similar third-party operational functionality. This change would harm all Internet content and services that use third party technologies to understand and protect their audiences. In particular, it would disproportionately harm the numerous small publishers that are often completely reliant on these technologies to operate and monetize their sites, thereby thwarting new job creation and chilling innovation.

The DAA will monitor changes in the marketplace and evaluate the impact of this type of unilateral decision on the Internet and advertising ecosystem. The online advertising industry is a beacon for innovation and job creation. In 2012, Internet advertising revenues reached a new high of \$36.6 billion, an impressive 15 percent higher than 2011's full-year number.¹ Because of this advertising support, small and medium-size publishers can provide consumers with access to a wealth of online resources at low or no cost. This model delights consumers and creates jobs across America, fostering a competitive marketplace that drives down prices for consumers and costs for businesses. A 2009 study found that more than three million Americans in every U.S. state are employed due to the advertising-supported Internet, contributing an estimated \$300 billion, or approximately 2 percent, to our country's GDP.² There is employment generated by this Internet activity in every single congressional district in every state across the United States.³

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BARBARA BOXER TO
LUIGI MASTRI

Question 1. The Digital Advertising Alliance (DAA) created the AdChoices icon to provide users notice and an opportunity to opt out of behavioral advertisements. In his written testimony, Mr. Anderson cited a study from Carnegie Mellon University that found that 0.0035 percent of users clicked on the AdChoices icon when presented with it and only 1 in 20 of these users proceeded to opt out. Would you say that the implementation of the AdChoices icon has been successful?

Answer. Yes. The DAA program developed a universal icon to give consumers transparency and control for interest-based ads. The icon provides consumers with notice that information about their online interests is being gathered to customize the web ads they see. Clicking the icon also allows consumers to choose whether to continue to allow this type of advertising.

The icon is served more than one trillion times each month on or next to Internet display ads on websites. The DAA reached this milestone within a short 18 months from program launch. This achievement represents an unprecedented level of industry cooperation and adoption.

¹Interactive Advertising Bureau Press Release, "Internet Ad Revenues Again Hit Record-Breaking Double-Digit Annual Growth, Reaching Nearly \$37 Billion, a 15 percent Increase Over 2011's Landmark Numbers" (April 16, 2013) (reporting results of PricewaterhouseCoopers study).

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

³*Id.* at 53.

The icon serves as the main gateway to the DAA's choice page. With the rise in the number of icons displayed, visitors to the DAA choice page have also increased. In 2012, more than 5.2 million unique users accessed the resources provided at www.aboutads.info, which is more than three times the 2011 figure. Overall, since program launch, more than 8 million visitors have accessed the DAA program opt-out tool, and more than 2 million unique users have exercised choice.

Question 2. How does the DAA measure the effectiveness of the AdChoices icon as a public education and user empowerment tool?

Answer. The DAA is deeply committed to consumer education. In 2012, the DAA launched a dedicated educational site at www.YourAdChoices.com. The site provides easy-to-understand messaging and informative videos explaining the choices available to consumers, the meaning of the DAA Icon, and the benefits they derive from online advertising.

In 2012, companies participating in the DAA program voluntarily donated more than four billion impressions to support an educational campaign for www.YourAdChoices.com.

Since the campaign launched in late January 2012, more than 13.5 million unique users have visited this educational site. This site also provides access to the DAA's user choice mechanism. The combination of the educational campaign and the ubiquitous availability of the DAA Icon have significantly increased consumer usage of the DAA program tools.

In 2012, more than 5.2 million unique users accessed the resources provided at www.aboutads.info. Of those visitors, nearly one million unique users exercised choice using the integrated opt out mechanism provided at that site; moreover, a total of two million unique visitors have now exercised opt out choices since the program launch. Many users visit the website, learn about their choices, and ultimately choose not to opt out. We believe that this shows that once consumers understand how online advertising works, many prefer to receive relevant ads over irrelevant ads. Research supports this proposition. A recent poll of U.S. consumers shows that 68 percent of Americans prefer to get at least some Internet ads directed at their interests and included in this total are 40 percent of Americans who prefer to get all their ads directed to their interests.⁴

Question 3. Mr. Brookman writes in his testimony that the DAA AdChoices program is almost entirely cookie-based. In other words, when a user deletes her cookies, she likely also deactivates her preference to opt out of tracking by DAA members. Is it true that a user's preference not to be tracked disappears when she deletes her cookies?

Answer. No. More than a year ago, the DAA developed, at great expense, a suite of browser plug-ins to make consumer choices persistent. Through these "hardened" opt-outs, a consumer's preferences will remain active even if she deletes her cookies.

Question 4. Is the DAA taking steps to create a more persistent opt-out mechanism?

Answer. The DAA currently provides consumers with persistent opt-out mechanisms.

Question 5. Mr. Brookman also claims in his testimony that opting out through the AdChoices program prevents only the display of targeted advertising to a user and not the tracking itself. Are DAA members permitted to track users who have opted out through the AdChoices mechanism as long as they do not display targeted advertisements to those users?

Answer. The DAA's Principles cover both the collection and use of web viewing data for purposes including, but not limited to, interest-based advertising. Where a consumer has exercised choice under the DAA Program, companies should stop the collection and use of data from the computer or device for any purpose except collection and use for narrow purposes specified in our Principles and described in our next response.

Question 6. If so, how may DAA members use the tracking data they collect from users who have expressed a preference to opt out from behavioral advertising, and how are these data used in practice?

Answer. In November 2011, the DAA extended its Principles beyond advertising to cover the collection and use of all Multi-Site Data except collection for narrow purposes including operational and system management purposes, fraud prevention and security, content delivery, market research, and product development, and data that has been de-identified. Some collection of data is vital to workings of the Inter-

⁴Interactive Survey of U.S. Adults commissioned by the DAA (April 2013), available at <http://www.aboutads.info/DAA-Zogby-Poll>.

net ecosystem, and limiting collection of this data would result in a reduced online experience for consumers.

Significantly, the DAA Multi-Site Data Principles prohibit the use of Web viewing data for employment eligibility, credit eligibility, healthcare treatment eligibility, and insurance eligibility and underwriting and pricing.

Question 7. In February 2012, the DAA announced plans to implement, within nine months, policy changes that would respect users' tracking preferences as expressed through browser header signals. Why has the DAA not implemented these policy changes?

Answer. For more than two years, the DAA has been offering an effective, one-button choice mechanism that empowers consumers to stop the collection of web viewing data by third parties. At a highly-publicized White House event last year, the DAA announced an agreement to honor the DAA Principles through a browser signal when consumers both (1) receive meaningful information about the effect of that choice, and (2) affirmatively makes that choice themselves. It was agreed that the DAA standard would not apply in instances where (1) and (2) do not occur or where any entity or software or technology provider other than the user exercises such a choice.⁵

Unfortunately, the White House agreement was short-circuited due to contrary approaches taken by Microsoft and Mozilla.

Microsoft subsequently released its new version of IE 10 with "do not track" turned "on" as a default setting, in direct conflict with the agreement they helped develop with the White House.

Mozilla has implemented what it refers to as a "do not track" tool in the current Firefox release also without following the White House agreement, for example by not describing for consumer the impact of their choice and creating inaccurate consumer expectations. Mozilla's interface permits users to check a box to "Tell websites I do not want to be tracked." Nothing more is provided to users; for example, consumers are not told that, by exercising such choice some data may still be collected. This implementation conflicts with the workable standard developed through industry consensus in 2012 and does not provide consumers with clear information about the effect of their choices.

Question 8. Are DAA members currently acknowledging browser-based signals from users?

Answer. The DAA's Principles call on companies to provide consumer with choice with respect to the collection and use of web viewing data. To help companies implement the Principle of Control, the DAA developed, implemented, and maintains a consumer choice page through which consumers can set their preferences.

Until there is a universal meaning and implementation consistent with the Agreement at the White House across all browsers, DAA will continue to call for companies to provide choice via DAA's effective choice tools and not require companies to adhere to tools that that promote confusion for consumers and do not meet the DAA's consensus standard for consumer control.

Question 9. If not, what prevents them from doing so?

Answer. The DAA seeks to develop universal standards that deliver a consistent user experience. Unfortunately, Microsoft and Mozilla implemented browser based choice mechanisms in ways that are inconsistent with the consensus achieved with the White House, Federal Trade Commission, the Department of Commerce, and the browser community.

Until there is a universal meaning and implementation consistent with the Agreement at the White House, DAA will continue promote its current, effective choice tools and not require companies to adhere to tools that do not meet the DAA's consensus standard for consumer control.

⁵DAA Position on Browser Based Choice Mechanism, available at https://www.aboutads.info/resource/download/DAA_Commitment.pdf.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RON JOHNSON TO
LUIGI MASTRIA

Question 1. What are the harms that are actually occurring to consumers through anonymous cookie-based “tracking?” As indicated in Mr. Mastria’s testimony, the primary privacy concerns for most consumers online have to do with identity theft, viruses and malware, and government surveillance. So, what harms are occurring that the FTC doesn’t currently already have the authority to address?

Answer. I am unaware of any consumer harm caused by the use of cookies to associate online data across sites and over time or any empirical evidence to support the idea that consumers are harmed from the collection and disclosure of this anonymized, aggregate data. Despite this lack of evidence of concrete harms, DAA-participating companies recognize that consumers have different preferences about online advertising and data collection. To continue to build consumer trust in the online experience, the DAA has developed principles that help ensure consumers have meaningful choices about how data is collected and used. For those consumers that do not want information collected via cookies, they may elect to opt out via a simple, easy-to-use choice mechanism available at www.aboutads.info/choices.

Cookies are a well-established and very transparent technology that benefits consumers in many ways, such as by facilitating the delivery of rich content, products, relevant content and advertising, and security and fraud prevention services.

Cookies are also used to enable online advertising, which fuels the Internet economic engine. The online advertising industry is a beacon for innovation and job creation. In 2012, Internet advertising revenues reached a new high of \$36.6 billion, an impressive 15 percent higher than 2011’s full-year number.¹ Because of this advertising support, small and medium-size publishers can provide consumers with access to a wealth of online resources at low or no cost. Revenue from online advertising facilitates e-commerce and subsidizes the cost of content and services that consumers value, such as online newspapers, weather, Do-It-Yourself websites, blogs, social networking sites, mobile applications, e-mail, and phone services. According to a recent poll by Zogby Analytics, 92 percent of Americans think free content like news, weather and blogs is important to the overall value of the Internet.²

This cookie-based model delights consumers and creates jobs across America, fostering a competitive marketplace that drives down prices for consumers and costs for businesses. The Internet has become the focus and a symbol of the United States’ famed innovation, ingenuity, inventiveness, and entrepreneurial spirit, as well as the venture funding that flows from these enormously productive and positive efforts. A 2009 study found that more than three million Americans are employed due to the advertising-supported Internet, contributing an estimated \$300 billion, or approximately 2 percent, to our country’s GDP.³ There is employment generated by this Internet activity in every single congressional district across the United States.⁴

To help preserve this vibrant ecosystem, the DAA developed the Multi-Site Data Principles (“MSD Principles”) to provide consumers with control with respect to their Web viewing data used for advertising and *non-advertising* purposes while preserving commonly-recognized uses of data, including for operational purposes such as fraud prevention, intellectual property protection, compliance with law, authentication and verification purposes, billing, and product or service fulfillment. The MSD Principles also permit the use of data that has gone or will within a reasonable period of time from collection go through a de-identification process, or that is used for market research or product development. This approach helps ensure the continued flow of data that is vital to the workings of the Internet, to the consumer online experience, and for building tomorrow’s Internet.

I have included a recent Zogby poll, which illustrates concrete concerns among consumers. Specifically, Americans’ privacy concerns are focused on real threats like identity theft, virus, malware, and cyber-bullying (see attached survey results). These harms are not caused by anonymous, cookie-based data collection.

¹ Interactive Advertising Bureau Press Release, “Internet Ad Revenues Again Hit Record-Breaking Double-Digit Annual Growth, Reaching Nearly \$37 Billion, a 15 percent Increase Over 2011’s Landmark Numbers” (April 16, 2013) (reporting results of PricewaterhouseCoopers study).

² Interactive Survey of U.S. Adults commissioned by the DAA (April 2013), available at http://www.aboutads.info/resource/image/Poll/Zogby_DAA_Poll.pdf.

³ Hamilton Consultants, Inc. with Professors John Deighton and John Quelch, *Economic Value of the Advertising-Supported Internet Ecosystem*, at 4 (June 10, 2009), available at <http://www.iab.net/media/file/Economic-Value-Report.pdf>.

⁴Id. at 53.

Question 2. Response to Written Questions Submitted by Hon. to Mr. Anderson points out in his testimony that the digital advertising business has grown, reaching a record breaking \$36.6 billion in 2012. As he puts it, “there is real money at stake.” Can you comment on the impact that government mandates, such as those proposed in several privacy bills, may have on your industry and the jobs that digital advertising supports?

Answer. Government mandates and regulation, particularly in such a rapidly-developing area as the digital space, can stifle innovation, reduce competition, slow job growth, and add unnecessary costs. In a congressional hearing on “Internet Privacy: The Impact and Burden of EU Regulation,” Professor Catherine Tucker of the MIT Sloan School of Management testified about the effect on advertising performance of the European Union’s e-Privacy Directive, which limits the ability of companies to collect and use behavioral data to deliver relevant advertising.⁵

Professor Tucker’s research study found that the e-Privacy Directive—government mandates impacting the digital advertising ecosystem—was associated with a 65 percent drop in advertising performance, measured as the percent of people expressing interest in purchasing an advertised product.⁶ The study also found that the adverse effect of such regulation was greatest for websites with content that did not relate obviously to any commercial product, such as general news websites. Professor Tucker cautions: “on the basis of this evidence, it is reasonable to say that privacy regulation could have sizable effects for the advertising-supported internet.”⁷ Professor Tucker advises that “policymaking in the area of privacy regulation needs to be careful and fulfill the twin aims of protecting consumer privacy and ensuring that the advertising-supported Internet continues to thrive.”⁸

As noted above, in 2012, Internet advertising revenues reached a new high of \$36.6 billion, an impressive 15 percent higher than 2011’s full-year number.⁹ In addition, a 2009 study found that more than three million Americans across the United States are employed due to the advertising-supported Internet, contributing an estimated \$300 billion, or approximately 2 percent, to our country’s GDP.¹⁰ We remain concerned that laws and regulations are inflexible and can quickly become outdated in the face of extraordinarily rapidly-evolving technologies. When this occurs, legislation thwarts innovation and hinders economic growth and can impede a competitive marketplace that offers a full range of choice to consumers. We believe that our commitment to and success in advancing industry self-regulation is the most efficient and effective way to balance consumers’ interests in privacy and innovation.

⁵*Empirical Research on the Economic Effects of Privacy Regulation*, Catherine Tucker (November 8, 2011), available at http://cetucker.scripts.mit.edu/docs/law_summary_2011.pdf.

⁶*Id.* at 5.

⁷*Id.* at 2.

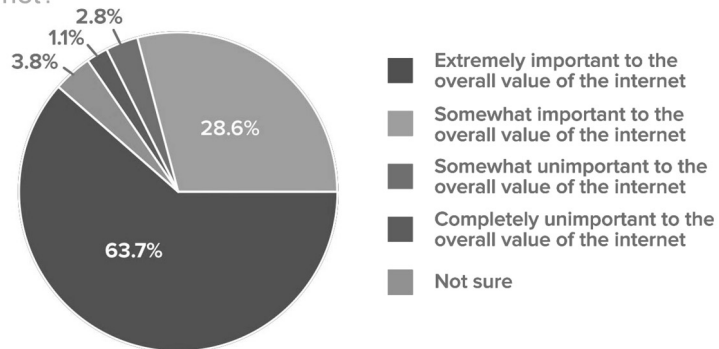
⁸*Id.* at 3.

⁹Interactive Advertising Bureau Press Release, “Internet Ad Revenues Again Hit Record-Breaking Double-Digit Annual Growth, Reaching Nearly \$37 Billion, a 15 percent Increase Over 2011’s Landmark Numbers” (April 16, 2013) (reporting results of PricewaterhouseCoopers study).

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

Interactive Survey of US Adults (April 2013)

In your opinion, how important is free content like news, weather, email, blogs and videos to the overall value to the Internet?

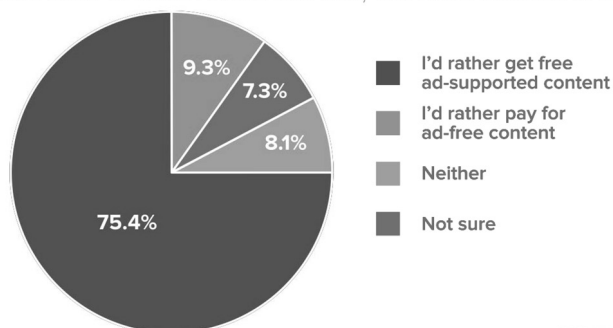


Margin of Error +/- 3.2 percentage points. Subsets have a larger margin of error than the whole data set. As a rule we do not rely on the validity of very small subsets of the data, especially sets smaller than 50-75 respondents. At that size subset we can make generalizations, but in these cases the data is more qualitative than quantitative.

Zogby
Analytics

Interactive Survey of US Adults (April 2013)

Which of the following would you prefer: an Internet where there are no ads, but you would pay for most content like blogs, entertainment sites, video content and social media, or today's Internet model in which there are ads, but most content is free?

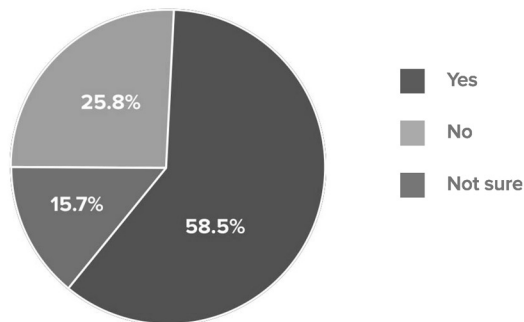


Margin of Error +/- 3.2 percentage points. Subsets have a larger margin of error than the whole data set. As a rule we do not rely on the validity of very small subsets of the data, especially sets smaller than 50-75 respondents. At that size subset we can make generalizations, but in these cases the data is more qualitative than quantitative.

Zogby
Analytics

Interactive Survey of US Adults (April 2013)

Has an Internet ad ever helped you find an offer or product that you wouldn't otherwise have known about?

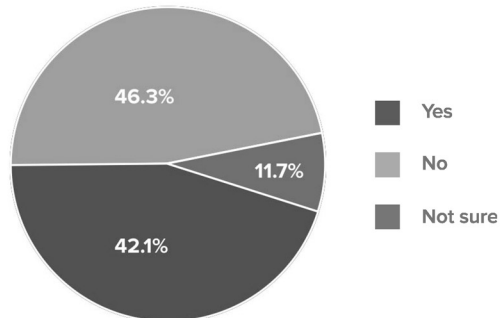


Margin of Error +/- 3.2 percentage points. Subsets have a larger margin of error than the whole data set. As a rule we do not rely on the validity of very small subsets of the data, especially sets smaller than 50-75 respondents. At that size subset we can make generalizations, but in these cases the data is more qualitative than quantitative.

Zogby
Analytics

Interactive Survey of US Adults (April 2013)

Have you ever purchased a product or service because you saw or clicked on an online advertisement?

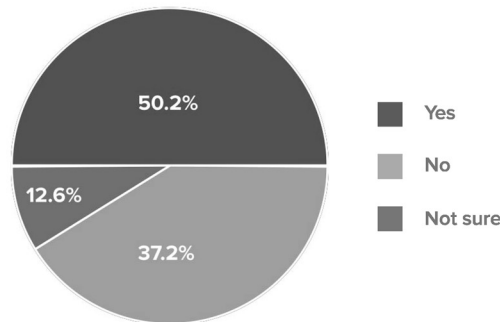


Margin of Error +/- 3.2 percentage points. Subsets have a larger margin of error than the whole data set. As a rule we do not rely on the validity of very small subsets of the data, especially sets smaller than 50-75 respondents. At that size subset we can make generalizations, but in these cases the data is more qualitative than quantitative.

Zogby
Analytics

Interactive Survey of US Adults (April 2013)

Has an online advertisement ever helped you save money on a purchase or saved you time in finding it?

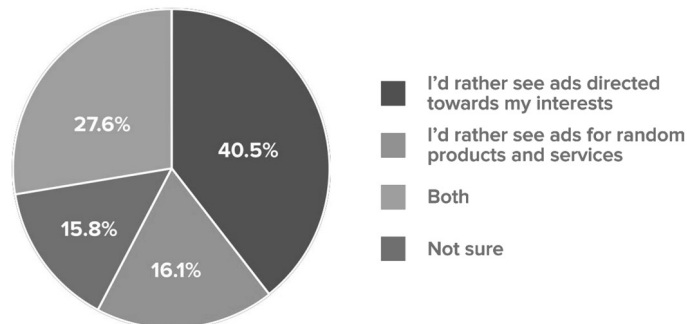


Margin of Error +/- 3.2 percentage points. Subsets have a larger margin of error than the whole data set. As a rule we do not rely on the validity of very small subsets of the data, especially sets smaller than 50-75 respondents. At that size subset we can make generalizations, but in these cases the data is more qualitative than quantitative.

Zogby
Analytics

Interactive Survey of US Adults (April 2013)

Would you rather see Internet ads for random/generic products and services, or ads for products and services that reflect your interests?

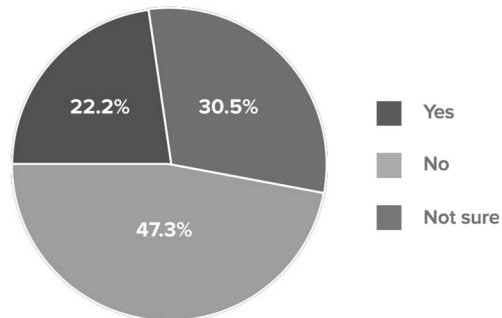


Margin of Error +/- 3.2 percentage points. Subsets have a larger margin of error than the whole data set. As a rule we do not rely on the validity of very small subsets of the data, especially sets smaller than 50-75 respondents. At that size subset we can make generalizations, but in these cases the data is more qualitative than quantitative.

Zogby
Analytics

Interactive Survey of US Adults (April 2013)

Would you support a law that restricted how data is used for Internet advertising, but also potentially reduced the availability of free content like blogs and video sites online?

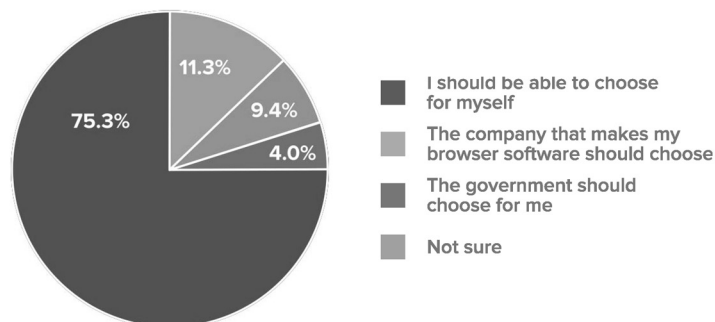


Margin of Error +/- 3.2 percentage points. Subsets have a larger margin of error than the whole data set. As a rule we do not rely on the validity of very small subsets of the data, especially sets smaller than 50-75 respondents. At that size subset we can make generalizations, but in these cases the data is more qualitative than quantitative.

Zogby
Analytics

Interactive Survey of US Adults (April 2013)

Who should be making choices about what sorts of ads I see and how they are generated?

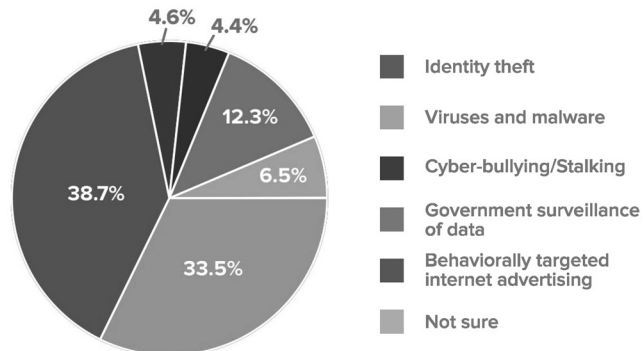


Margin of Error +/- 3.2 percentage points. Subsets have a larger margin of error than the whole data set. As a rule we do not rely on the validity of very small subsets of the data, especially sets smaller than 50-75 respondents. At that size subset we can make generalizations, but in these cases the data is more qualitative than quantitative.

Zogby
Analytics

Interactive Survey of US Adults (April 2013)

What is your biggest concern about the Internet?

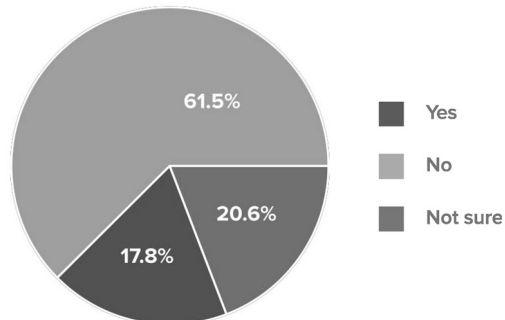


Margin of Error +/- 3.2 percentage points. Subsets have a larger margin of error than the whole data set. As a rule we do not rely on the validity of very small subsets of the data, especially sets smaller than 50-75 respondents. At that size subset we can make generalizations, but in these cases the data is more qualitative than quantitative.

Zogby
Analytics

Interactive Survey of US Adults (April 2013)

Do you trust the government to regulate how Internet advertising is delivered?

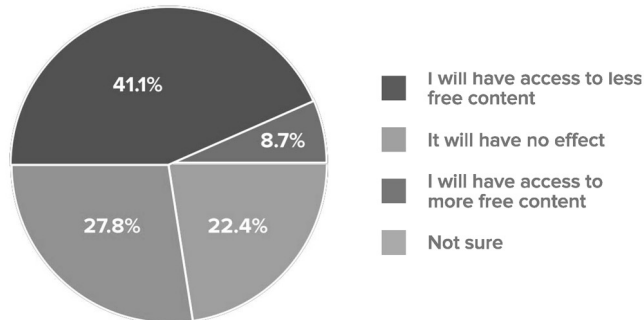


Margin of Error +/- 3.2 percentage points. Subsets have a larger margin of error than the whole data set. As a rule we do not rely on the validity of very small subsets of the data, especially sets smaller than 50-75 respondents. At that size subset we can make generalizations, but in these cases the data is more qualitative than quantitative.

Zogby
Analytics

Interactive Survey of US Adults (April 2013)

If a major Internet browser makes it harder for companies to display advertising to users, what do you think will be the impact on your user experience?



Margin of Error +/- 3.2 percentage points. Subsets have a larger margin of error than the whole data set. As a rule we do not rely on the validity of very small subsets of the data, especially sets smaller than 50-75 respondents. At that size subset we can make generalizations, but in these cases the data is more qualitative than quantitative.

Zogby
Analytics

Methodology

About the Survey:

The Digital Advertising Alliance commissioned Zogby Analytics to conduct the survey of 1,000 U.S. likely voters nationwide from April 2-3, 2013. Slight weights were added to age, race, gender, region, party, education, and religion to more accurately reflect the population. The margin of error is +/- 3.2 percentage points.

About Zogby Analytics:

For three decades, the Zogby companies have produced polls with an unparalleled record of accuracy and reliability. Zogby telephone and interactive surveys have generally been the most accurate in U.S. Presidential elections since 1996.

Zogby Analytics conducts a wide variety of surveys internationally and nationally in industries, including banking, IT, medical devices, government agencies, colleges and universities, non-profits, automotive, insurance and NGOs.



Zogby
Analytics

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV
TO JUSTIN BROOKMAN

Question 1. The DAA's testimony focused largely on its own self-regulatory program, the basis of which can be found in its *Self-Regulatory Principles for Multi-Site Data*. Mr. Mastria says that the DAA's choice mechanism is consistent with the recommendations of the Federal Trade Commission, and that its program and choice tools "share and meet the goals" of my Do-Not-Track legislation. Do you believe that the DAA's self-regulatory program and choice mechanism, in their current form, are sufficient for consumers? Why or why not?

Answer. CDT believes that the DAA's self-regulatory program has made some improvements in recent years in response to concerns voiced by consumers, regulators, and members of Congress. However, the current DAA opt-out structure still suffers from a number of fundamental flaws:

- It only applies to advertisers that are members of the DAA; companies that don't sign up and pay for membership are not included, and receive no indication that indication that a user does not want to be tracked. Although Mr. Mastria repeatedly described the DAA program as "universal" both in his written and oral testimony,¹ at one point he admitted that the program only covers "90 to 97 percent" of the advertising ecosystem.² Mr. Mastria did not reveal the methodology behind these numbers.
- The DAA opt-out is almost always cookie-based. If a user deletes her cookies—or if they are routinely deleted by her anti-virus software, as is often the case—the opt-out disappears, and even DAA companies subsequently have no way of knowing that the user does not want to be tracked. Users do have the opportunity to download and install browser add-ons to preserve opt-outs on the DAA site, but only if a user clicks on a vague link entitled "Protect My Choices" in the corner of the page.³ The link is offered without any explanation or context about what "Protect My Choices" means. Somewhat confusingly, the opt-out page later implies that the only effective approach to protecting one's choices is to periodically visit the DAA page:

The opt out choices you select are stored in opt out cookies only in this browser, so you should separately set your preferences for other browsers or computers you may use. Deleting browser cookies can remove your opt out preferences, so you should visit this page periodically to review your preferences, or update to include new participating companies.

- The opt-out only prevents users from seeing targeted ads, which are based on information gathered from tracking. However, it does not prevent tracking itself. While the DAA's Multi-Site Principles in principle agree with the notion of collection limitation, in practice, the code's bases for collection are extremely broad, and any justification to understand "consumer preferences and behaviors [or] research about consumers, products, or services" could justify individualized data collection despite the user's opting out.⁴
- It is not clear how many consumers have noticed the ad icon or understand that it is intended to signal that behavioral data collection is occurring. Moreover, the interface through which users are presented their choices around tracking and opting out both through the AdChoices icon and on the DAA website are confusing.⁵ For example, the TrustE interface lists a handful of tracking compa-

¹Testimony of Luigi Mastria before the Senate Committee on Commerce, Science & Transportation, Hearing on A Status Update on the Development of Voluntary Do-Not-Track Standards, April 24, 2013, http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=cd2e39e0-6825-4b8c-9789-40d26a72d457; Draft Transcript, Senate Committee on Commerce, Science & Transportation, Hearing on A Status Update on the Development of Voluntary Do-Not-Track Standards, April 24, 2013, at 25–2.

²Draft Transcript, Senate Committee on Commerce, Science & Transportation, Hearing on A Status Update on the Development of Voluntary Do-Not-Track Standards, April 24, 2013, at 70–17.

³Digital Advertising Alliance, Opt Out from Behavioral Advertising (Beta), <http://www.aboutads.info/choices/>.

⁴Digital Advertising Alliance, Self-Regulatory Principles for Multi-Site Data, <http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf>.

⁵A. M. McDonald and Lorrie Faith Cranor, *Social Science Research Network*, "Beliefs and behaviors: Internet users' understanding of behavioral advertising," October 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092; Pedro G. Leon *et al.*, *Carnegie Mellon University CyLab*, "Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising," October 2011, http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html.

nies, but not all for which a user could opt out. Even then, TrustE's interface does not allow a user to opt out of all of even this handful—instead a user is instructed to go to the third-party service to opt out individually. You can only opt out of all DAA members if you click through to an undefined link reading “Industry Resources” in the corner of the page:

TRUSTe Your Advertising Choices

How does it work?

Advertisers may collect data about your online browsing activity and use it to show you targeted ads (a process known as “behavioral advertising”).

You can prevent the companies listed below from showing you targeted ads by submitting opt-outs. Opting-out will only prevent targeted ads so you may continue to see generic (non-targeted ads) from these companies after you opt-out.

You may opt in to behaviorally targeted ads anytime by deleting your browser's cookies.

AD PROVIDER → **Targeted Ad** → **WEBSITE**
Generic Ad → **AD**

[Learn More >](#)

Educate Yourself

Learn more about behavioral advertising and your choices.
[Industry Resources >](#)
[TRUSTe Resources >](#)

Contact TRUSTe

Questions? Concerns? Let us know!
[Contact TRUSTe >](#)

Follow TRUSTe

In San Jose for #app academy? Join us TONIGHT for a cocktail hour @sancbar <http://t.co/ET4uO4Ym>

new post from our EMEA director @dibovic: is enforcement around the corner for the EU Cookie Directive? <http://t.co/22o8Qqhb>

[f](#) [t](#) [in](#)

Company	Company Type	Status	Opt-out
+ eXelate Media	Exchange		☐
+ Experian	Data Provider / Aggregator		☐
+ IXI	Attribution / Analytics		☐
+ Magnetic (Domdex)	Exchange	no cookie	☐
+ Proximi	Data Provider / Aggregator		☐
+ Quantcast	Data Provider / Aggregator		☐
+ Simpli.fi	Retargeting / Optimization		☐
+ TARGUSinfo	Data Provider / Aggregator	no cookie	☐
+ uKnow	Retargeting / Optimization		☐

[Submit Opt-outs](#)

[About TRUSTe](#) | [Contact Us](#) | [Privacy Policy](#) | [Terms of Service](#)

Question 2. Can the DAA's existing self-regulatory scheme be narrowed or changed in some way as to place reasonable, meaningful limits on the collection of consumer's information? How?

Answer. As we have previously advocated,⁶ any global opt out regime must more meaningfully address data collection and retention than the current DAA principles do. We believe that product improvement and market research should not be permitted exceptions that trump a user's opt out instruction. Furthermore, we believe that DAA should require companies to state their data retention periods for legitimate permitted exceptions such as security and fraud prevention.

However, improvements to the DAA still will not achieve universality of protection. As I noted at the hearing in response to a question from Senator Heller, there are ad networks like Dataium that operate outside of the DAA that use personally identifiable information to track users' web surfing habits.⁷ Moreover, companies like Facebook and Twitter—who have more third-party tracking elements on websites than any ad network—are not DAA members and are not bound by their principles.⁸

Ultimately, we believe that comprehensive data protection law is needed to ensure that all companies honor user control mechanisms online and offline. Self-regulatory codes of conduct such as the DAA principles and Do Not Track could qualify for safe harbor status under the privacy protection frameworks proposed by President Obama in his Consumer Privacy Bill of Rights, if the Federal Trade Commission

⁶Center for Democracy & Technology, *What Does Do Not Track Mean?*, April 27, 2011, https://www.cdt.org/files/pdfs/20110447_DNT_v2.pdf; Erica Newland, *CDT compromise proposal to the W3C Washington Face to Face meeting*, April 7, 2012, <http://lists.w3.org/Archives/Public/public-tracking/2012Apr/0078.html>.

⁷Jennifer Valentino-Devries and Jeremy Singer-Vine, “They Know What You're Shopping For,” *Wall Street Journal*, December 7, 2012, <http://online.wsj.com/article/SB10001424127887324784404578143144132736214.html>.

⁸Digital Advertising Alliance, Participating Companies, <http://www.aboutads.info/participating>.

deems them sufficient to fully protect user privacy. Unfortunately, the current DAA code, despite significant improvement in recent years, would be unlikely to merit such a finding today.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BARBARA BOXER TO
JUSTIN BROOKMAN

Question 1. In your written testimony, you recommend that third-party companies be permitted to collect and use unique identifiers from users for operational purposes but not for secondary purposes. How do you distinguish operational purposes from secondary purposes?

Answer. We believe that data collection that is *reasonably necessary* for the delivery of non-targeted advertising qualifies as a purpose for which a company may collect data despite a Do Not Track signal from the user. For example, a third-party ad network needs to collect a user's IP address as well as information about the user's device and browser just to be able to render an advertisement. We believe that cookies may in some cases be reasonably necessary to meaningfully prevent click-fraud and for accounting and attribution purposes. However, if those same necessary purposes could be reasonably accomplished without using cookies, companies should be prevented from using cookies for those purposes when Do Not Track is enabled.

We believe that purposes such as targeted advertising, market research, and product improvement are secondary uses that are not necessary for the mere delivery of advertisements, and should be prevented when Do Not Track is enabled. While we certainly agree that there can be societal value from these activities, we believe that a user's decision to disable cross-site tracking should be honored in these cases, and all others where the collection and retention of user data is not actually required for third-party (non-behavioral) advertising to function.

Question 2. How do consumers' expectations differ with respect to first-party and third-party tracking?

Answer. First-party tracking is considerably more intuitive than tracking by third parties. It is not particularly surprising to a user when Amazon suggests products based on items previously purchased from the service, when *The New York Times* recommends stories based on what you've read on their site, or when Weather.com remembers the locations for which you've requested weather forecasts. In each of these cases, the user has made the decision to utilize a service and to affirmatively provide information to the service, either actively (by purchasing products or filling out web forms) or at least passively (in the case of *The New York Times* above, by clicking on articles).

On the other hand, users often have no relationship whatsoever with most third-party tracking elements on websites. They have not made the decision to interact with those services, and have not intended to provide them with information. Moreover, third-party tracking services have the capacity to track users over multiple websites, so they have the ability to glean much more information about a user over a variety of disparate services, with little to no indication to the user that the tracking is occurring other than potentially targeted advertisements. For these reasons, we believe that third-party tracking is of more privacy concern than first-party tracking, though we believe that users should have control over first-party tracking as well. However, Do Not Track was originally formulated as a means to address just the more vexing third-party tracking issue.⁹

Question 3. Do you support Mozilla's and Apple's decisions to block third-party cookies by default?

Question 4. What steps can be taken to address non-cookie tracking such as digital fingerprinting?

Answer. Given the proliferation of tracking in recent years¹⁰ and the lack of reliable control over third-party data collection,¹¹ we believe that Mozilla's and Apple's decisions to disable third-party cookies are justified. Both companies can legiti-

⁹Center for Democracy & Technology, Submission *In advance of the FTC Town Hall, "Behavioral Advertising: Tracking, Targeting, and Technology,"* to be held November 1-2, 2007 in Washington, D.C., October 31, 2007, <https://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf>.

¹⁰Julia Angwin, "The Web's New Gold Mine: Your Secrets," *The Wall Street Journal*, July 30, 2010, <http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html>; George Simpson, "Suicide by Cookies," *MediaPost*, February 22, 2013, <http://www.media-post.com/publications/article/194073/suicide-by-cookies.html#axzz2REncGaSy>.

¹¹See *supra* pp 1-2.

mately claim that the majority of users do not like behavioral advertising, as Microsoft did in explaining why it pushes users to turn on Do Not Track during the installation of Internet Explorer 10.¹² On the other hand, Google's decision to enable third-party cookie setting is defensible as well, so long as there are reliable controls through which users can disable such cookies. Fortunately, there appears to be sufficient competition among browsers at the moment to give users a range of options in balancing privacy and usability.

While we are supportive of Apple's and Mozilla's decision to block third-party cookie setting by default, that is a short-term solution. Both browsers still make available other information to ad networks, including IP address and information about the configuration of the user's browser, through which companies can identify users across services with some reliability using digital fingerprinting techniques. Currently, the only way to reliably prevent fingerprinting is through preventing third-party connections from websites. Unfortunately, this results in ad and widget blocking, which prevents publishers from serving even privacy-protective advertising (non-behavioral ads with limited data retention). We are hopeful that browsers will ultimately be able to obscure individual browsers enough—or otherwise limit information about browsers that can be called by third parties—that digital fingerprinting will no longer be a reliable tracking technique. However, until that occurs, users (or software acting on behalf of users) can justifiably block third parties that do not publicly commit to honor user requests to stop cross-site tracking.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. FRANK R. LAUTENBERG TO
JUSTIN BROOKMAN

Question. A 2010 *Wall Street Journal* series on online privacy illustrated the extent to which individuals are being tracked and how the invasive practice can cause real harm. A recent high-school graduate, who had been identified by advertisers as concerned about her weight, told the paper she sees weight-loss ads every time she goes on the Internet. She said, "I'm self-conscious about my weight. I try not to think about it . . . then [the ads] make me start thinking about it." Do you believe this qualifies as a real harm?

Many believe the lack of transparency—particularly with regard to 3rd party cookies—and an individual's inability to know what personal information is actually being collected can cause real harm because consumers don't have the ability to understand how to protect themselves from invasive tracking. Do you agree that this is a harm?

Do you believe that consumers have a basic right to privacy online?

Answer. First of all, we do not believe that *harm* is the appropriate threshold to meet for when private companies should decide to comply with user preferences. "Do Not Track" is largely intended to mirror the opt-out regime that the advertising industry already supports, but with some improvements to durability and scope. Previously, neither browsers nor advertising companies argued that users should have to demonstrate harm in order to opt out of behavioral advertising, or to block or delete third-party tracking elements such as cookies.

We agree that users can experience some degree of harm through being reminded that some unknown third parties possess sensitive and potentially embarrassing information about the user, as in the weight loss example you suggest. However, more fundamentally, we believe that a user has a fundamental interest in protecting all their personal information from being exposed to unwanted parties—including an interest in shielding information about their web surfing from advertising companies. Users have a right to read online content anonymously that stems from a natural desire to preserve a personal space where our activities and motivations are not recorded, evaluated, and preserved. Unfortunately, online tracking today is hardly anonymous. In some cases, behavioral profiles are tied explicitly to personally identifying information.¹³ In other cases, because those profiles are persistently linked to individual devices, they necessarily could be tied to personally identifying information in the future (either by obtaining identifying information such as a name or e-mail address from a website that has possesses that information, or

¹²Brad Smith, *Privacy and Technology in Balance?*, Microsoft on the Issues, October 26, 2012, http://blogs.technet.com/b/microsoft_on_the_issues/archive/2012/10/26/privacy-and-technology-in-balance.aspx.

¹³Jennifer Valentino-Devries and Jeremy Singer-Vine, They Know What You're Shopping For, *Wall Street Journal*, December 7, 2012, <http://online.wsj.com/article/SB10001424127887324784404578143144132736214.html>; Jonathan Mayer, Tracking the Trackers: Where Everybody Knows Your Username, Center for Internet and Society Blog, October 11, 2011, <http://cyberlaw.stanford.edu/blog/2011/10/tracking-trackers-where-everybody-knows-your-username>.

through a subpoena to an Internet service provider for identifying information associated with an Internet protocol (IP) address.

We do not believe, however, that this right—or privacy rights in general—are absolute. Many times they intersect with others’ free expression rights, such as the right of the press to report truthful factual information about individuals. Other times, we believe that information about individuals may justifiably be collected on an opt-out, instead of opt-in basis, based on the sensitivity of the information at stake. Many categories of behavioral data collection might fall into rights that are reasonably enforceable only on an opt-out basis. However, that opt-out right must be robust and scalable, so that users can stop (or at least meaningfully limit) data collection by third parties with which a user has no relationship.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. AMY KLOBUCHAR TO
JUSTIN BROOMAN

Question 1. Most consumers would like to believe that their information is private, secure, and accurate. However, with rapidly changing technologies and platforms consumers are no longer sure. Can you discuss how you feel consumers are reacting to the host of privacy options that are out there and share your views on if they are more or less trusting when it comes to online information?

Answer. There is ample evidence that users are increasingly skeptical of online tracking behaviors, and that they reject the basic behavioral advertising model as illegitimate.¹⁴ Users are also starting to take advantage of tools to fight back against the monitoring of their online activities. A large percentage of users have installed anti-spyware/anti-virus software that deletes third-party tracking cookies on a regular basis. The most popular web extension on the Internet is Ad Block Plus, which prevents third parties from doing *any* tracking of users (but also prevents privacy-protective advertising as well).¹⁵ And over 17 percent of users have turned on “Do Not Track” in the Firefox web browser—despite the fact that it is not yet being honored by the majority of third-party trackers—with the percentage of Firefox mobile users likely to be significantly higher.¹⁶

Unfortunately, each of these approaches is imperfect. “Do Not Track” was conceived as a middle-ground solution that allows for the serving of third-party content while significantly limiting the amount of information that third parties can collect about users. If industry cannot agree to honor users’ Do Not Track signals, then browsers are likely to take more drastic actions to protect their user base. For years, privacy advocates have worried that in an arms race between users and ad networks, users, who by and large lack the sophistication and technical skills of the ad networks, were destined to lose. However, with the browsers increasingly acting in accordance with the desires of their user base, that result is no longer a foregone conclusion. If trade associations continue to stick their heads in the sand and ignore consumer sentiment about their practices (instead of establishing a value proposition to users about behavioral advertising’s benefits), moves like Mozilla’s and Ap-

¹⁴ See e.g., Scott Cleland, Americans Want Online Privacy—Per New Zogby Poll, PUBLIUS’ FORUM, June 9, 2010, <http://www.publiusforum.com/2010/06/19/americans-want-online-privacy-per-new-zogby-poll/>; Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessey, Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It (Sept. 2009), http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf. See also Alan F. Westin, Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles: Level of Comfort Increases when Privacy Safeguards Introduced, HARRISINTERACTIVE, April 10, 2008, <http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Majority-Uncomfortable-withWeb-sites-Customizing-C-2008-04.pdf> (in which majority of respondents said they were not comfortable with online companies using their browsing behavior to tailor ads and content to their interests even when they were told that such advertising supports free services); John B. Horrigan, Use of Cloud Computing Services, PEW INTERNET & AMERICAN LIFE PROJECT, September 2, 2008, http://www.pewinternet.org/~media/Files/Reports/2008/PIP_Cloud_Memo.pdf (showing that 68 percent of users of cloud computing services say they would be very concerned if companies that provided these services analyzed their information and then displayed ads to them based on their actions).

¹⁵ Firefox Add-ons, Mozilla.org, <https://addons.mozilla.org/en-us/firefox/extensions/?sort=users>.

¹⁶ Alex Fowler, Mozilla’s new Do Not Track dashboard: Firefox users continue to seek out and enable DNT, May 3, 2013, <http://blog.mozilla.org/privacy/2013/05/03/mozillas-new-do-not-track-dashboard-firefox-users-continue-to-look-out-and-enable-dnt/>; Alex Fowler, Do Not Track Adoption in Firefox Mobile is 3x Higher Than in Desktop, Mozilla Privacy Blog, November 2, 2011, <http://blog.mozilla.org/privacy/2011/11/02/do-not-track-adoption-in-firefox-mobile-is-3x-higher-than-desktop/>.

ple's to frustrate cross-site tracking will become the norm, and an inability to set cookies may be the least of their concerns.

Question 2. What role should the Federal Trade Commission or the Department of Commerce have regarding Do-Not-Track?

Answer. We believe that the FTC and Department of Commerce have been right to use the bully pulpit to call for the enactment of a voluntary Do Not Track standard, but they are otherwise limited in what they can enforce. CDT has previously argued that the Federal Trade Commission could interpret its Section 5 authority more aggressively to implement the full range of Fair Information Practice Principles—to require transparency, data minimization, and a right to opt out of certain uses, including behavioral advertising.¹⁷ However, Section 5 is a vaguely worded statute, and it is not clear that the courts would agree with such an interpretation: indeed, Wyndham Hotels is certainly challenging in Federal court the FTC's argument that Section 5 requires companies to implement reasonable security practices to safeguard consumer data.¹⁸

We think it would be better for consumers and businesses to have more certainty about the scope of personal privacy protections, which is why we have long advocated for the enactment of reasonable, flexible comprehensive privacy legislation based on the Fair Information Practice Principles.¹⁹ We continue to believe that carefully crafted legislation is the best approach to encouraging legitimate innovation while preserving user's ability to exercise control over their personal information. We do see a role for self-regulatory codes of conduct such as Do Not Track as a potential safe harbor under an omnibus privacy law, provided that the Federal Trade Commission deems them sufficient to fully protect user privacy. We are gratified that both the FTC and the White House have now called for the enactment of such comprehensive privacy legislation. It is now up to Congress to enact these privacy protections into law.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BRIAN SCHATZ TO
JUSTIN BROOKMAN

Question 1. One of the rallying cries of the online advertising industry against do-not-track defaults and additional regulation of online data collection is that, if you prevent online advertisers from collecting information about consumers online, you will jeopardize the availability of free content on the internet. Do you think that there is necessarily a trade-off between a universally recognized do-not-track system or standard and the availability of free content on the Internet?

Answer. Behavioral advertising certainly provides some marginal value to the advertising ecosystem, though it has not been demonstrated how significant this increase is. It is also not evident how much of the extra value provided by behavioral advertising is absorbed by the increased intermediaries in the digital advertising and data broker infrastructure, and how much trickles down to the first-party publishers. Given the limited bargaining power of smaller, long-tail websites, it is not evident that they see much benefit from advertisements that are personalized based on web tracking.

Moreover, it is important to note that the considerable majority of web advertising is not behavioral. Stanford research Jonathan Mayer estimated that behavioral advertising constituted 4 percent of web advertising in 2009, though that number is likely rising as companies find more sophisticated and reliable methods to track users.²⁰

Regardless of the extent of the trade-off, we believe that consumers should be the ones assessing the relative benefits, not industry or government. If a user turns on Do Not Track, and sites start to limit the content they make available to that user,

¹⁷ Center for Democracy & Technology, The Role of Privacy by Design in Protecting User Privacy: Comments of the Center for Democracy & Technology in regards to the FTC Consumer Privacy Roundtable, December 21, 2009, <http://www.ftc.gov/os/comments/privacyroundtable/544506-00067.pdf>.

¹⁸ Danielle Walker, Wyndham Hotels challenges FTC security suit over breaches, SC Magazine, September 11, 2012, <http://www.scmagazine.com/wyndham-hotels-challenges-ftc-security-suit-over-breaches/article/258559/>.

¹⁹ Center for Democracy & Technology, Testimony of Leslie Harris before the House Energy & Commerce Committee, Subcommittee on Commerce, Trade, and Consumer Protection on The BEST PRACTICES Act of 2010 and Other Federal Privacy Legislation, July 22, 2010, https://www.cdt.org/files/pdfs/CDT_privacy_bill_testimony.pdf.

²⁰ Jonathan Mayer, *Do Not Track Is No Threat To Ad-Supported Businesses*, Center for Internet and Society Blog, January 20, 2011, <http://cyberlaw.stanford.edu/blog/2011/01/do-not-track-no-threat-ad-supported-businesses>.

she should make the decision about whether to continue to block tracking, or to allow tracking just on this site, or to face the consequences of her decision and accept less content—or to pay another price. However, we reject the paternalistic assertions that users should be deprived of control of their personal information because of a judgment that it is in their best interests to have their browsing habits invisibly tracked online—despite significant evidence that consumers broadly reject such practices.²¹

Question 2. In 2009, the FTC called on the online advertising industry to provide consumers with transparency, notice, and personal control to control behavioral advertising—in the ensuing three years, do you think that online advertisers have succeeded in providing that to consumers?

Answer. The Digital Advertising Alliance has made improvements in recent years, most notably by enacting the Self-Regulatory Principles for Multi-Site Data in 2011. The most significant improvement was around the limitation of purposes for which behavioral data may be used, including a prohibition on the usage of behavioral data for employment, credit, health care treatment, and insurance eligibility.²²

However, those improvements are somewhat separate from transparency, notice and control. The DAA has embarked on a program to place an icon in all targeted advertisements as a method to provide notice to users. However, we are not convinced that this program has been successful in educating average users about behavioral advertising. Anecdotally, when asking friends and acquaintances outside of privacy circles whether they have noticed the icon, the answer has been universally “no.” Moreover, the interface that a user encounters after clicking on the icon is often confusing and unintuitive.²³

The controls over behavioral data collection remain flawed: First, the opt-out only prevents users from seeing targeted ads, which are based on information gathered from tracking. However, it does not prevent tracking itself. While the DAA’s Multi-Site Principles in principle agree with the notion of collection limitation, in practice, the code’s bases for collection are extremely broad, and any justification to understand “consumer preferences and behaviors [or] research about consumers, products, or services” could justify individualized data collection despite the user’s opting out.²⁴

Second, the DAA opt-out is almost always cookie-based. If a user deletes her cookies—or if they are routinely deleted by her anti-virus software, as is often the case—the opt-out disappears, and even DAA companies subsequently have no way of knowing that the user does not want to be tracked. Users do have the opportunity to download and install browser add-ons to preserve opt-outs on the DAA site, but only if a user clicks on a vague link entitled “Protect My Choices.”²⁵ The link is offered without any explanation or context about what “Protect My Choices” means. Somewhat confusingly, the opt-out page later implies that the only effective approach to protecting one’s choices is to periodically visit the DAA page:

The opt out choices you select are stored in opt out cookies only in this browser, so you should separately set your preferences for other browsers or computers you may use. Deleting browser cookies can remove your opt out preferences, so you should visit this page periodically to review your preferences, or update to include new participating companies.

Question 3. Even if do-not-track is an available option for consumers, it does not seem to be an effective tool for protecting consumer’s privacy. First, online advertisers largely ignore do-not-track headers. Second, the lack of consensus on what do-not-track means, in terms of what data is still collected and for what purpose, renders do-not-track meaningless.

Is it true that, currently, when a user *thinks* he or she has opted out of tracking—whether it is through an opt-out cookie or using a do-not-track heading on a browser—online advertisers are still collecting information about that user for advertising purposes?

Answer. Today, when a user turns on Do Not Track or opts out through the DAA process, behavioral data collection and retention is unaltered in most cases (some companies, such as Google, use non-unique opt-out cookies when a user opts out,

²¹See *supra* note 14.

²²Self-Regulatory Principles for Multi-Site Data, Digital Advertising Alliance, November 2011, <http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf>.

²³See *supra* p 3.

²⁴Digital Advertising Alliance, Self-Regulatory Principles for Multi-Site Data, <http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf>.

²⁵Digital Advertising Alliance, Opt Out from Behavioral Advertising (Beta), <http://www.aboutads.info/choices/>.

making it more difficult to correlate third-party users over time). We remain hopeful that a meaningful Do Not Track standard can be negotiated that will be adopted and enforced by major trade associations such as the DAA. However, even then, participation will be strictly voluntary, and tracking companies such as Dataium can simply choose not to pay to join a trade association and could continue to track users both online and off.²⁶ Ultimately, we believe that baseline privacy legislation should be enacted that encourages adoption of codes of conduct such as Do Not Track by providing safe harbor status and deemed compliance for programs certified by the Federal Trade Commission.²⁷ Only then will companies be sufficiently incentivized to provide sufficiently robust privacy protections for users.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RON JOHNSON TO
JUSTIN BROOKMAN

Question 1. What are the harms that are actually occurring to consumers through anonymous cookie-based “tracking?” As indicated in Mr. Mastria’s testimony, the primary privacy concerns for most consumers online have to do with identity theft, viruses and malware, and government surveillance. So, what harms are occurring that the FTC doesn’t currently already have the authority to address?

Answer. The Center for Democracy & Technology is willing to concede that identity theft and malware may be of greater concern to the average user than online Internet tracking. However, that does not logically mean that consumers are not concerned about behavioral tracking as well; merely because one problem is considered of more significance than another does not mean we should ignore the lesser problem. It would not be a valid argument, for example, to argue that Congress should ignore allegations that the Internal Revenue Service signaled out tea party groups¹ because a poll showed that Americans were relatively *more concerned* about the economy and job growth. And, it should be noted, identity theft and malware are currently illegal. The FTC and private citizens have legal tools to seek redress from bad actors who engage in those sorts of behaviors.

On the other hand, users do not have robust tools to address online behavioral data collection, and a vast majority of Americans still consider that to be a problem.² Increasingly, we live in a world where everything we do is observable. Pervasive closed-circuit television and drone surveillance, and the emergence of facial recognition, may soon allow companies to persistently track users across space and over time by their individual identities.³ Indeed, even the privacy that we expect inside our house is threatened by technological developments. Researchers at the University of Washington have uncovered ways to determine what television shows

²⁶ Jennifer Valentino-Devries and Jeremy Singer-Vine, “They Know What You’re Shopping For,” *Wall Street Journal*, December 7, 2012, <http://online.wsj.com/article/SB10001424127887324784404578143144132736214.html>.

²⁷ See *supra*, p 4.

¹ See Mark Stanley, IRS Targeting of Tea Party Groups Shows Need for ECPA Reform; CDT Blog, May 10, 2013, <https://www.cdt.org/blogs/mark-stanley/1005irs-targeting-conservative-groups-illustrates-need-ecpa-reform>.

² See e.g., Scott Cleland, Americans Want Online Privacy—Per New Zogby Poll, PUBLIUS’ FORUM, June 9, 2010, <http://www.publiusforum.com/2010/06/19/americans-want-online-privacy-per-new-zogby-poll>; Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessey, Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It (Sept. 2009), http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf. See also Alan F. Westin, Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles: Level of Comfort Increases when Privacy Safeguards Introduced, HARRISINTERACTIVE, April 10, 2008, <http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Majority-Uncomfortable-with-Websites-Customizing-C-2008-04.pdf> (in which majority of respondents said they were not comfortable with online companies using their browsing behavior to tailor ads and content to their interests even when they were told that such advertising supports free services); John B. Horrigan, Use of Cloud Computing Services, PEW INTERNET & AMERICAN LIFE PROJECT, September 2, 2008, http://www.pewinternet.org/-/media/Files/Reports/2008/PIP_Cloud_Memo.pdf (showing that 68 percent of users of cloud computing services say they would be very concerned if companies that provided these services analyzed their information and then displayed ads to them based on their actions).

³ See Harley Geiger, The Drones are Coming, CDT Blog, December 21, 2011, <https://www.cdt.org/blogs/harley-geiger/2112drones-are-coming>; Harley Geiger, Facial Recognition and Privacy, CDT Blog, December 6, 2011, <https://www.cdt.org/blogs/harley-geiger/612facial-recognition-and-privacy/>.

are being watched inside a home by measuring the electromagnetic radiation emitted from the power lines publicly observable outside your house.⁴

There is an incredible amount that we as a society have to gain from innovative new technologies, but there is also an incredible amount that we have to lose. Without a framework in place to assure everyday consumers of the ability to limit the collection and retention of the minutiae of their lives by unknown third parties, any sense of a realm of personal privacy may completely evaporate. In short, we may lose:

- Our right to read newspapers unnoticed: to throw a quarter into the vending box and grab a copy, to privately choose which articles we read and which we don't, gradually slips away each time a local paper shuts its presses or halts print distribution.
- Our right not just go for a drive unnoticed, but to talk to friends unnoticed, to write letters unnoticed,⁵ to read books unnoticed, to watch a TV show unnoticed, to buy a gift unnoticed—all of these rights are eroding as these activities move into the networked world and surveillance technologies become more sophisticated.
- Our right to walk down the street unnoticed, whether en route to a political rally or to a doctor's office, is eroding as facial recognition technology advances and becomes more widely deployed.⁶

The right to read online content anonymously stems from a natural desire to preserve a personal space where our activities and motivations are not recorded, evaluated, and preserved. Unfortunately, online tracking today is hardly anonymous. In some cases, behavioral profiles are tied explicitly to personally identifying information.⁷ In other cases, because those profiles are persistently linked to individual devices, they necessarily could be tied to personally identifying information in the future (either by obtaining identifying information such as a name or e-mail address from a website that has possesses that information, or through a subpoena to an Internet service provider for identifying information associated with an Internet protocol (IP) address).

People are understandably concerned with the creation of these stores of very personal information about what they do online, as the information could subsequently be exposed through a data breach, obtained by law enforcement without due process of law (and for potentially illegitimate and ideologically discriminatory purposes), viewed internally by employees within the company, or used to offer differential prices and user experience without transparency. More fundamentally, many people merely want to have some control over the sharing of their reading habits—to be able to access the web without having dozens of companies storing and evaluating what they do online. Do Not Track is intended an opt-out for those people—a way for consumers to tell companies that they don't want them looking over their shoulder. As I noted during my testimony, the advertising industry has already conceded the need to address such user objections by offering its own opt-out program; Do Not Track simply offers a more persistent and scalable solution.

CDT has previously argued that the Federal Trade Commission could interpret its Section 5 authority more aggressively to implement the full range of Fair Information Practice Principles—to require transparency, data minimization, and a right to opt out of certain uses, including behavioral advertising.⁸ However, Section 5 is a vaguely worded statute, and it is not clear that the courts would agree with such an interpretation: indeed, Wyndham Hotels is certainly challenging in Federal court the FTC's argument that Section 5 requires companies to implement reasonable se-

⁴Miro Enev, et al, Televisions, Video Privacy, and Powerline Electromagnetic Interference, Working Paper, <http://abstract.cs.washington.edu/~miro/docs/ccs2011.pdf>.

⁵USPS mail currently receives more privacy protections than does electronic mail. See, Federal Statutes and Regulations Relation to the Privacy and Security of Mail, <http://about.usps.com/who-we-are/privacy-policy/intelligent-mail-privacy.htm#H7>.

⁶See Harley Geiger, Facial Recognition and Privacy, CDT Blog, December 6, 2011, <https://www.cdt.org/blogs/harley-geiger/612facial-recognition-and-privacy/>.

⁷Jennifer Valentino-Devries and Jeremy Singer-Vine, They Know What You're Shopping For, *Wall Street Journal*, December 7, 2012, <http://online.wsj.com/article/SB10001424127887324784404578143144132736214.html>; Jonathan Mayer, Tracking the Trackers: Where Everybody Knows Your Username, Center for Internet and Society Blog, October 11, 2011, <http://cyberlaw.stanford.edu/blog/2011/10/tracking-trackers-where-everybody-knows-your-username>.

⁸Danielle Walker, Wyndham Hotels challenges FTC security suit over breaches, SC Magazine, September 11, 2012, <http://www.scmagazine.com/wyndham-hotels-challenges-ftc-security-suit-over-breaches/article/258559/>.

curity practices to safeguard consumer data.⁹ We think it would be better for consumers and businesses to have more certainty about the scope of personal privacy protections, which is why we have long advocated for the enactment of reasonable, flexible comprehensive privacy legislation based on the Fair Information Practice Principles.¹⁰ We continue to believe that carefully crafted legislation is the best approach to encouraging legitimate innovation while preserving user's ability to exercise control over their personal information.

Question 2. You state on the one hand that browsers are increasingly competing on privacy but on the other hand that we need a comprehensive privacy law. That doesn't add up to me. If industry is evolving its self-regulatory approach and browsers like our witness Mozilla is adopting its own standards, isn't the marketplace working today? Wouldn't new regulations thwart these important actions industry is undertaking today?

Answer. We are hopeful that the market will be able to deliver a comprehensive solution to online behavioral tracking, which is why we have spent two years within the World Wide Web Consortium trying to negotiate a reasonable consensus standard for Do Not Track. However, it is important to place this effort in historical context. We have been advocating for privacy protections over online behavioral profiles for over *fifteen years* now.¹¹ Numerous previous efforts to address the issue have failed.¹² At the same time, other industries have sprung up—such as mobile computing—that expose considerably more personal information than mere behavioral data, with often less control over that information.¹³ Personal privacy should not be a constant game of catch-up: trying to append after-the-fact privacy protections to existing business models after press attention draws scrutiny to unwanted (and previously unknown) practices.

A properly crafted privacy law would incentivize companies to build privacy into products from the beginning. If the United States had a comprehensive privacy statute such as we have previously supported,¹⁴ I do not believe this hearing would have been necessary, as companies would have a legal requirement to recognize a user's opt out request. That is not to say that a company would necessarily have to abide by that request. If a company were to insist on third party behavioral data collection as a condition of providing service to a consumer, privacy law should not interfere with such a business model in a robust marketplace. However, a privacy law could require that that business model be meaningfully messaged to a user—especially in response to an opt-out request—whereas today, much data collection and usage is not at all transparent to the average consumer. To the contrary, because the primary privacy law in this country today is Section 5 of the FTC Act's prohibition on deceptive practices, companies are meaningfully deincited from making privacy disclosures to consumers, because of the potential of exposing themselves to liability if they do not live up to those statements (even inadvertently).¹⁵

Privacy law should not try to make choices for users, but should empower them to make their own decisions about data. Unfortunately, many voices in the privacy debate insist on making paternalistic decisions on behalf of users—either prescribing broad swaths of data collection and usage because consumers do not like the practice, or in justifying all hidden data collection and usage without user transparency or choice because it supports content that users might not want to pay for. We instead prefer a solution where consumers can make informed decisions about

⁹Center for Democracy & Technology, Testimony of Leslie Harris before the House Energy & Commerce Committee, Subcommittee on Commerce, Trade, and Consumer Protection on The BEST PRACTICES Act of 2010 and Other Federal Privacy Legislation, July 22, 2010, https://www.cdt.org/files/pdfs/CDT_privacy_bill_testimony.pdf.

⁸Center for Democracy & Technology, The Role of Privacy by Design in Protecting User Privacy: Comments of the Center for Democracy & Technology in regards to the FTC Consumer Privacy Roundtable, December 21, 2009, <http://www.ftc.gov/os/comments/privacyroundtable/544506-00067.pdf>.

¹¹FTC Staff Report, Public Workshop on Consumer Privacy on the Global Information Infrastructure, December 1996, <http://www.ftc.gov/reports/privacy/Privacy1.shtm>, at II.C.2 (Consumer Choice).

¹²Pam Dixon, The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation, World Privacy Forum, Fall 2007, http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.

¹³Center for Democracy & Technology, Testimony of Justin Brookman before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law on Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones, and Your Privacy," May 10, 2011, <http://www.judiciary.senate.gov/pdf/11-5-10%20Brookman%20Testimony.pdf>.

¹⁴Center for Democracy & Technology, *supra* note 10.

¹⁵Federal Trade Commission, Complaint for Civil Penalties and Other Relief, *United States v. Google*, CV 12-04177, August 8, 2012, <http://www.ftc.gov/os/caselist/c4336/120809googlecmp.txt>.

their data, and to which companies in the marketplace can respond with a range of options. Unfortunately, consumers today trying to evaluate and choose among the data practices of various online and offline companies cannot get the information they desire. A privacy law would, *inter alia* require usable transparency, allowing the market to innovate in response to more meaningful signals about privacy practices and user intent.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BARBARA BOXER TO
ADAM THIERER

Question 1. In your written testimony, you express support for alternatives to Do Not Track such as the use of advertisers' ad preference managers and "private browsing" browser settings. Are these alternative approaches as persistent as a Do Not Track signal?

Answer. First, it is unclear at this stage exactly how persistent the Do Not Track signal would be because (a) the technical standard has not been finalized, and (b) it is unclear how many operators (advertisers, publishers, browser companies, etc) would honor the DNT request. Moreover, as I noted in my written testimony, even if Do Not Track takes root and some consumers turn it on, many will be incentivized by ad networks or publishers to opt right back in to "tracking" to retain access to sites and services they desire. In doing so, they may end up sharing even more information than they do today.

Regardless, to answer your original question, yes, some of these alternative approaches are persistent, especially tools like cookie-blockers and "private browsing" browser settings. And, when used in combination, these tools can provide extremely effective privacy protection. Of course, it is also true that with each additional layer of privacy protection a user adds, the browsing experience may grow more cumbersome.

Question 2. Do consumers understand the extent to which their activities are tracked online?

Answer. Evidence suggests that many consumers aren't aware of how online advertising and marketing work. It is also true that most consumers don't read site privacy policies. However, as I noted in a recent law review article,¹ it is also true that most consumers don't read or fully understand every proviso contained in the stacks of paper placed in front of them when they sign a home mortgage. The same is true for life insurance policies, which are full of incomprehensible provisions and stipulations, even though regulations govern those policies as well. It is also unlikely that consumers read and understand every provision of their car loan or warranty. The same is also true of mandatory Food and Drug Administration disclosures on pharmaceuticals. In each of these cases, far more is at stake for consumers than whatever "risk" they face by not fully comprehending online privacy policies. Accordingly, a certain amount of "rational ignorance" about privacy policies should be expected. Consumers will never be perfectly informed and it remains unclear exactly how much information they need for online markets to work effectively.

Question 3. Do consumers expect to be tracked by third-party companies with which they have never interacted?

Answer. Probably not, but it is unclear what harm comes from it. Meanwhile, enormous benefits accrue to those consumers from such "tracking." Specifically, it helps keep the price of online sites and service low or at zero. Moreover, it allows new products and services to be targeted to the public. Nonetheless, more could be done to educate the public about data collection and online "tracking."

Question 4. How would you recommend educating consumers about the alternative privacy-enhancing tools available to them?

Answer. A multi-layered strategy is needed to better educate consumers and encourage "digital citizenship." For youth, privacy education begins at home with parental guidance and mentoring about sensible online practices and behavior. Schools also have an essential role in mentoring youth about media literacy and acceptable online practices. Companies and trade associations also have a role here in that they should be doing more to inform users about what their data is being used for and how it benefits them. They should also better explain how to easily opt-out of data collection practices or, more simply, offer them simple tips for enhancing their online privacy. Many companies and trade associations already do this and much more.

¹Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 Harvard Journal of Law & Public Policy 409, 446–449 (2013).

Finally, government also has an important role in this educational process. In its most recent *Strategic Plan*, the Federal Trade Commission noted that, “Consumer and business education serves as the first line of defense against fraud, deception, and unfair practices.”² The FTC already partners with several other Federal agencies to offer OnGuardOnline, a site that offers wide-ranging security, safety, and privacy tips for consumers and businesses. As part of that effort, the FTC produces dozens of informational videos that are also available on dedicated YouTube page.³ Similarly, the FCC offers smartphone security advice on its website.⁴ State and local officials can also take steps to integrate privacy and security lessons and messaging into school curricula or other public awareness-building programs.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO
ADAM THIERER

Question 1. A 2010 *Wall Street Journal* series on online privacy illustrated the extent to which individuals are being tracked and how the invasive practice can cause real harm. A recent high-school graduate, who had been identified by advertisers as concerned about her weight, told the paper she sees weight-loss ads every time she goes on the Internet. She said, “I’m self-conscious about my weight. I try not to think about it . . . then [the ads] make me start thinking about it.” Do you believe this qualifies as a real harm?

Answer. While the individual may take great offense at such messages, it would be hard to classify them as “harmful,” at least in a legally actionable sense. More importantly, such commercial messages are protected by the First Amendment since they convey useful information.

Question 2. Many believe the lack of transparency—particularly with regard to 3rd party cookies—and an individual’s inability to know what personal information is actually being collected can cause real harm because consumers don’t have the ability to understand how to protect themselves from invasive tracking. Do you agree that this is a harm?

Answer. Consumers have the ability to protect themselves from all forms of online “tracking,” even if they do not understand how those things work in practice. The privacy tools already on the market today—which are widely available and either free of charge or very inexpensive—can be extremely effective in terms of protecting user privacy.

Question 3. Do you believe that consumers have a basic right to privacy online?

Answer. Citizens have a right to be free of actual harms to themselves or their property, but privacy has always been a highly subjective philosophical concept. It is also a constantly morphing notion that evolves as societal attitudes adjust to new cultural and technological realities. For these reasons, America may never be able to achieve a coherent fixed definition of the term or determine when it constitutes a formal right outside of some narrow contexts.⁵ For example, some specific uses of highly sensitive personal information may create harms, but laws already exist to deal with such concerns as they relate to health and financial privacy, among others.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RON JOHNSON TO
ADAM THIERER

Question 1. What are the harms that are actually occurring to consumers through anonymous cookie-based “tracking?” As indicated in Mr. Mastria’s testimony, the primary privacy concerns for most consumers online have to do with identity theft, viruses and malware, and government surveillance. So, what harms are occurring that the FTC doesn’t currently already have the authority to address?

Answer. As recent privacy-related enforcement actions against both Google¹ and Facebook² illustrate, the FTC already has broad discretion and plenary authority

²Federal Trade Commission, *Federal Trade Commission Strategic Plan for Fiscal Years 2009 to 2014*, 4, <http://www.ftc.gov/opp/gpra/spfy09fy14.pdf>.

³<http://www.youtube.com/user/FTCVideos>.

⁴<http://www.fcc.gov/smartphone-security>.

⁵Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 *Harvard Journal of Law & Public Policy* 409, 414–417 (2013).

¹Alex Howard, *Google Reaches Agreement with FTC on Buzz Privacy Concerns*, GOV20.GOVFRESH, March 30, 2011, <http://gov20.govfresh.com/google-reaches-agreement-with-ftc-on-buzz-privacy-concerns>.

²Brent Kendall, *Facebook Reaches Settlement with FTC on Privacy Issues*, WALL ST. J., Nov. 29, 2011, <http://online.wsj.com/article/BT-CO-20111129-710865.html>.

under Section 5 of the FTC Act to hold companies to the promises they make to their users as it pertains to information collection and data security.³ In consent decrees with both those companies, the FTC extracted a wide variety of changes to their privacy and data collection practices while also demanding that they undergo privacy audits for the next 20 years.⁴

Thus, the FTC certainly is not lacking the authority to address these issues. Professors Kenneth A. Bamberger and Deirdre K. Mulligan note that, “since 1996 the Federal Trade Commission has actively used its broad authority under Section 5 . . . to take an active role in the governance of privacy protection, ranging from issuing guidance regarding appropriate practices for protecting personal consumer information, to bringing enforcement actions challenging information practices alleged to cause consumer injury.”⁵

Question 2. It has been estimated that American websites would lose \$33 billion over five years if Congress mandates EU-style opt-in consent for interest-based advertising. You stated in your testimony that restrictions on data collection could undermine America’s global competitive advantage in this space. Is this what you had in mind?

Answer. Yes, that is exactly the sort of danger I was referring to in my testimony. If the American privacy regime was adjusted to look more like the one found in the European Union, which is far more regulatory in character, it is likely that compliance costs would increase for many online operators. “If applied to American companies, these European laws would restrict the breakneck innovation of the commercial web,” argues the NetChoice Coalition, which represents a variety of online vendors.⁶ Thus, privacy regulation could affect the global competitiveness of U.S. firms and diminish their competitive advantage in the global digital arena.

Economists have verified this. “In a setting where first-party advertising is allowable but third-party marketing is not, substantial advantages may be created for large incumbent firms,” argue Professors Avi Goldfarb and Catherine Tucker.⁷ “For example, if a large website or online service were able to use its data to market and target advertising, it will be able to continue to improve and hone its advertising, while new entrants will find it difficult to challenge the incumbent’s predominance by compiling other data or collecting their own data.”⁸

Goldfarb and Tucker found that “after the [European Union’s] Privacy Directive was passed [in 2002], advertising effectiveness decreased on average by around 65 percent in Europe relative to the rest of the world.”⁹ They argue that because regulation decreases ad effectiveness, “this may change the number and types of businesses sustained by the advertising-supporting Internet.”¹⁰ The European Union’s experience makes it clear that regulation of online advertising and data collection can affect market structure, competitive rivalry, and the global competitiveness of online firms.¹¹



³ Berin Szoka, *FTC Enforcement of Corporate Promises & the Path of Privacy Law*, TECH. LIBERATION FRONT, July 13, 2010, <http://techliberation.com/2010/07/13/ftc-enforcement-of-corporate-promises-the-path-of-privacy-law>.

⁴ Kashmir Hill, *So, What Are These Privacy Audits That Google And Facebook Have To Do For The Next 20 Years?* FORBES, November 30, 2011, <http://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years>; Matthew Sundquist, *Online Privacy Protection: Protecting Privacy, the Social Contract, and the Rule of Law in the Virtual World*, 25 REGENT U. L. REV. 153, 173–175 (2012).

⁵ Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 273 (2011).

⁶ Steve DelBianco & Braden Cox, *NetChoice Reply Comments on Department of Commerce Green Paper 7*, (Jan. 28, 2011), <http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=1EA98542-23A4-4822-BECD-143CD23BB5E9>.

⁷ Avi Goldfarb & Catherine Tucker, *Comments on ‘Information Privacy and Innovation in the Internet Economy,’* Comments to the U.S. Department of Commerce, Jan. 24, 2011, at 4, http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/NTIA_comments_2011_01_24.pdf.

⁸ *Id.*

⁹ Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Online Advertising*, 57 MANAGEMENT SCIENCE 57 (Jan. 2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259. Also see, Catherine Tucker, *Empirical Research on the Economic Effects of Privacy Regulation*, J. ON TELECOMM. & HIGH TECH. L. 265 (2012).

¹⁰ *Id.*

¹¹ Quentin Fottrell, *Will Privacy Protections Ruin the Internet?* MARKETWATCH, Feb. 3, 2012, http://www.marketwatch.com/story/will-privacy-protections-ruin-the-internet-2013-02-05?mod=wsj_share_tweet.