

**THE NEED FOR PRIVACY PROTECTIONS: IS
INDUSTRY SELF-REGULATION ADEQUATE?**

HEARING

BEFORE THE

**COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE**

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

—————
JUNE 28, 2012
—————

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



U.S. GOVERNMENT PRINTING OFFICE

81-711 PDF

WASHINGTON : 2013

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

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

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

ELLEN L. DONESKI, *Staff Director*

JAMES REID, *Deputy Staff Director*

JOHN WILLIAMS, *General Counsel*

RICHARD M. RUSSELL, *Republican Staff Director*

DAVID QUINALTY, *Republican Deputy Staff Director*

REBECCA SEIDEL, *Republican General Counsel and Chief Investigator*

CONTENTS

	Page
Hearing held on June 28, 2012	1
Statement of Senator Klobuchar	1
Statement of Senator Ayotte	2
Statement of Senator Rockefeller	45
Statement of Senator Thune	48

WITNESSES

Bob Liodice, President and CEO, Association of National Advertisers, Inc. on Behalf of The Digital Advertising Alliance	3
Prepared statement	5
Alex Fowler, Chief Privacy Officer, Mozilla	12
Prepared statement	14
Peter Swire, C. William O'Neill Professor of Law, The Ohio State University ..	19
Prepared statement	21
Berin Szoka, President, TechFreedom	29
Prepared statement	31

APPENDIX

Statement of Computer & Communications Industry Association	55
---	----

THE NEED FOR PRIVACY PROTECTIONS: IS INDUSTRY SELF-REGULATION ADEQUATE?

THURSDAY, JUNE 28, 2012

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

The Committee met, pursuant to notice, at 10 a.m. in room SR-253, Russell Senate Office Building, Hon. Amy Klobuchar, presiding.

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

Senator KLOBUCHAR. Call the hearing to order. Thank you, everyone, for being here. There are a few other things going on in Washington, so Senator Ayotte and I are chairing this hearing. I wonder why.

[Laughter.]

Senator KLOBUCHAR. But I know Chairman Rockefeller will be here soon. And I think you all know this is a very important subject to this committee. I see that Senator Thune is also here with us.

This is an important issue for the future of commerce in the U.S., and more and more of our daily lives, as we all know, as I checked Twitter and Facebook already this morning, more and more of our daily lives are connected to the Internet.

I believe that consumers need to have a larger voice when it comes to their online experience and their data, and that is why Chairman Rockefeller has worked with the FTC to create Federal policy that protects consumers' data online. And I hope that this committee will continue to work together to find the appropriate legislative balance.

I'm also pleased to see the efforts of the industry to self-regulate its practices regarding data collection and tracking. And I believe that industry actions are moving this privacy conversation forward in a positive way.

I hope we'll be able to work together in the Commerce Committee on consumer data privacy legislation going forward. And I would also like to commend the FTC and the Department of Commerce for keeping these issues in the forefront this year.

We always have to be as sophisticated as those that are trying to play around with some of the rules. And I think that we have tried to track that, but, most importantly, we've also worked with the industry to track that.

So, with that, Senator Ayotte, would you like to say a few words?

**STATEMENT OF HON. KELLY AYOTTE,
U.S. SENATOR FROM NEW HAMPSHIRE**

Senator AYOTTE. I would. Thank you, Madam Chair.

Last month, in this committee, we had the opportunity to hear from the FTC on privacy, so I look forward to hearing an additional perspective from the witnesses that are here before us today. So thank you for being here with us, including representatives from the technology and advertising industries and experts from the academic community.

This debate centers on how online information is legally collected and disseminated for commercial usage. It's critical that we first understand this process before we begin to debate how privacy should be regulated or legislated.

This field is evolving so rapidly that we must proceed cautiously and carefully before diving into any legislation. It is imperative that any legislation we consider guarantees that usage of collected data is not hampered by overly restrictive and burdensome Federal and regulatory policies.

As we all know, e-Commerce is a vibrant, thriving sector of the global economy. The Information Technology and Innovation Foundation estimated that the annual global economic benefit of the commercial Internet is \$1.5 trillion. This is more than medicine, investment in renewable energy, and government investment in R&D combined.

The Internet generates at least \$300 billion of economic activity annually, accounting for an astonishing 2 percent of the United States GDP.

The Kelsey Group estimates that Internet advertising, which was \$45 billion in 2007, is expected to grow to \$147 billion by the end of 2012. These statistics are just the tip of the iceberg and will continue to grow exponentially.

However, we are not here today to talk about statistics. The broader point here is that we are seeing the online world flourish, and that reality dictates that we find the proper balance between ensuring e-commerce has the tools it needs to thrive, innovate, and create jobs, and making sure our regulatory climate is one that provides adequate consumer safeguards.

As we all know, Microsoft set off quite a firestorm when it announced Internet Explorer 10 will have its "do not track" component default set to opt out of tracking. Whether or not this is the best policy shouldn't be up to Congress to determine.

The beauty of living in a free enterprise society is that the market has a way of determining what works and what does not, and what is popular with consumers and what is not. And at the end of the day, there is enough competition in the marketplace for consumers to have the opportunity to decide what works best for them without congressional interference.

Last, we must also acknowledge that there are certain benefits to data collection for consumers. For instance, we all enjoy free e-mail, countless free streaming videos, and free news services, just to name a few of the free online benefits that consumers enjoy. This is all possible because the collection of data leads to targeted advertising to pay for these services, and, more importantly, consumers choose to use these services because they value them.

I know that some members of this committee are aggressively calling for stringent privacy legislation. But as I mentioned, we must not act too quickly or haphazardly, and we need to be thoughtful in our approach in striking a proper balance.

This is a fast-moving field, and I'm concerned that hastily written legislation could be outdated by the time the ink dries and it becomes law.

I look forward to a robust discussion today with our distinguished panel. And I yield back the balance of my time. Thank you, Madam Chair.

Senator KLOBUCHAR. Thank you very much.

Now we're going to hear from our panel of witnesses. I will introduce them all and then have them give their opening statement.

First, Mr. Bob Liodice, who is the President and CEO of the Association of National Advertisers.

Second, Mr. Alex Fowler, who is the Global Privacy and Policy Leader with Mozilla.

Third, Mr. Peter Swire, who is the C. William O'Neill Professor of Law with Ohio State University.

And then, fourth, Mr. Berin Szoka, who is the President of TechFreedom.

Thank you all for being here, and we will begin with Mr. Liodice. Thank you.

**STATEMENT OF BOB LIODICE, PRESIDENT AND CEO,
ASSOCIATION OF NATIONAL ADVERTISERS, INC. ON BEHALF
OF THE DIGITAL ADVERTISING ALLIANCE**

Mr. LIODICE. Good morning, Senators. Thank you for the opportunity to be here, and thank you for your opening remarks.

My name is Bob Liodice. I am President and Chief Executive Officer of the Association of National Advertisers, also known as the ANA. We were founded in 1910, and our membership includes 460 member companies that represent over 10,000 brands that collectively spend over \$250 billion every year in marketing, communications, and advertising.

Today, I am pleased to testify on behalf of the Digital Advertising Alliance, also known as the DAA. The DAA is a nonprofit organization of leading companies and trade associations, including the ANA, the American Association of Advertising Agencies, the Direct Marketing Association, the Interactive Advertising Bureau, the American Advertising Federation, and the Network Advertising Initiative. Collectively, these associations represent over 5,000 corporations.

And my written testimony provides greater detail, but please let me highlight a few key points.

Let me begin by stating very clearly: our self-regulatory system works.

I've learned a long time ago not to confuse effort with results. Senators, we have results that few, if any, can claim. We have built and implemented a system that is operating and is effective.

Four years ago, we began this journey when 5,000 companies came together, recognizing the enormity and complexity of the challenge. We agreed that the pathway to success was through a highly perfected and enormously effective self-regulatory body.

It was created in 1971. It's administered by the Council of Better Business Bureaus. It is heralded by many Federal Trade Commission chairs as one of the best self-regulatory processes in the U.S. It's dynamic. It's fluid. It's evolutionary. And it's respected. And it is beyond reproach and without peer.

The DAA was built from this self-regulatory body to tackle the challenges and complexities of interest-based advertising, and to address the concerns that you all expressed through legislators, agencies, privacy groups, and consumers.

And we have succeeded. Our business system was created from a disciplined, seven-prong strategy that has had significant marketplace impact that has been enormously successful in a very short span of time.

Those seven planks are principles that were crafted and approved in July 2009, which includes consumer education, enhanced notice, innovative choice mechanisms, data security, sensitive data protection, consent for policy changes, and, most importantly, enforcement.

The second plank is monitoring. And that required an investment to ensure compliance with our principles that were established in 2009.

Importantly, the third plank is reporting to ensure that we can provide the necessary information to enforcement bodies.

And then following that is accountability, to ensure that those people who are with our program are absolutely compliant.

We've created the fifth plank, which is enforcement.

Sixth is education, which I will talk about in just a moment.

And then, seventh, and something that we don't always give a lot of credence to: it's evolutionary. To address the point that you made about technology before, this is continuing to evolve. And we have to be on our game to keep up with the pace of changes that are taking place.

As I said at the beginning, I've learned a long time ago not to confuse effort with results, but we have both. The system is operational. It works and works well. Our effectiveness is rapidly growing. And we're structured to evolve to address new challenges.

Let me address some of the progress that we've made. The existing DAA program clearly shows the merits of self-regulation. It is easy for consumers, and it works. As this committee is aware, the cornerstone of the DAA program is our ubiquitous advertising icon, which appears right in the chart over here.

Consumers can click on this icon to access more information in a simple, universal tool for existing choice, as shown here. Through this choice tool, consumers can opt out for all participating companies with a single click or can opt out for specific companies.

All the DAA's self-regulatory principles are backed by robust enforcement mechanisms through the Council of Better Business Bureaus and the Direct Marketing Association.

Several key milestones: The icon is licensed by hundreds of companies and served in over a trillion ad impressions each month. We believe that virtually all U.S. consumers are being exposed to the icon and offered choice.

More than 1 million consumer opt-outs have been registered under the DAA principle since January 2011, which clearly shows

that the program is enabling consumers to exercise their individual choices.

Next, the DAA's release tools have enabled persistent consumer choices in Chrome, Firefox, and Internet Explorer browsers, and these tools respond to concerns that consumers could unintentionally change their preferences by erasing cookies.

And last, we believe that consumers need to be educated about the program. So in January 2012, the DAA launched a major consumer education program, designed by McCann Erickson Worldwide, with a brand new website at *www.YourAdChoices.com* that features educational videos and access to DAA's uniform choice mechanism. This website is averaging over 1 million visitors each month.

We've done a lot. We've accomplished a lot. And a lot of that is embodied in the recognition that we received from the White House and the FTC in a ceremony here in February.

Thank you for inviting me to testify before the Committee. And I look forward to any questions you may have.

[The prepared statement of Mr. Liodice follows:]

PREPARED STATEMENT OF BOB LIODICE, PRESIDENT AND CEO, ASSOCIATION OF NATIONAL ADVERTISERS, INC. ON BEHALF OF THE DIGITAL ADVERTISING ALLIANCE

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

My name is Bob Liodice. I am President and Chief Executive Officer of the Association of National Advertisers ("ANA"). Founded in 1910, ANA's membership includes 457 companies with 10,000 brands that collectively spend over \$250 billion every year in marketing communications and advertising. ANA strives to communicate marketing best practices; lead industry initiatives; influence industry practices; manage industry affairs; and advance, promote, and protect all advertisers and marketers. Today, I am pleased to testify on behalf of the Digital Advertising Alliance ("DAA") and to report to the Committee on the substantial progress of our Self-Regulatory Program.

The DAA is a non-profit organization of leading companies and trade associations including the Association of National Advertisers (ANA), the American Association of Advertising Agencies (4A's), The Direct Marketing Association (DMA), the Interactive Advertising Bureau (IAB), the American Advertising Federation (AAF) and the Network Advertising Initiative (NAI). The DAA was formed to administer and promote the Self-Regulatory Principles for online data collection. The ANA has played a leading role in these efforts since their inception.

My testimony today will describe how the online advertising industry has successfully worked to give consumers transparency about online data collection practices and to create easy, uniform, and effective tools for consumers to control online data collection. DAA participating companies recognize that consumers may have different preferences about online advertising and data collection in general, and want 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 be balanced with consumers' desire for innovative products and services. We believe that industry self-regulation, coupled with consumer education, is the best way to strike this balance. Our standards support both privacy and innovation by enabling consumers to make intentional choices about online data collection and use. Industry self-regulation 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. The business community has a strong incentive to enforce self-regulation against participating companies and I will be explaining how accountability is built into our Self-Regulatory Program.

Benefits of Online Advertising

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. Simply put: the Internet economy and the interactive advertising industry create jobs. 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.¹ There is employment generated by this Internet activity in every single congressional district.²

Advertising fuels the Internet economic engine. The support provided by online advertising is substantial and growing despite the difficult economic times we are presently facing. In 2011, Internet advertising revenues reached a new high of \$31 billion, an impressive 22 percent higher than 2010's full-year number.³

Because of this advertising support, consumers can access a wealth of online resources at low or no cost. Revenues from online advertising facilitate e-commerce and subsidize the cost of content and services that consumers value, such as online newspapers, blogs, social networking sites, mobile applications, e-mail, and phone services. These advertising-supported resources have transformed our daily lives.

Interest-based advertising is an essential form of online advertising. As the Committee knows, interest-based advertising, also called online behavioral advertising ("OBA"), is delivered based on consumer preferences or interests as inferred from data about Internet activities. Consumers are likely to find interest-based advertisements more relevant to them, and advertisers are more likely to attract consumers that want their products and services. Websites also benefit because interest-based advertising garners better responses, allowing websites to earn more revenue—and support more content and services—with fewer advertisements. Advertisers have demonstrated that they believe that interest-based advertising is particularly effective by paying higher rates for such ads.

Interest-based advertising is especially vital for small businesses because it is efficient. Smaller advertisers can stretch their marketing budgets to reach consumers who may be interested in their offerings. Smaller website publishers that cannot afford to employ sales personnel to sell their advertising space, and may be less attractive to large brand-name advertising campaigns, can increase their revenue by featuring advertising that is more relevant to their users. 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.

Recent research highlights the importance of interest-based advertising. In a recent 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. We believe that by creating a worldwide marketplace of relevant and timely advertising, competition and innovation are also enhanced.

In general, the data used for interest-based advertising is not personally identifiable, except when consumers choose to provide personally identifiable information. Nevertheless, the industry recognizes and respects that some consumers may prefer not to receive such advertising or to have data collected about their Web browsing even on an anonymous basis. I will be updating the Committee on our industry's tremendous efforts to make sure that consumers have transparency about online data collection and can exercise control over their preferences—including opting out, if they so desire.

¹Hamilton 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>.

²*Id.* at 53.

³Interactive Advertising Bureau Press Release, "Internet Ad Revenues Hit \$31 Billion in 2011, Historic High Up 22 percent Over 2010 Record-Breaking Numbers" (April 18, 2012) (reporting results of PricewaterhouseCoopers study).

II. Browser-Based Choice Mechanisms

Over the last three and a half years, the DAA has worked with a broad set of stakeholders with significant input from businesses, consumers, and policy makers to develop a program governing the responsible collection and use of Web viewing data. The DAA has championed a balanced approach 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 enjoy the diverse range of websites and services subsidized by relevant advertising. Recognizing that DAA members must also provide consumers with appropriate transparency and choices, industry has spearheaded the self-regulatory process with the support of leading companies.

The DAA's work led to an event in February at the White House where the Chairman of the Federal Trade Commission, the Secretary of Commerce and White House officials publicly praised the DAA's cross-industry initiative. The White House recognized our Self-Regulatory Program as "an example of the value of industry leadership as a critical part of privacy protection going forward."⁴ At that event, the DAA committed to honor browser settings that enable the use of data to continue to benefit consumers and the economy, while at the same time providing consumers with the ability to make their own choices about the collection and use of Web browsing data.

However, a recent technology announcement from Microsoft includes requirements that are inconsistent with the consensus achieved over the appropriate standards for collecting and using Web viewing data. The DAA is concerned that this unilateral decision by one browser maker may ultimately significantly narrow the scope of consumer choices, undercut thriving business models, and reduce the availability and diversity of the Internet products and services that millions of American consumers currently enjoy and use at no charge. The resulting marketplace confusion will not benefit consumers, and will profoundly adversely impact the broad array of advertising-supported services they currently widely use. In fact, as we will now detail, it is only the DAA program that provides a comprehensive set of interest-based privacy choices to consumers, greater consumer education and information, enforcement activities, and true consumer empowerment in the area of OBA privacy.

III. Industry Self-Regulation of Online Data Practices

A. Implementation Update on DAA's Self-Regulatory Principles

The DAA's Self-Regulatory Program for online data collection amply demonstrates the merits of industry self-regulation. The DAA, as noted, is comprised of the six leading advertising and marketing trade associations: the ANA, the 4A's, the DMA, the IAB, the AAF and the NAI. Collectively, these trades represent more than 5,000 U.S. corporations across the full spectrum of businesses that have shaped and participate in today's media landscape.

Our trade associations, along with leading companies, released the Self-Regulatory Principles for Online Behavioral Advertising ("OBA Principles")⁵ in July 2009. The OBA Principles are a set of consumer-friendly standards that apply across the entire online advertising ecosystem. They address all of the key elements called for by the Federal Trade Commission in its 2009 Staff Report on interest-based advertising,⁶ namely: (1) consumer education, (2) enhanced notice of data practices, (3) innovative choice mechanisms, (4) data security, (5) sensitive data protection, (6) consent for retroactive material policy changes, and (7) enforcement. The Principles are designed to apply broadly to the diverse set of actors that work independently to deliver relevant advertising intended to enrich the consumer online experience. Together, these Principles aim to increase consumers' trust and confidence in how information is gathered from them online and how it is used to deliver advertisements based on their interests. Let me briefly review how the Principles work from a consumer's perspective:

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 Self-Regulatory Principles for Online Behavioral Advertising (July 2009), available at <http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>.

⁶ Federal Trade Commission Staff Report, *Self-Regulatory Principles for Online Behavioral Advertising* (February 2009), available at <http://www.ftc.gov/os/2009/02/P085400behavadvreport.pdf>.

- First, an advertisement covered by the Principles is identified with the distinctive Advertising Option Icon (“Icon”) (Attachment 1), which appears in the advertisement right where the consumer will notice it. Launched in 2010, this Icon is now a familiar sight across the Internet as a means for uniformly providing consumers with transparency and control.
- Clicking the Icon brings up a brief statement about online behavioral advertising, with a link to more information and opt-out choices.
- Interested consumers can click this link to visit AboutAds.info, an industry-sponsored website that provides consumer education and, most importantly, consumer choice. Through this mechanism, a consumer can learn, in real time, which participating companies are currently tailoring advertising to their browser.
- Consumers can elect to opt out from all participating companies through a prominent, single-click button or select individually the companies they want to tailor advertising to their browser. This approach empowers consumers, if they wish, to make an informed and intentional choice to stop collection of information that will provide them with relevant tailored advertising.

Over the past year, the DAA has achieved several significant milestones in its implementation of the Self-Regulatory Program:

- The Icon is being served in over one trillion ad impressions per month.
- We estimate that the DAA program now covers over 90 percent of the online behavioral advertising being delivered, based on the participation of the top 15 U.S. ad networks.
- More than 100 companies are providing choice to consumers via the DAA’s universal choice mechanism.
- More than one million consumer opt outs have been registered under the DAA Principles since January 2011.
- Participation in the Program has quadrupled over the last year. Hundreds of companies are licensed to use the Icon (including leading global advertisers like American Express, AT&T, Disney, General Motors and Kraft Foods). Not only is the DAA working directly with large publishers, it has also forged innovative partnerships to enable small business publishers to display the Icon on their websites for free.
- The DAA’s AboutAds website (www.aboutads.info) provides consumers with information about online advertising and provides an easy-to-use opt out mechanism. There have been over 8 million page views at AboutAds.info since its inception in the fall of 2010, and traffic to the website has increased in recent months as the Icon is more widely adopted.
- In November 2011, the CBBB announced its first enforcement cases. In June 2012, the CBBB announced another round of enforcement cases.
- In December 2011, the DAA began to offer tools that enable persistent consumer opt outs in Chrome and Firefox browsers. The DAA released a persistence tool for users of Internet Explorer in March 2012. These tools respond to concerns that consumers could unintentionally change their opt-out preferences by erasing cookies from their browsers.
- In January 2012, the DAA launched an education campaign to inform consumers about interest-based advertising and how to take greater control of their online privacy. This multi-phase online campaign, designed by McCann Erickson Worldwide, includes banner advertising that directs consumers to the DAA’s Icon and links to a new, informational website, www.youradchoices.com, which features three educational videos and a user-friendly consumer choice mechanism. The website has already had over 7.6 million visitors since its launch. With an average of more than *a million visitors each month*, this is a very promising start. To continue driving traffic to this website, the DAA has already secured over 3 billion donated ad impressions from companies participating in the Program.

B. Evolution of the Self-Regulatory Principles

Alongside these implementation efforts, the Self-Regulatory Principles have continued to evolve in response to emerging policy issues. In November 2011, the DAA extended the OBA Principles significantly with the release of the Self-Regulatory Principles for Multi-Site Data (“MSD Principles”). The MSD Principles establish comprehensive self-regulatory standards governing the collection and use of “multi-site data,” defined as data collected from a particular computer or device regarding

Web viewing over time and across non-affiliated websites. This principle applies control beyond opting consumers out of receiving targeted ads, and empowers consumers to control the collection and use of Web viewing data for other purposes.

The MSD Principles strike an appropriate balance by targeting specific concerns while maintaining the flow of information for legitimate uses. For instance, some policymakers have raised concerns that data collected for advertising purposes could be used as a basis for employment, credit, health care treatment, or insurance eligibility decisions. In fact, these are hypothetical concerns that do not reflect actual business practices. Nevertheless, industry has stepped forward to address these concerns by expanding our guidelines via the MSD Principles to clarify and ensure that such practices are prohibited and will never occur. This prohibition will help to ensure that consumers' browsing histories will not be used against them when applying for a mortgage, job, or insurance, or when seeking health care.

The DAA's record of success demonstrates why industry self-regulation is so successful. The business community is in the best position to craft standards, like the MSD Principles, that respond to specific, articulated concerns while allowing beneficial uses of data to continue. As recognized by the Federal Trade Commission, limitations on collection, often misleadingly referred to as "Do Not Track", should not be a flat restriction on all collection of all data in all contexts.⁷ We agree. We designed the MSD Principles to provide consumers with control with respect to their Web viewing data 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 and to the consumer online experience.

Data collected pursuant to the exceptions listed above provides a grand array of consumer benefits. Data supports robust consumer safety mechanisms, ranging from fraud detection in financial services to prevention of online threats. In addition, the use of data leads to continued innovation, which has the potential to offer consumers untold benefits. For example, data can be leveraged to provide web-enabled smart grid services that enable consumers to obtain actionable information that saves them money and lowers energy consumption. The MSD Principles also allow companies to use data for market research and product development, so that we can keep building tomorrow's Internet. Market research and product development actively rely on consumer data, not to market directly back to consumers, but to gain broad insight about consumers' collective preferences and needs so that businesses can better serve their customers.

We expect that the DAA Self-Regulatory Program will continue to adapt over time to respond to changes in technology and consumer concerns. Currently, the DAA has convened a subcommittee of its Principles and Communications Advisory Committee that is working to extend the Principles to the mobile ecosystem. This effort has already made significant progress with the active participation of stakeholders representing all major elements of the mobile ecosystem.

C. Commitment to Accountability

For the past 40 years, the advertising industry has distinguished itself through its self-regulatory system 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 our Self-Regulatory Principles are backed by the robust enforcement programs administered by the Council of Better Business Bureaus ("CBBB") and the DMA.

The CBBB accountability program builds on the successful track records of the National Advertising Division, operating since 1971; the Children's Advertising Review Unit, operating since 1974; and the Electronic Retailing Self-Regulation Program, operating since 2004. These programs feature 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 that do not or choose not to participate are referred to the appropriate government agency for further review.

The CBBB administers its Interest-Based Advertising Accountability Program under the Advertising Self-Regulatory Council's ("ASRC") self-regulatory procedures. Like other ASRC programs, the CBBB Accountability Program generates cases

⁷ FTC Report at 53, available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>.

through monitoring, consumer complaints and review of news stories and technical reports from academics and advocacy groups. The CBBB Accountability Program receives weekly reports on technical monitoring of various compliance requirements of the Principles. The CBBB Accountability Program's technical staff analyzes this data, independently performs further research and, where there is a potential compliance issue, initiates formal inquiries.

The CBBB's Accountability Program has brought over a dozen cases since November 2011, and has the enviable track record of 100 percent industry compliance. 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.

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 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 Operating 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 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 with the Committees 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 illustrate how effectively self-regulation is working and its many benefits, including its ability to evolve to meet new challenges.

D. 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 online advertising practices. We appreciate the positive recognition of the White House and the Federal Trade Commission for our efforts. We believe that 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.

Based on the DAA's commitment to advancing industry self-regulation, we are concerned about some of the proposals put forward by the Administration and the Federal Trade Commission in their respective consumer data privacy frameworks.⁸ In particular, both the Administration and the Federal Trade Commission have called for comprehensive legislation in the area of consumer data privacy. The DAA does not believe that such new legislation is needed at this time. There has been no demonstration that legislation is necessary, nor has there been any evaluation of the likely impact that legislation would have on this leading area of American job creation. The DAA is 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.

Formal rules can also serve as a disincentive to the marketplace to innovate in the area of privacy. Companies are increasingly offering consumers new privacy features and tools such as sophisticated preference managers, persistent opt outs, universal choice mechanisms, and shortened data retention policies. These developments demonstrate that companies are responsive to consumers and that companies are focusing on privacy as a means to distinguish themselves in the marketplace. The DAA believes that this impressive competition and innovation should be encouraged. New laws or rules could impede future developments or discourage companies from continuing to compete over privacy features. We believe that the DAA program, which industry has already invested millions of dollars to develop, is clearly one of the most successful and fastest-developing self-regulatory systems in U.S. history and should be allowed to continue to flourish without unneeded governmental intervention or legislation at this time.

Thank you again for inviting me to testify before the Committee. I look forward to answering any questions the Committee may have.

ATTACHMENT 1: ADVERTISING OPTION ICON



⁸The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012); Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012).

Senator KLOBUCHAR. Mr. Fowler?

**STATEMENT OF ALEX FOWLER, CHIEF PRIVACY OFFICER,
MOZILLA**

Mr. FOWLER. Thank you, Chairman Rockefeller and distinguished members of the Committee, for the opportunity to testify today.

I am Alex Fowler. I oversee privacy for Mozilla and lead our work on Internet-related policy issues.

Mozilla is an independent global community of people who have been working together since 1998 to build a better Internet. We're dedicated to promoting openness, innovation, and opportunity online.

Mozilla does not own or operate a search or advertising business. Our most popular product is the Firefox Web browser used by more than 500 million people.

As a core principle, we believe the Internet is a public resource that must be improved and protected. We also believe enabling and maintaining an economic ecosystem is an important component of a robust and healthy Internet.

However, we do not believe that the commercial imperative and choice and control are mutually exclusive. They can and must coexist through a combination of technical capabilities and user-centric business and data practices.

The public is increasingly uneasy about the extent to which their online lives are invisibly profiled, analyzed, packaged, sold, and re-used to target advertising content and services. This is leading a growing number of users to want to understand and take measures to control the collection and use of data about them.

We have an opportunity to work together to develop innovative mechanisms that address real business challenges and empower people to engage in an ecosystem that's both sustainable and fair.

Mr. Chairman, the remainder of my statement briefly touches on industry self-regulation, our "do not track" feature in Firefox, and the ability for industry to provide meaningful privacy choices.

Regarding self-regulation, it's unclear whether industry self-regulation by itself is a viable way to allow users to understand and control data collected and used about them.

Consider the following three examples.

First, industry self-regulation focused on notice and choice as a way to inform people to make decisions about which sites and services meet their privacy values. Unfortunately, as I outline in my written statement, privacy policies have not worked to inform or empower users.

Seals and trust marks are a second example of a self-regulatory effort to improve transparency online. Research has shown that users don't know what trust marks mean, and they don't help them distinguish between data practices of different businesses.

Last, we commend the DAA for its considerable work bringing together the online advertising industry into its self-regulatory initiative. While its Ad Choices icon program is an important effort, research has shown it still remains unclear to users. Many believe that clicking on the icon will trigger pop-up ads or invite more ad-

vertising. And many more think it's related to purchasing advertising space.

The ad industry's own research shows the number of users who use the icon is below four-hundredths of a percent.

If the consumer wants to opt out, she must first see the icon, understand it, and then click on it, and then go to a site that offers the chance to find and set opt-out cookies.

Opt-out cookies are not persistent and can easily be deleted by accident or by following recommended security practices. And different companies interpret their opt-outs differently, rendering them ambiguous in the end.

My point here is that without input and commitments from stakeholders outside of any one industry group, self-regulatory efforts that brought us policy, seals, and icons have not established public trust and engagement and still invite regulation and all the risks of unintended consequences that go with it.

Not all hope is lost from our perspective. We're seeing an important shift in self-regulatory efforts away from closed-door, industry-led efforts to open multi-stakeholder approaches. By broadening self-regulation into forums that involve all relevant parties, we can hopefully address past misses and avoid the need for regulation.

We need to give this approach time to mature. But in the event that multi-stakeholder processes are unsuccessful, then it may be necessary to explore regulatory measures.

Turning my attention to the current state of the "do not track" feature in Firefox, Mozilla was the first browser to implement "do not track" in March of last year. "Do not track" is a signal sent and transmitted by the user via the browser to websites. Nine percent of our users have turned on "do not track" in Firefox and 18 percent have it on in our mobile browser. Numerous companies already honor "do not track," including Twitter, the Associated Press, Jumtap, and more are on the way.

"Do not track" does not enforce, break, control, disable, or impair any online tracking or personalization technology. To make it effective, recipients must breathe life into the signal by honoring the user's intent.

The crucial questions, therefore, become what does the user intend by the "do not track" signal? What should a site do when it receives a signal? These questions are the subject of a consensus-driven, multi-stakeholder effort currently underway at the World Wide Web Consortium.

The W3C's tracking protection group includes, among others, over 35 leading advertisers, publishers, and technology companies. While the group has agreement on most of the technical requirements, there are still two competing views on what "do not track" should mean.

One is that "do not track" means literally what it says—no third-party tracking of users, whether it's for targeted ads or other purposes. The other is that "do not track" means no targeting, but allows some tracking and collection. Currently, the working group is pursuing a middle ground, so stay tuned.

Last—I only have a little time left—I wanted to share a quick point about the value of privacy tools. As long as there are incentives for companies to collect lots of user information, scale-up, and

then bolt on privacy protections after the fact, we are unlikely to see users satisfied with the promise of privacy tools.

Instead, privacy by design is a crucial concept for the Committee to champion. Privacy by design is an approach that addresses user data and privacy implications from the outset. And I'd be pleased to come back another time to share more about this approach and how it works in the context of the technical marketplace.

In conclusion, Mozilla strives to ensure privacy and security innovations support consumers in their everyday activities online. But the key for us, and the key for users on the Internet, is that it's informed and reasonable choice enabled through transparency.

Thank you, again, for the opportunity to participate today.
[The prepared statement of Mr. Fowler follows:]

PREPARED STATEMENT OF ALEX FOWLER, CHIEF PRIVACY OFFICER, MOZILLA

Chairman Rockefeller, Ranking Member Hutchison, and Members of the Committee, thank you for the opportunity to testify today on the need for privacy protections, the status of self-regulation, and Do Not Track.

I am Alex Fowler; I oversee privacy for Mozilla and lead our work on Internet-related policy issues. I've spent the last twenty years working on privacy as a technology policy analyst here in Washington, a consumer advocate, in a start-up developing privacy software tools and as a Big 4 consultant advising leading banks, healthcare and technology companies.

Mozilla is a global community of people who have been working together since 1998 to build a better Internet.¹ As an independent organization, we are dedicated to promoting openness, innovation, and opportunity online.² Mozilla does not own or operate a search or advertising business. Our mission is to pursue the interests of users, developers and the Web as a whole. Mozilla and its contributors advance our goals by making free, open source technologies for consumers and developers that reflect these values. Our most popular product is the Firefox Web browser used by more than 500 million people worldwide. As a core principle, we believe that the Internet, as the most significant social and technological development of our time, is a precious public resource that must be improved and protected.

We also believe that commerce is a vital and beneficial Internet activity. Enabling and maintaining economic ecosystems online is an important component of a robust and healthy Internet. However, we do not believe that the commercial imperative and user choice/control are mutually exclusive. They can and must coexist through a combination of technical capabilities and user-centric business and data practices.

As a privacy professional, I see the Web ecosystem as increasingly relying on a *guesswork* economy. Many of our best and brightest engineering minds are hard at work on new technologies to predict and deliver what the user wants at just the right moment. They use content delivery networks, profiling, tracking, social graphs, and data analytics to grasp at tiny clues about us and piece them together to *guess* who we are, where we live, and what we like or want. Just recently it was reported that Orbitz presents higher priced hotels based in part on the operating system of the user. Apparently Mac users spend more on hotels, so Orbitz lists higher-priced rooms for them.³ These results represent impressive feats of business and technological prowess, and the industry reports record growth,⁴ yet they have not led to a Web ecosystem where the user is an active and informed participant.

The public is increasingly uneasy about the extent to which their online lives are invisibly profiled, analyzed, packaged, sold, and reused to personalize advertising,

¹ See <http://www.mozilla.org> for more information about Mozilla, its mission and many initiatives.

² The Mozilla Manifesto is available at <http://www.mozilla.org/about/manifesto.en.html>.

³ Mattioli, Dana. On Orbitz, Mac Users Steered to Pricier Hotels. *The Wall Street Journal* (June 26, 2012). <<http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html>>.

⁴ Ha, Lyons. Internet Ad Revenue Reaches \$31B In 2011, Mobile Up 149 Percent (IAB Report). *TechCrunch* (April 18, 2012). <<http://techcrunch.com/2012/04/18/iab-revenue-report-2011/>>.

content and services.⁵ ⁶ This unease leads many users to want to understand and control the collection and use of data about them. We see new online privacy protecting services launching every month and privacy browser add-ons are growing in popularity. Many of the most popular approaches disrupt and are in direct conflict with common business models. Some of the tools block interactions between users and sites, third party advertising or data brokers.⁷ ⁸ This pattern has been likened to an “arms race,” with industry and Web users locked in opposition to one another.

We have an opportunity to break this cycle by working together with industry to develop innovative mechanisms that address real business and technical challenges and empower people to engage in an online ecosystem that’s both sustainable and fair.

Mr. Chairman, the remainder of my statement focuses on the three areas you requested in your invitation on the current state of: industry self-regulation; our Do Not Track feature in Firefox; and the ability for industry to provide meaningful privacy tools.

The Current State of Industry Self-Regulation

It is unclear whether industry self-regulation, by itself, is a viable way to allow users to manage and control data collected and used about them by third parties. Any process that does not represent the users’ interest is unlikely to be successful. Outside of the processes undertaken many years ago to develop fair information practices in the 1980s⁹ and Website privacy policies in the 1990s,¹⁰ we have tried to address current privacy issues either through narrowly construed, industry-led efforts or a patchwork of state, Federal and international privacy laws.

In particular, industry promoted the notice and choice model as a way to harness the power of the free market to provide the transparency needed for people to make individual decisions about which sites and services meet their privacy needs. This is an important goal: it is clear that different people have very different privacy preferences, so ideally they would have the tools they need to make informed choices for themselves and their families. Unfortunately, the notice and choice approach has some flaws, which have led to failure in the market. Under our current model, choice was supposed to be enabled by consumers using the sites, services and applications with the privacy notices that best reflect their values. Yet privacy notices are a mix of legal and technical jargon, impenetrable to all but the most sophisticated. Privacy policies are not going away, however. They are required under California law. We continue to see new best practices emerge, and the process of developing privacy notices for mobile may lead to some new innovations. But the original idea that people would read multiple privacy policies to decide which sites to visit or buy from has not happened. Today, the privacy practices are indistinguishable across sites. Privacy policies have not worked to inform or empower users.

Seals and trust marks are another form of notice that have only partially improved privacy online. The Better Business Bureau (BBB) offers a seal program.¹¹ TRUSTe, which does so, too, has weathered some rough years, with findings that the business practices of TRUSTe customers are less privacy protective than average.¹² BBB’s and TRUSTe’s work has been valuable in helping companies clarify their privacy practices. However, seals are an approach by business for business that has not measured up to the high hopes of empowering users’ online privacy choices.

⁵ TRUSTe. 2008 study: Consumer attitudes about behavioral targeting. (March 2008). <http://danskprivacynet.files.wordpress.com/2009/02/truste2008_tns_bt_study_summary1.pdf>.

⁶ Turov, J. et al., Americans Reject Tailored Advertising and Three Activities That Enable It (September 29, 2009). <<http://ssrn.com/abstract=1478214>>.

⁷ Lyons, Sean. Privacy Concerns Spark Innovations Among Companies, Startups. *International Association of Privacy Professionals* (May 11, 2012). <https://www.privacyassociation.org/publications/2012_05_10_privacy_concerns_spark_innovations_among_companies_startups>.

⁸ Several of the most popular add-ons for Firefox are aimed at blocking advertising and tracking, including Adblock Plus, Ghostery and NoScript. Adblock Plus alone has been downloaded 160 million times, and has almost 14 million daily users.

⁹ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *Organisation for Economic Co-operation and Development (OECD)* <http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html>.

¹⁰ Privacy Online: A Report to Congress. *Federal Trade Commission* (June 1998). <<http://www.ftc.gov/reports/privacy3/toc.shtml>>.

¹¹ BBB Accredited Business Seal for the Web <<http://www.bbb.org/us/bbb-online-business/>>.

¹² Vila, T., Greenstadt, R., and Molnar, D. Why we can’t be bothered to read privacy policies models of privacy economics as a lemons market. In *ICEC 2003 Proceedings of the 5th International Conference on Electronic Commerce* (2003) Pages 403–407.

One of the more recent and visible industry self-regulation efforts has focused on online behavioral advertising.¹³ We join many others in commending the Digital Advertising Alliance (DAA) for its work to bring together the online advertising industry, and the growth of its ad-based icon. While the icon program is a good step, it suffers from material implementation hurdles¹⁴ and technological limitations that cause it to fall short.¹⁵ Despite the advertising industry's extensive expertise on succinctly communicating complex messages, the advertising option icon is incredibly unclear to users.¹⁶ Many believe that clicking on it will trigger pop-up ads or invite more advertising, and many more expect that it is related to purchasing advertising space.¹⁷ According to the industry's own research, the number of users who use the icon is low: 0.0035 percent click, and only 1 in 20 of those actually opt out.¹⁸

Since the icon is just a gateway to the industry's current cookie-based opt-outs, it suffers from drawbacks and fragility. One significant challenge is that the mechanism is not persistent because it is cookie-based. Users who routinely clear their cookies for security or to limit tracking also inadvertently remove their opt-out cookies under the current industry self-regulatory program. The Ad Choice interface also does not work on all platforms, leaving Mac users without a way to opt-out. Opt-outs are also ambiguous: different companies interpret their opt-out cookies differently. Some stop collecting info about users, while others continue collecting info, but stop customizing content and advertising, making their data collection practices invisible to users. Finally, opt-out cookies are not a scalable option for users. Even if a user requests opt-out cookies for all advertisers today, that choice is not extended for new advertising companies tomorrow. With this mechanism, users have to keep a vigilant eye out for new companies.

My primary point here is that without input and commitments from stakeholders outside of the ad industry, industry efforts like seals and the one led by DAA will remain insufficient. They do not establish the public trust and engagement needed for success. Such options invite stronger measures like regulation and all the risks of unintended consequences that go with it.

We are seeing an important shift in self-regulation away from closed-door, industry-led efforts to multi-stakeholder approaches where industry, users, academics, service providers, browser providers and consumer advocates come together to develop holistic frameworks and standards for the protection of privacy.¹⁹ This is different from what has happened in the past where a single industry adopted its own unilateral scheme. It is precisely this broadening of self-regulation to deliberately involve all relevant stakeholders, combined with FTC and Administration support, that will increase chances of success and potentially avoid the need for regulation.

Many of these new discussions are occurring in the World Wide Web Consortium (W3C) Tracking Protection Working Group.²⁰ Despite dialogue that could sometimes be characterized as atypically aggressive (for standards working groups) and even personal at times, the process has been open, transparent, and inclusive. The group consists of over 35 leading companies,²¹ including advertisers, publishers, and Internet companies, together with consumer advocates, industry trade associations, academics from the U.S. and Europe, and independent experts. The discussions have been productive so far. The group is committed to following a consensus-based approach to achieve a protocol that everyone can live with.

¹³Kaye, Kate. Icon War? Two Behavioral Ad Notice Icons Could Confuse. *ClickZ* (January, 2010). <<http://www.clickz.com/3636315>>

¹⁴For example, "These results suggest that the icons and tagline are failing to effectively communicate their purpose to users" in Cranor, Lorrie F. Can Users Control Online Behavioral Advertising Effectively? *Security and Privacy Economics* (March/April 2012).

¹⁵Five technical hurdles described in Mayer, Jonathan R. and Mitchell, John C. Third-Party Web Tracking: Policy and Technology. In *IEEE Symposium on Security and Privacy* (2012), page 422.

¹⁶Leon, 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>

¹⁷*Ibid.*

¹⁸Consumer Interactions with Ad Notice. *Evidon* (2011). <http://cdn.betteradvertising.com/misc/consumer%20impact%20of%20ad%20notice%2011_11.pdf>

¹⁹See the NTIA's Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct <<http://www.ntia.doc.gov/federal-register-notice/2012/multistakeholder-process-develop-consumer-dataprivacy-codes-conduct>>, as well as Mozilla's comments to the National Technology and Information Administration, <http://www.ntia.doc.gov/files/ntia/mozilla_comments_040212_final.pdf>.

²⁰See the Tracking Protection Working Group page <<http://www.w3.org/2011/tracking-protection/>>.

²¹See the Tracking Protection Working Group participants list <<http://www.w3.org/2000/09/dbwg/details?group=49311&public=1>>.

As a member of the W3C group, we remain optimistic that the process will produce a meaningful standard that ultimately provides people with more choice and control related to targeted ads and user tracking by 3rd parties. Together with the Administration's multi-stakeholder process to develop a code of conduct that promotes transparent disclosures to consumers concerning mobile apps' treatment of personal data,²² we are hopeful that a more representative cadre of concerns will produce effective self-regulatory practices without the need for legislation. However in the event that an open, multi-stakeholder process is not successful it may be necessary to explore regulatory measures.

The Current State of the Do Not Track Feature in Firefox

Mozilla was the first browser to implement Do Not Track in March 2011 inspired by innovations from privacy and security researchers Christopher Soghoian and Dan Kaminsky.²³ When we first announced it, the ad industry was critical and Microsoft publicly ridiculed the feature,²⁴ but the FTC strongly supported it and our users wanted it. Today 9 percent of our users have turned on DNT in the desktop version of Firefox and 18 percent have turned on DNT in the mobile version. Microsoft has announced it will ship IE with DNT turned on by default in Internet Explorer 10, and soon it will be possible for users to turn on DNT in all major browsers. Numerous companies already honor the DNT signal, including social networks like Twitter, publishers like the Associated Press, and mobile advertisers like Jumtapp, AdTruth, and more are on the way. We are building DNT into Thunderbird, our e-mail client, and our mobile operating system, code named Boot2Gecko, where the user's DNT signal will be available to every app on the device. In addition to our engineering contributions, a Mozilla engineer submitted the first standards proposal for Do Not Track, and a member of our community is co-chair of the W3C standards effort.

Do Not Track is a simple, digital signal sent by the user via the browser to websites. As a signal, Do Not Track does not enforce, break, control, disable or impair any online tracking or personalization technology. It is a signal that is sent along with Internet traffic, indicating that the user sitting behind the keyboard would like their privacy to be respected more strongly than might otherwise be the case. To make it effective, the recipients—websites and ad networks—must breathe life into the signal by honoring the user's intent. The crucial questions therefore become:

- What does the user intend by the DNT signal?
- What should a site do when it receives this signal?

These questions are the subject of a consensus driven multi-stakeholder effort currently underway at the W3C, as I mentioned a moment ago. The Do Not Track working group is chartered²⁵ to develop a robust self-regulatory framework for user choice and control on the Web. While the group has agreement on most of the technical requirements of the protocol, there are still two competing views on what DNT should mean. One is that DNT means what it says, no 3rd party tracking of users whether its targeted ads or for other purposes. The other position is that DNT means no targeting, but tracking and collection are still acceptable. Currently, the working group is perusing a middle ground. The participants are collaborating in an open process to determine both the technical and compliance requirements for a Do Not Track system.

No single party can address privacy related to personalization and tracking on their own. The ecosystem is so diverse and specialized that there is no one entity who knows exactly which data is going where. Publishers can't predict which ads will show up on their sites after an auction. Advertisers can't predict which sites their ads will land upon. There is no single place for users to go to find out: "Where did my data end up?"

²²United States Department of Commerce. First Privacy Multistakeholder Meeting: July 12, 2012. *National Telecommunications & Information Administration* (June 15, 2012). <<http://www.ntia.doc.gov/headlines/2012/first-privacy-multistakeholder-meeting-july-12-2012>>

²³Soghoian, C. The History of the Do Not Track Header (January 21, 2011). <<http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html>>

²⁴Mullin, J. Microsoft: It's Naive To Trust Tracking Sites To Obey Anti-Tracking Orders. *paidContent* (February 10, 2011). <<http://paidcontent.org/2011/02/10/419-microsoft-its-naive-to-trust-tracking-sites-to-obeyanti-tracking-signa/>>

²⁵See the Tracking Protection Working Group charter <<http://www.w3.org/2011/tracking-protection/charter>>.

There is likewise no party that can build a complete solution on their own. Browsers have many options to provide strong choices and controls to their users.²⁶ However, browsers' technical measures risk being overly blunt, and disabling some features as well as protecting against privacy threats. As noted earlier, the cookie-based opt-outs provided by advertisers and analytics engines are ambiguous, do not scale, are not persistent, and do not truly address many users' privacy concerns. Advertising self-regulatory groups do not include social networks like Facebook or Twitter. Users are concerned about being followed across the Web whether or not there is advertising involved. In contrast, DNT sends a signal with every request—whether to a publisher, advertiser, or social network—with no need to worry about new businesses or new business models. DNT is a protocol that can address users' concerns and augment existing systems and initiatives.

Research shows that some users want personalization, many favor privacy, but the majority will make up their minds based on whether they see value to them or not.²⁷ Tracking, in and of itself, is not necessarily a problem when users can participate in the decision and understand how they benefit. Issues arise when users are unable to control their browsing experience, or worse, loose confidence that they are an active participant in how information about them is collected, used and shared among sites and apps.

DNT is narrowly-tailored to give users choice and control in a persistent, accessible way without preventing the customization and valuable advertising that powers our rapidly-growing Web economy. Innovative and transparent ways for users to obtain personalized content in a manner that respects user choice are both desirable and good for the Web. The DNT standard also envisions ways for users to request personalization and offers new opportunities for compelling user engagement and trusted relationships. In addition, unlike the Do Not Call list and the Ad Choices program, DNT is free to advertisers. There are no annual subscriptions to lists or fees to use icons. There is no cost to the taxpayer.

It will take more time for stakeholders to agree and best practices to emerge, as Do Not Track is a unique multi-party, client-server approach to addressing privacy. We will also need a period to educate users and listen to their feedback so that we can match the DNT system with their expectations and produce a compelling experience.

A DNT signal is not the beginning or the end of the privacy conversation, nor the only way user data is protected. Websites, service providers, ad networks play an essential role, and have much to offer by their own data practices and policies.

III. Industry's Ability to Provide Users With Tools to Adequately Protect Their Personal Information Online

Privacy by Design is a crucial concept for the Committee to champion. As long as the Web economy provides incentives for companies to start collecting lots of user information, scale up, and then bolt on privacy protections after the fact, we are unlikely to see users satisfied with the promise of the available privacy tools and services. Privacy by design is an approach that addresses user data and privacy implications of new products and services from the outset. There are many successful examples of traditional and nontraditional companies that have built fully scalable and commercially viable products and services on the Web based on this approach. For example, one Web search engine never collects any logs²⁸ that can be associated with a particular person while still capturing all the information they need to build a powerful and viable service. And the GMAT switched to a less-intrusive method of verifying test-takers' identities as it balanced important business needs with student privacy concerns.²⁹

For years, the Internet worked on the model that anyone on the same mainframe was a co-worker, not a threat, and networking meant sending text files over modems. Worms, malware, and phishing attacks highlighted how much had changed in a short time. Since then, security has become a priority for companies. Microsoft famously retooled their operating system and software development process to address security problems. Now we are finding a similar crisis with the privacy dimensions of user choice and control. It is not just users who lack a complete

²⁶Lowenthal, T. Browser Vendors: fight for your users (April 29, 2011). <http://www.w3.org/2011/trackprivacy/papers/lowenthal_position-paper.pdf>.

²⁷McDonald, Aleecia M. and Cranor, Lorrie F. Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising. In *38th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference)* (October 2, 2010).

²⁸DuckDuckGo Privacy. <<https://duckduckgo.com/privacy.html>>.

²⁹Hill, Kashmir. Why 'Privacy By Design' Is The New Corporate Hotness. *Forbes* (July 28, 2011). <<http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporatehotness/>>

privacy picture. Companies are starting to realize they do not know what cookies they set, how they use data, and where it flows internally or externally. As an industry, we are going to need efforts to figure that out, plus ensure we design with privacy in mind.

We often talk about “personal information,” but we are beginning to understand that even data that does not include someone’s name, e-mail address, or social security number can have real privacy impacts. For example, Netflix viewing history—which on its face appears not to be personally identifiable at all—has been used to identify specific people’s sexual orientation and medical conditions.³⁰ The truth is that it’s incredibly hard to predict how several pieces of apparently unrelated information can be combined to produce uncomfortably personal insights. We already have the technology to implement much of the Web ecosystem while leaving users in control of even this sort of information.

In conclusion, data sharing, control, security, and management are critical consideration for Mozilla. It is embraced in the products and services we create, and derives from a core belief that people should have the ability to maintain control over their entire Web experience, including how their information is collected, used and shared with other parties. We strive to ensure privacy and security innovations support consumers in their everyday activities whether they are sharing information, conducting commercial transactions, engaging in social activities, or browsing the Web, but the key is informed and reasonable choice enabled by transparency. Mozilla is pleased to be part of a vibrant user data landscape that is rapidly evolving to a future that will give people more choice and more control to participate fully in their online experience.

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

Senator KLOBUCHAR. Thank you very much, Mr. Fowler.
Mr. Swire?

**STATEMENT OF PETER SWIRE, C. WILLIAM O’NEILL
PROFESSOR OF LAW, THE OHIO STATE UNIVERSITY**

Mr. SWIRE. Thank you, Madam Chair, Senator Rockefeller, and other distinguished members of the Committee. It’s a pleasure to testify here today on “The Need for Privacy Protections: Is Industry Self-Regulation Adequate?”

I come here as a law professor and also as a former government official. I started working on privacy and self-regulation in the mid-1990s, and was Chief Counselor for Privacy under President Clinton. I was the White House lead for the HIPAA and Gramm-Leach-Bliley medical rules, and have worked on numerous self-regulatory rules, in the room negotiating these.

So it’s with that background that the Committee asked me to talk about this history of what we’ve seen here, and, specifically, to look at the DAA’s exceptions in some of their things that we’ll get to. And that’s what I’ll focus my remarks on.

My testimony has four sections. The first is when does privacy and self-regulation work? And the big theme here is, when you look at it, is that industry works a lot harder at this when government is paying attention. When industry thinks the government is not focused on it, the temptation is to say, “You know, we could do this, but we don’t have to. And it’s hard, and it’s a lot of work, and it might cost us money. We’re really not sure we want to do that.”

But when you’re paying attention, when the White House is paying attention, the FTC is paying attention, the conversation is entirely different. The conversation then is, “You know, if we don’t do

³⁰Narayanan, A. and V. Shmatikov. Robust De-anonymization of Large Sparse Datasets (2008). <http://www.cs.utexas.edu/~#x0303;shmat/shmat_oak08netflix.pdf>

it, they're going to do it for us. So we have to come up with something good."

And I think we saw that in the 1990s when industry stepped forward in a lot of ways. We're seeing industry digging in and doing a lot of things right now.

But in between, there was a period when the attention wasn't here. And so the second point is, what have we seen from the history?

The history is, in the late 1990s, as the first Internet was ramping up, a lot of people were paying attention to privacy. It was the dot-com boom. Privacy policies were going up on websites.

And then after 2000, things changed. The attacks of 2001 made privacy not nearly the same issue. A lot of other things were changing. So we have studies by academics on what happened to self-regulation after 2001.

Most of the self-regulatory organizations in privacy disappeared. The others shrank drastically. That's the history.

Now there are some reasons for that. Part of it is the Internet economy changed. So the advertising economy went down and effort went down.

But if you look at the history, the history is, the pressure came off, and self-regulation dismantled to a very large extent.

Now, some of the self-regulatory things continued. The ones that did tended to be when they were working together with government efforts, like under the Children's Online Privacy Protection and CAN-SPAM.

My third point, after the sort of theory and history is, what do we see right now with the Digital Advertising Alliance and, specifically, the exceptions for market research and product development?

The testimony goes through these in detail, looks at these market research and product development exceptions. They're part of something in the report of the DAA that are called limitations on collection of multi-site data. The problem is, when you read them, there is no limitations on collection that I think are enforceable by the FTC.

If a company makes these promises, I can't figure out what they actually could be held to. And I came to DAA and talked to counsel in preparation for this hearing. We went through the language. And after that conversation, the DAA counsel specifically said that they are now willing to meet and discuss on market research and product development, and see what concrete changes can be made here.

So industry once again is saying, "We're going to work harder on this." And I think this hearing helped to prompt attention to that, and I thank the Committee for that.

Briefly, the fourth point before I conclude is, there is an area for win/win when it comes to the Internet and privacy, how to build that. And that's the area of anonymization or de-identification.

I think what happens here is, if we can do a better technical job of de-identifying, so that your name or your devices aren't linked to what you're doing, then that way we can use the data intensively, and we can have privacy protections.

I'm involved in a research project on that with the Future of Privacy Forum. Some of the proposed statutes talk about this issue of anonymization. I think it's an area for future work.

So, in summary, we're in a period right now where there's strong interest in this from Congress, from the press, the White House, the Federal Trade Commission, on "do not track" and related issues. There are many intelligent people of good will working hard on these issues.

This is a time when it is time to lock in some of the progress that's being made. Issues come and go. This is the time when this issue is in people's attention.

I think this hearing and the effort you're doing can really help to make progress for better privacy and also for a better Internet going forward.

Thank you and I look forward to any questions.

[The prepared statement of Mr. Swire follows:]

PREPARED STATEMENT OF PETER SWIRE, C. WILLIAM O'NEILL PROFESSOR OF LAW,
MORITZ COLLEGE OF LAW, THE OHIO STATE UNIVERSITY

Chairman Rockefeller, Ranking Member Hutchison, and distinguished Committee Members, thank you for inviting me to testify on "The Need for Privacy Protections: Is Industry Self-Regulation Adequate?"

I am the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University. I began working on privacy and self-regulation in the mid-1990s. In 1999 I was named Chief Counselor for Privacy, in the U.S. Office of Management and Budget. In that role, I was the first (and thus far the only) person to have government-wide responsibility for privacy policy. As Chief Counselor for Privacy, I worked on both government regulation and self-regulation initiatives to protect privacy while meeting other societal goals. Since then, I have continued to write and speak extensively on privacy and security issues.

For this testimony, Committee Staff requested that I provide historical context about self-regulation and privacy. I was also asked to discuss the Digital Advertising Alliance's recent announcements with respect to Do Not Track, including the exceptions included in the DAA approach. In preparing this testimony, I have spoken at length with industry leaders, privacy advocates, and technologists. This testimony reflects my personal views as a law professor, a former government official, and a person who tries to help develop effective privacy practices in the U.S. and globally.

This testimony has four sections, with the key points set forth in the introduction:

- (1) *The threat of government regulation spurs the adoption of self-regulation.* In 1997 I presented a paper on privacy and self-regulation at a conference hosted by the U.S. Department of Commerce in which I explained that self-regulation works best when there is a credible threat that government will step in if industry does not do a good job. Simply put, the industry dynamic around self-regulation is entirely transformed when there is a credible threat of government intervention.
- (2) *The history of self-regulation after the 1990s shows that self-regulation declined when the credible threat of government action eroded.* When public policy attention shifted away from privacy after the first wave of effort in the 1990s, there was little new progress in self-regulation to match technological change. Indeed, critics who have examined the history have found greatly reduced effort in self-regulation. Some self-regulatory efforts continued, and initiatives that were linked with ongoing government involvement seem to have endured more than others.
- (3) *The current wave of attention to online privacy has produced progress on Do Not Track, but with broad exceptions to the announced collection limits.* The Digital Advertising Alliance's recent announcement that members would honor a Do Not Track header is potentially important to providing users with choice about their privacy online. However, the current exceptions for market research and product development swallow the Do Not Track rule. In addition, counsel for the DAA has informed me that they are open to concrete discussion about how to further improve these definitions in practice.

- (4) *We should focus more attention on technical and administrative measures for de-identification in online privacy.* The testimony concludes with a brief discussion of an area for possible win/win scenarios when it comes to privacy and beneficial uses of data online. The idea is simple—technical and administrative safeguards can help ensure data is collected and used in ways that are not linked to the individual.

In summary, there is currently strong attention on the part of Congress, the White House, and the Federal Trade Commission to Do Not Track and privacy issues for online advertising. With this public attention, now is the best opportunity to craft a good regime. When Do Not Track and related efforts are completed, there will be a temptation for policy makers to move onto other issues. That is why it is so important for the current Do Not Track standards and other current initiatives to be as well thought out as possible.

The Threat of Government Regulation Spurs the Adoption of Self-Regulation

In 1997 Secretary of Commerce William Daley and the National Telecommunications and Information Administration hosted a conference on “Privacy and Self-Regulation in the Information Age.” My paper for that conference, entitled “Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information,”¹ emphasized that self-regulation works best when there is a credible threat that government will step in if industry does not do a good job. Simply put, the threat of government regulation is what spurs the adoption of self-regulation. As discussed in the next section, this conclusion matches the historical experience in privacy self-regulation.

Self-regulation in privacy is a potentially useful approach where there are significant market failures as well as governmental failures. The 1997 paper highlighted a market failure that still applies to today’s online advertising market: “A chief failure of the market approach is that customers find it costly or impossible to monitor how companies use personal information. When consumers cannot monitor effectively, companies have an incentive to over-use personal information: the companies get the full benefit of the use (in terms of their own marketing or the fee they receive from third parties), but do not suffer for the costs of disclosure (the privacy loss to consumers).”

The challenge for consumers to monitor online collection of data today in many ways is greater than it was for consumers in 1997. During that period, the Internet was dominated by first-party sites, where the user decided to surf at a particular website that might collect data. Today, collection by third parties is famously complex.² News stories in the *Wall Street Journal* “What They Know” series and elsewhere have shown that even the savviest users find it difficult to opt out of online tracking in a world where cookies respawn and a typical web page can send data to literally dozens of different companies.

Along with these market imperfections, we know that government solutions are imperfect as well. Statutes and regulations are often slow to update to changed circumstances. Needed statutes sometimes face gridlock. Rules can be over-broad (prohibiting net beneficial uses) and under-broad (permitting uses that consumers would object to in the market if they knew about them).

These imperfections in market and regulatory approaches have repeatedly led those in the privacy debate to search for a third way, often called “self-regulation.” There are circumstances where self-regulation may be better than the alternative approaches. For instance, self-regulation is more tempting the greater the market and government regulatory failures. Some other factors that tend to favor self-regulation include:

- Industry expertise that leads to better-informed rules;
- Use for technical standards where many participants benefit from cooperation (i.e., network effects from adoption of standards for inter-connection or other purposes);
- Protections against using self-regulation for cartel or other anticompetitive purposes;

¹<http://ssrn.com/abstract=11472>.

²A chart of the complex display advertising ecosystem is at page 4 of *Comments of the World Privacy Forum regarding the Federal Trade Commission Preliminary Staff Report “Protecting Consumer Privacy in an Era of Rapid Change,”* (2011), at <http://www.ftc.gov/os/comments/privacyreportframework/00376-58005.pdf>.

- Incentives for the industry to enhance its reputation by adopting and complying with a self-regulatory regime; and
- Effective mechanisms for enforcement through legal, reputational, or other means.

We must also be realistic about the limits of self-regulation. Sometimes self-regulation has been chosen where those involved believed a statute or regulation would do a better job—even much-needed bills are often difficult to get through the legislative process, and the Federal Trade Commission lacks Administrative Procedure Act rulemaking authority for most privacy issues. Where obstacles to a law are serious enough, self-regulation may be the second best option.

A credible threat of government action is often the single greatest impetus to self-regulatory codes. Government action shapes the agenda, as we see today with this Senate hearing, and as the White House and FTC have shown on Do Not Track and other recent privacy issues. The threat of government action also transforms the dialogue inside industry meetings. When government is not interested, the person proposing the self-regulatory effort says: “Nothing is forcing us to do this, but the right thing would be to adopt a binding code of conduct.” When legislation and regulation are looming, the industry discussion is entirely different: “If we don’t do this ourselves, they will do it for us. We’ll be stuck with compliance for years to come, so we better have something good to say on this issue.”

When the Credible Threat of Government Action Erodes so Do Self-Regulatory Programs

The United States had a “first wave” of privacy policy activity related to the Internet from roughly 1996 to 2000.³ Internet privacy then became a less prominent issue, especially after the attacks of September 11, 2001 focused national attention on uses of data to fight terrorism. We are now in a “second wave” of major attention to Internet privacy. This section of the testimony discusses lessons learned from what happened after the first wave subsided. *When the credible threat of government action eroded, new self-regulatory activity essentially ceased and many self-regulatory programs eroded as well.*

This pattern matches the classic analysis of the “issue-attention cycle” by political scientist Anthony Downs, who wrote: “American public attention rarely remains sharply focused upon any one domestic issue for very long—even if it involves a continuing problem of crucial importance to society.”⁴ Downs emphasized that we should expect interest in an issue to wax and wane. Downs’ discussion is consistent with the thrust of my 1997 paper: “Over time, however, the legislative threat might ease. Agency attention may be directed elsewhere. As the threat of government action subsides, we might expect that self-regulatory efforts would also become more lax.”

Examining the history of self-regulation after 2000, even defenders of self-regulation would agree that there was little new progress to match technological change, while critics are far harsher. Some self-regulatory efforts continued, and initiatives that were linked with ongoing government involvement seem to have lasted longer than others.

The World Privacy Forum has written detailed reports about the failings of self-regulation after 2000.⁵ Here are some key conclusions:

- “We now have repetitive, specific, tangible examples of failed self regulation in the area of privacy. These examples are not mere anecdotes—these were significant national efforts that regulators took seriously.”
- “Privacy self-regulation organizations were loudly promoted despite their limited scope and substance.”
- “Privacy self-regulation organizations were structurally weak, lacking meaningful ability to enforce their own rules or maintain memberships. Those who subscribed to self-regulation were usually free to drop out at any time.”

³Peter Swire, *Why Privacy Legislation is Hot Now*, Thehill.com, June 23, 2011, at <http://thehill.com/component/content/article/72-opinion/168267-why-privacy-legislation-is-hot-now>.

⁴Anthony Downs, *Up and Down with Ecology—the “Issue-Attention Cycle,”* 28 *Public Interest* (Summer 1972), at 38.

⁵Robert Gellman & Pam Dixon, *Many Failures: A Brief History of Privacy Self-Regulation in the United States*, (2011), at <http://www.worldprivacyforum.org/pdf/WPFselfregulationhistory.pdf>; World Privacy Forum, *The Network Advertising Initiative: Failing at Consumer Protection and Self Regulation*, (2007), http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007/s.pdf.

Similar conclusions come from Chris Hoofnagle, a law professor at the University of California, Berkeley and co-chair of the annual Privacy Law Scholars Conference. Based on his extensive experience with self-regulation, Hoofnagle wrote the following in 2011: “Self-regulatory groups in the privacy field often form in reaction to the threat of regulation. They create protections that largely affirm their current and prospective business practices. The consumer rights created are narrow. They do not update their standards in response to changes, until the regulatory spotlight returns. Nor do they address new actors that raise similar concerns but fall outside of the self-regulatory regime.”⁶ Just this week, Professor Hoofnagle released a study of the 100 most popular websites, finding that 21 of them placed 100 or more cookies onto users’ computers, with 84 percent of the cookies placed by third parties.⁷

The World Privacy Forum highlights five prominent examples of self-regulation from the first wave.⁸ I quote these important examples verbatim, and then offer observations:

1. “*The Individual Reference Services Group* (IRSG) was announced in 1997 as a self-regulatory organization for companies that provide information that identifies or locates individuals. The group terminated in 2001, deceptively citing a newly passed regulatory law that made self-regulation unnecessary. However, that law did not cover IRSG companies.”
2. “*The Privacy Leadership Initiative* began in 2000 to promote self regulation and to support privacy educational activities for business and for consumers. The organization lasted about two years.”
3. “*The Online Privacy Alliance* began in 1998 with an interest in promoting industry self regulation for privacy. OPA’s last reported activity appears to have taken place in 2001, although its website continues to exist and shows signs of an update in 2011.”
4. “*The Network Advertising Initiative* had its origins in 1999, when the Federal Trade Commission showed interest in the privacy effects of online behavioral targeting. By 2003, when FTC interest in privacy regulation had evaporated, the NAI had only two members. Enforcement and audit activity lapsed as well. NAI did nothing to fulfill its promises or keep its standards up to date with current technology until 2008, when FTC interest increased.”
5. “*The BBBOnline Privacy Program* began in 1998, with a substantive operation that included verification, monitoring and review, consumer dispute resolution, a compliance seal, enforcement mechanisms and an educational component. Several hundred companies participated in the early years, but interest did not continue and BBBOnline stopped accepting applications in 2007.”

Based on my own experience and some interviews conducted in the days leading up to this hearing, I offer the following observations on these five prominent examples. These observations are subject to the disclaimer about the limited time I have had to double-check each factual situation:

1. *Individual References Services Group*: A lawyer who worked with the IRSG said that passage of Gramm-Leach-Bliley was indeed the key reason for the group’s demise. That law did set new limits on sales by financial institutions to data brokers. It did not, however, directly cover most activities of the data brokers who were members of IRSG. My impression is that the data broker industry felt the political pressure was off by the time the group terminated. FTC Commissioner Julie Brill has recently emphasized the need for new privacy initiatives concerning data brokers.
2. *Privacy Leadership Initiative*: According to published reports at the time of its creation in 2000, the PLI planned to spend \$30 to \$40 million to support self-regulation rather than have online privacy legislation. Because political attention to the issue soon faded, the sponsors apparently believed there was little reason to continue that level of effort after 2002.
3. *Online Privacy Alliance*: The OPA was highly visible during the privacy debates in 1998–2000. If the online privacy issue had remained prominent, I think it is likely that the OPA would have remained much more active for considerably longer.

⁶Chris Hoofnagle, *Can Privacy Self-Regulation Work for Consumers?*, Jan. 26, 2011, <http://www.techpolicy.com/CanPrivacySelf-RegulationWork-Hoofnagle.aspx>.

⁷James Temple, *Web Privacy Census Shows Tracking Pervasive*, SFGate, June 26, 2012, at <http://www.sfgate.com/default/article/Web-Privacy-Census-shows-tracking-pervasive-3663642.php>.

⁸Gellman & Dixon, *supra*.

4. *Network Advertising Initiative*: A senior person who worked with the NAI confirmed the low membership number (two) by 2002, after the considerable fanfare accompanying negotiation of the NAI code in 1999 and 2000. This source gave a different reason, however, for this decline: the collapse of the online advertising market when the dot.com bubble burst.
5. *BBBOnline Privacy Program*. One source explained its demise this way: “Its business model didn’t work.” It is unclear what combination of factors contributed to its demise. However, factors likely included a poor fundraising structure along with decreased demand for privacy services and a lack of political pressure for privacy protection.

As with any description of recent history, different observers are likely to emphasize different aspects of this record. My own view, however, is that the most optimistic reasonable view of privacy self-regulation after 2000 was that there was little progress until privacy began to get “hot” again in the last few years. These five prominent self-regulatory examples are consistent with the view that self-regulatory effort fades as the credible threat of government intervention fades. All of these programs garnered headlines when there was political focus on protecting privacy. All of these programs also disappeared or shrunk substantially when political attention focused elsewhere.

With that said, it is useful to examine areas of self-regulation that persisted after 2000:

1. *Website privacy policies*. I have previously written about the effectiveness of the government efforts in the late 1990s to encourage commercial websites to post privacy policies.⁹ Within three years, the portion of commercial sites with privacy policies rose from only 12 percent to a resounding 90 percent, without legislation. Commercial websites overwhelmingly continued to post privacy policies through the 2000s, encouraged in part by a 2003 California statute that requires such policies for companies targeting consumers there. The existence of these policies is central to the FTC’s ability to bring enforcement actions for deceptive trade practices. It is true, of course, that the quality of privacy policies is variable and often low. But this “self regulatory” practice of having privacy policies has remained in effect, and is now extending to the mobile application space.
2. *CAN-SPAM*. In the late 1990s and early 2000s, responsible companies sending commercial e-mail developed codes of good practice. A fundamental element of these practices was to permit consumer choice about receiving commercial e-mail from a particular company. Congress passed the CAN-SPAM Act in 2003. The law is subject to many criticisms, notably that (as with any law) it does not create a technological blockade against malicious spammers. With that said, I submit that the law has been very successful in a core aspect of consumer choice—CAN-SPAM requires companies to include an easy unsubscribe feature in each e-mail. I personally use this feature regularly, and legitimate companies stop sending me e-mail when I unsubscribe. In this instance, a self-regulatory effort was essentially incorporated into statute, and the unsubscribe feature continues to work. The Direct Marketing Association has also continued with its E-mail Preference Service, going beyond CAN-SPAM minimum requirements.¹⁰
3. *Safe Harbor*. The U.S.-E.U. Safe Harbor was negotiated in 2000. Companies become subject to the Safe Harbor if they certify their membership to the Department of Commerce, and participants are considered to have “adequate” privacy protections under the E.U. Data Protection Directive. Self-regulation is a prominent part of the Safe Harbor because participants must establish an independent recourse mechanism—must select a self-regulatory program—to investigate unresolved complaints.¹¹ Views about the effectiveness of the Safe Harbor vary widely. My own view is that there was a slow start initially for adoption of the Safe Harbor, but thousands of companies have entered it over time, and its principles are widely used even by companies that have not formally certified. The Safe Harbor has endured fairly well in contrast to the purely private-sector self-regulatory efforts; its official nature, furthermore, has

⁹Peter Swire, *Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy*, 52 *Hastings L.J.* 847 (2003), at <http://ssrn.com/abstract=424167>.

¹⁰http://www.dmaconsumers.org/consumers/optoutform_emp.shtml.

¹¹See http://export.gov/safeharbor/eu/eg_main_018495.asp.

created a helpful framework for ongoing discussions and conferences for the relevant U.S. and E.U. officials and other stakeholders.

These three examples all feature a mixed model of self-regulation, where self-regulatory codes are a precursor to or component of government action. This mixed model is sometimes called “co-regulation,” to emphasize the explicit role the government plays along with industry and other stakeholders. Historical evidence from the first wave of Internet privacy, however, suggests that co-regulatory efforts survived better through the highs and lows of the issue-attention cycle than did pure self-regulatory approaches.

The current wave of attention to online privacy has produced progress on Do Not Track, but with broad exceptions to the announced collection limits.

In the last few years, online privacy has become a hot issue again. Three major industry trends are driving this process: the rise of Facebook and other social media sites; the rapid growth in mobile devices, with their implications for location privacy; and the online advertising issues that are the subject of this hearing.¹² These industry trends have been extensively covered in the press. These technological and market changes have prompted political leaders to respond. The E.U. has promulgated a directive limiting use of online cookies and now its draft omnibus Data Protection Regulation. The Administration issued its Green Paper and now its Consumer Online Privacy Bill of Rights. The FTC has been very active on privacy, and has focused public attention on Do Not Track. Congress has devoted much more time to privacy, including today’s hearing.

The issue-attention cycle has returned to online privacy. Predictably, so has self-regulation. The Network Advertising Initiative has recovered from its slump in the early 2000s to reach a record membership and level of activity. The Digital Advertising Alliance has spent an enormous number of hours bringing to the table a wide range of players who have never before worked in such detail on privacy issues. Later this month, the Commerce Department will convene a multistakeholder process to address mobile application privacy issues.

Committee Staff have specifically asked me to discuss the Digital Advertising Alliance’s recent announcements with respect to Do Not Track, including the exceptions included in the DAA approach. *In my view, the DAA’s announcement to honor a Do Not Track header is potentially important to providing users with choice about their privacy online. In their current form, however, the exceptions for market research and product development swallow the Do Not Track rule. In addition, counsel for the DAA has informed me that they are open to concrete discussion about how to further improve these definitions in practice.*

The DAA is a coalition of online advertising organizations, including the Association of National Advertisers, whose President, Bob Liodice, is testifying here today. In 2009, the DAA released “Self-Regulatory Principles for Online Behavioral Advertising,” which contained principles on education, transparency, consumer control, data security, material changes, sensitive data, and accountability.¹³ In November 2011, the DAA released “Self-Regulatory Principles for Multi-Site Data,” which extended the 2009 principles beyond online behavioral advertising and also defined a number of important exceptions. In connection with the White House privacy event in February, the DAA agreed that its members would comply when consumers selected Do Not Track in their browsers, with enforcement by the FTC.¹⁴

These actions by the DAA have accompanied lengthy negotiations on a standard for Do Not Track in the World Wide Web Consortium (W3C). The W3C is a respected organization that has been instrumental to promulgation of many of the technical standards at the core of the modern Internet. The W3C process has involved privacy advocates, technologists, and industry leaders, including members of the DAA. I have not personally attended the W3C meetings, but I have stayed in close contact with participants from all the major perspectives. The W3C working group met for three days last week in Seattle. Although there has been important progress toward consensus on some issues, the scope of the exceptions has remained controversial, including but not limited to the exceptions for market research and product placement.

¹²Peter Swire, *Why Privacy Legislation is Hot Now*, Thehill.com, June 23, 2011, at <http://thehill.com/component/content/article/72-opinion/168267-why-privacy-legislation-is-hot-now>.

¹³<http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>

¹⁴The White House, *We Can’t Wait: Obama Administration Unveils Blueprint for a “Privacy Bill of Rights” to Protect Consumers Online*, Feb. 23, 2012, at <http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights>.

To place these exceptions in context, the consumer control part of the 2009 DAA principles enables “users of websites at which data is collected for online behavioral advertising purposes the ability to choose whether data is collected and used or transferred to a non-affiliate for such purposes.” The 2011 DAA principles go further by saying that third parties and service providers “should provide consumers with transparency and consumer control” for purposes other than online behavioral advertising. Along with these limits on collection of multi-site data, the 2011 principles restrict the use of multi-site data for eligibility for employment, credit, health care, or insurance.

The 2011 principles contain important exceptions to the general rule of transparency and consumer control. One category of exceptions is for “operations and system management purposes.” Those purposes appear quite broad: “intellectual property protection; compliance, public purpose and consumer safety; authentication, verification, fraud prevention and security; billing or product or service fulfillment; or Reporting or Delivery.” There is also an exception for data that will go through a de-identification process, as discussed further below.

I will focus my remarks on the remarkably broad exceptions in the 2011 DAA principles, “for market research or product development.” These exceptions are so open-ended that I have not been able to discern any limits on collection under them. Market research includes “research about consumers.”¹⁵ That would seem to include keeping track of every click made by a consumer. Market research also includes analysis of “consumer preferences and behaviors.” Again, if I were an FTC enforcer, I don’t know what lies outside the scope of the exception. The definition of product development is similarly broad. It includes analysis of “the characteristics of a market or group of consumers.” To analyze a “group of consumers” would seemingly permit collecting each click made by those consumers. Similarly, product development includes analysis of “the performance of a product, service, or feature.”

The 2011 DAA principles place one limit on information collected under the market research and product development exceptions. They state that the terms do not “include sales, promotional, or marketing activities directed at a specific computer or device.” Thus, companies should not collect information from Alice or Bob under the exceptions, and then use their specific knowledge about Alice or Bob to target their computers or other devices. The scope of this consumer protection, however, is currently unclear. The principles do permit any contact back to the computer of Alice or Bob “based on an aggregate use of data.” The current principles do not offer further guidance on what is permitted based on that aggregate use of data.

After reading the text of these exceptions to prepare this testimony, I then spoke about experts from both industry and the advocacy community to test the accuracy of my reading. My understanding, under the 2011 DAA principles, is that under the market research and product development exceptions:

- Companies have no transparency requirement;
- Companies have no consumer choice requirement;
- Companies can keep the data indefinitely;
- Companies can identify data that is collected without the user’s name, and combine it with identified data;
- Companies can combine their data with data from other sources, to build up a more detailed profile; and
- Companies can share data with other third parties so long as it is not used to market back to the specific computer or device.

To summarize, the 2011 DAA principles have a section called “Limitations on the Collection of Multi-Site Data.” The market research and product development exceptions are part of that section. As drafted, it is difficult to see what limitations on collection could be enforced given the breadth of the exceptions.

What should be done in light of these findings? The counsel for the DAA, has informed me that they are open to concrete discussions about how to further improve these definitions in practice. Counsel specifically understood that I would state that in this testimony.

My view is that considerably more work needs to be done in defining the market research and product development exceptions. As one person, I don’t presume to

¹⁵ “Market Research means the analysis of: market segmentation or trends; consumer preferences and behaviors; research about consumers, products, or services; or the effectiveness of marketing or advertising. A key characteristic of market research is that the data is not re-identified to market directly back to, or otherwise re-contact a specific computer or device. Thus, the term “market research” does not include sales, promotional, or marketing activities directed at a specific computer or device.”

know the answers to these complex questions. I do believe, however, that participants can get helpful insights from the way that market research and research generally have been handled in other contexts that implicate privacy. For instance, telephone market research has existed for decades. My understanding is that there are well-developed practices, and perhaps codes of conduct, for protecting confidentiality in telephone market research. To my knowledge, there have not been recent scandals about whether Gallup or some other research firm has re-identified an individual's response to a telephone survey. Based on discussions with participants in the W3C process, these offline market research precedents have not been discussed at the W3C. Perhaps the online community can learn from the historical practice for offline market research.

Similarly, we have extensive experience on how to define and conduct research in other settings. Many Federal agencies gather data for statistical research, from the Census to economic statistics and many other purposes. These agencies have years of experience of how to get needed statistical information while preserving confidentiality, and the current online advertising debates should draw on that expertise.¹⁶ Under the HIPAA medical privacy rule, there are at least four methods for conducting research on protected health information: (1) individual consent; (2) de-identification of the data; (3) with authorization from an Institutional Review Board or Privacy Board; or (4) on limited data sets, where the researchers agree to comply with confidentiality conditions in order to get the data.

I am not saying that the rules for medical research should apply online; instead, the point is that *researchers have used data intensively in many settings other than online advertising. The online advertising debates should be better informed by the institutional options that have been developed in areas such as offline market research, government statistics, and medical research.*

Improve & Employ Technical and Administrative Measures for De-Identification in Online Privacy

Before concluding, I will briefly discuss an area where there may be important win/win outcomes both for privacy and beneficial uses of data about online activities. With the Future of Privacy Forum, I am conducting a research project on de-identification in the online advertising space. We have received expressions of interest from industry, privacy advocates, and technologists.

The idea is simple—we should employ technical and administrative safeguards so that data is collected and used in ways that are not linked to the individual. If we can build effective safeguards, then data can be used more intensively while protecting against privacy problems.

Doing de-identification well is a challenging problem, but I believe we are now in a time when more work is needed about how to do it online. In its recent report, the FTC proposed a promising approach to de-identification, which includes technical measures as well as public statements from companies that they will not re-identify individuals, with those statements being enforceable under the FTC Act.¹⁷ The 2011 DAA principles contemplate greater use of de-identification, where “an entity has taken reasonable steps to ensure that the data cannot reasonably be re-associated or connected to an individual.” I have started to write on this topic,¹⁸ and recently submitted comments to the Department of Commerce about how de-identification could be a candidate for a multi-stakeholder process.¹⁹

Due to its highly technical nature, it is difficult to craft a statute that states specifically how to achieve de-identification. To date, there has not been enough work to understand what mix of technical and administrative safeguards will best protect privacy while also enabling beneficial uses of information. I hope that many parties will focus more attention on how to build de-identification more effectively into our Internet practices.

Conclusion

In conclusion, let me state my optimism about the intelligence, good faith, and willingness to work hard on these issues in industry, the privacy advocacy community, and among technologists. The online advertising eco-system today is much more complex than in the 1990s. There are major institutional challenges in understanding the technology and market forces, and coordinating a response.

¹⁶For a history of confidentiality and Federal statistics, see Douglas J. Sylvester & Sharon Lohr, *Counting on Confidentiality: Legal and Statistical Approaches to Federal Privacy Law After the USA PATRIOT Act*, 2005 Wisc. L. Rev. 1033.

¹⁷Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (2012), at <http://ftc.gov/os/2012/03/120326privacyreport.pdf>.

¹⁸<http://www.peterswire.net/psspeeches2011.htm>.

¹⁹<http://www.ntia.doc.gov/federal-register-notice/2012/comments-multistakeholder-process>.

In making progress on such issues, we should be informed by the history. When Congress and agencies focus on an issue, the attention often brings out the best in industry. The public attention empowers technologists and other privacy experts within companies and industry groups to convince their colleagues to take effective measures to protect privacy. By contrast, if the pressure is off, the privacy experts within industry find it more difficult to get their colleagues to protect personal information.

Getting online privacy right is important for each of us as Americans. In testimony last fall before the House Energy & Commerce Committee, I explained that a “we don’t care about privacy” approach from the United States would create risks for American jobs, exports, and businesses.²⁰

More simply, I personally would not like to have an Internet where I believed that each moment of my browsing might easily be breached and shown to the entire world. For you and your families, it would reduce the quality of the Internet if you thought that any page you visited needed to be treated like something that might be released to the public. That is not the experience we have today. However, if we do not foster good practices, then we risk losing confidence in our use of the Internet.

Thank you once again for the invitation to testify today. I am happy to respond to your questions.

Biographical Information

Peter Swire is the C. William O’Neill Professor of Law at the Moritz College of Law of the Ohio State University. He began working on privacy and self-regulation in the mid-1990s. In 1998, he was the lead author, with Robert Litan, of “None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive,” published by the Brookings Institution. In 1999, he was named Chief Counselor for Privacy, in the U.S. Office of Management and Budget. In that role, he was the first (and thus far the only) person to have government-wide responsibility for privacy policy.

As Chief Counselor for Privacy, he worked on both government regulation and self-regulation initiatives to protect privacy while meeting other societal goals. On the government regulation side, he was the White House lead on the HIPAA medical privacy rule and on the financial privacy rules implementing the Gramm-Leach-Bliley Act. For self-regulation, he worked extensively in connection with the Network Advertising Initiative code of 2000, and helped negotiate the Safe Harbor agreement for data flows between the E.U. and the U.S., including a major role under the Safe Harbor for self-regulatory associations.

In 2001, Swire returned to law teaching. He has since continued to write and speak extensively on privacy and security issues, with publications and speeches available at www.peterswire.net. In 2009 and 2010 he was Special Assistant to the President for Economic Policy, serving in the National Economic Council under Dr. Lawrence Summers. In 2010, he once again returned to law teaching at The Ohio State University. He lives in the D.C. area.

Senator KLOBUCHAR. Thank you very much.
Mr. Szoka?

STATEMENT OF BERIN SZOKA, PRESIDENT, TECHFreedom

Mr. SZOKA. Chairman Rockefeller, members of the Committee, thank you again for inviting me here to testify about privacy today.

First, at the Progress and Freedom Foundation and now at TechFreedom, I’ve worked for over 4 years to articulate from the think-tank world an alternative perspective on privacy that stresses the enormous value created by data, while recognizing the need to prevent its abuse.

While we’re all here engaged in fixing the problems, we mustn’t lose sight of the forest for the trees. The benefits of collection and the use of data to date have dramatically outstripped its costs of the relatively few abuses.

²⁰Peter Swire, *Internet Privacy: The Impact and Burden of EU Regulation*, Statement before the House Energy & Commerce Committee, Sept. 15, 2011, at http://www.americanprogressaction.org/issues/2011/09/swire_testimony.html.

So in considering how to address abuses, I agree: self-regulation is not enough. So-called baseline legislation is, indeed, necessary.

But such a baseline already exists. Section V empowers the FTC to prohibit as unfair uses of data that do more harm than good and that consumers themselves cannot reasonably avoid. Further, the act empowers the FTC to enforce self-regulation by holding companies to their promises.

Above this baseline, we've built a layered approach to privacy protection, including narrow legislation to address particularly thorny problems. But the genius of American law is our largely evolutionary, common-law model, addressing problems as they arise, and learning from past successes and failures, rather than attempting to design a comprehensive regulatory scheme wholesale.

Our system is what Richard Epstein famously called "Simple Rules for a Complex World."

The FTC's effectiveness should be measured not by counting settled cases but in development of a quasi-common law of privacy. Yet today, companies have only FTC complaints and consent decrees with little analysis to guide them.

I suggest the agency take four steps. First, explain its analysis and consent decrees. Second, issue no-action letters when deciding not to sue. Third, issue advisory opinions upon request to guide industry on how the agency might evaluate new privacy practices. And fourth, issue guidelines explaining how the agency has applied unfairness and deception in past cases and how it plans to do so in the future, in particular, clarifying the boundaries of privacy harm.

Congress should encourage the FTC to do these things and ensure that they have the resources necessary to do these things and to keep pace with technological change. But policymakers and, I hasten to add, everyone else necessarily lack the expertise and foresight to freeze in place today fair information practices. The technologies involved are simply evolving too rapidly and the trade-offs are too complex.

This is why the White House stressed the flexibility, speed, and decentralization that only self-regulation can provide.

Congress should, however, carefully scrutinize how the FTC has used soft power to influence self-regulation, and how that power has reinforced incumbents' market power. Nowhere is this more true or potentially more dangerous than in W3C's "do not track" process.

As FTC Commissioner Tom Rosch has noted, the major browser firms' interest in developing "do not track" mechanisms begs the question of whether and to what extent these major browser firms might act strategically and opportunistically.

The W3C process has rested on the principle of user choice. Microsoft breached this consensus when it decided in its new IE 10 browser that it would set "do not track" headers by default. Default "do not track" on doesn't empower users any more than would setting ad blocking by default. Default "do not track" on simply empowers browser makers to force fundamental changes in the Internet's ecosystem.

From today's low friction, flat ecosystem of independent sites and services, funded by generally impersonal data collection, default

“do not track” on could take us to an Internet with fewer players who collect more data with less transparency.

In the worst case, opt-in dystopia, consumers could be made significantly worse off in three ways.

First, if publishers have to rely on micropayments or subscriptions, their revenues will likely drop.

Ironically, second, in the name of privacy, we could actually increase user tracking, because those sites and services that do obtain opt-ins will likely collect more personal data.

And third, few publishers in data-driven companies will be able to obtain opt-in exceptions to “do not track.” This will force unprecedented consolidation in the Internet ecosystem. And thus, with the best of intentions, we may be blithely heading toward reshaping the Internet.

But even more troubling is the way we’re doing it. This isn’t the result of a bottom-up evolutionary process. It’s more like collusion between government and powerful market players. It is not self-regulation but co-regulation.

It is the European model, where governments steer by extra legal threats, and the industry merely rows; where government encourages powerful incumbents who use market power to serve their own agendas with government’s blessing.

Given the FTC’s heavy involvement in the W3C process, Congress should ask the FTC to explain what exactly its role has been, especially in Microsoft’s decision to defy W3C’s principle of user choice.

No one would deny that regulatory agencies play a significant role in encouraging self-regulation. But with due respect to my friend and colleague, Peter, the extra legal intimidation that he and Tim Wu have endorsed is deeply dangerous.

If government can regulate the Internet without statutory authority or judicial review simply because its goals seem noble, the rule of law does not exist online.

The better way for the FTC to encourage self-regulation is through the legal means I have suggested—building a quasi-common law subject to clear standards and subject to review, if not by the courts than by Congress.

Again, thank you for inviting me here today. And I look forward to your questions.

[The prepared statement of Mr. Szoka follows:]

PREPARED STATEMENT OF BERIN SZOKA, PRESIDENT, TECHFREEDOM¹

I. Introduction

Chairman Rockefeller, Ranking Member Hutchison—thank you for inviting me to testify about privacy again before your Committee. As President of TechFreedom, a non-profit think tank, and before that, as Director of the Center for Internet Freedom at The Progress & Freedom Foundation, I have worked for over four years to articulate an alternative perspective on privacy that recognizes both the enormous value created by data and the need to prevent abuses of data. The debate thus far has systematically underestimated the benefits to consumers from the use of per-

¹Berin Szoka (@BerinSzoka) is President of TechFreedom, a non-profit, non-partisan technology policy think tank. He has written and commented extensively on consumer privacy. In particular, he testified on Balancing Privacy and Innovation before the House Energy & Commerce Committee, Subcommittee on Commerce, Manufacturing, and Trade on March 29, 2012, available at <http://tch.fm/KCrz8k>, (“Szoka Testimony”).

sonal data to tailor advertising, develop new products, and conduct research, while overstating the dangers of data, which remain largely conjectural.

With the best of intentions, we are heading towards reshaping the fundamentals of the Internet—in ways that may have serious negative unintended consequences for privacy, the sites and services consumers enjoy, and the health of the ecosystem. But the *way* we're doing it may be even more troubling. This is not the result of a bottom-up evolutionary process, but of collusion between government and powerful market players. We are heading for opt-in dystopias.

II. The American Layered Approach to Privacy

I agree that self-regulation is not enough, that so-called “baseline” legislation is, indeed, necessary. I disagree, however, that *new* baseline legislation is needed. We already have baseline consumer protection legislation: Section V of the Federal Trade Commission Act² empowers the FTC not only to enforce self-regulation by holding companies to their promises, but also to prohibit as “unfair” uses of personal data that do more harm than good and that consumers themselves cannot reasonably avoid. States have similar legislation, empowering Attorneys General to act,³ and class action lawsuits also deter privacy violations.⁴

On top of this baseline, we have built a layered approach to privacy protection. Where the FTC's authority has proven inadequate, Congress has enacted legislation to address specific problems, such as the Children's Online Privacy Protection Act⁵ and the Fair Credit Reporting Act.⁶ But in general, American law follows a common law model, addressing problems on a case by case basis rather than attempting to design a comprehensive regulatory scheme adequate for both present and future. This is what Richard Epstein famously called “Simple Rules for a Complex World.”⁷ The Electronic Frontier Foundation's Mike Godwin put it best in 1998 when he said: “It's easier to learn from history than it is to learn from the future. Almost always, the time-tested laws and legal principles we already have in place are more than adequate to address the new medium.”⁸

Applying baseline principles of consumer protection is the best way to address new privacy challenges, given the ever-changing nature of the technologies involved and the inevitable trade-offs among competing conceptions of privacy, and between privacy and other values—such as:

- Funding for innovative media and services that would not otherwise be available;
- The diversity and competitiveness of an Internet ecosystem with low barriers to entry;
- The ease of use for consumers of an Internet that is not divided by checkpoints asking for consent or payment as users cross domain name boundaries;
- The innovation driven by discoveries made possible by analyzing what some have pejoratively labeled “Big Data,” and so on.

Policymakers simply do not have the expertise or foresight to make complex rules to decide these trade-offs—or the time to become experts in complex technologies. So it is here that self-regulation plays a critical role in our layered approach to privacy. As the White House privacy report acknowledged, self-regulation alone “can provide the flexibility, speed, and decentralization necessary to address Internet policy challenges.”⁹

In short, self-regulation is necessary, but not sufficient. It must work in tandem with the enforcement of existing laws—which I believe can be enhanced significantly *without* new legislation. But we must also understand that self-regulation is merely

² 15 U.S.C. § 45 (2006).

³ Henry N. Butler & Joshua D. Wright, Are State Consumer Protection Acts Really Little-FTC Acts?, 63 Fla. L. Rev. 163, 165 (2011) (discussing state laws empowering attorneys general to “combat consumer fraud and other deceptive practices”).

⁴ Glenn G. Lammi, “Thanks, Google Buzz: Class Action Lawyers Celebrate Impending Fees,” *Forbes*, Nov. 3, 2010, available at <http://www.forbes.com/sites/docket/2010/11/03/thanks-google-buzz-class-action-lawyers-celebrate-impending-fees/>.

⁵ Children's Online Privacy Protection Act of 1998, Pub. L. No. 105–277, 112 Stat. 2581–728 (codified in 15 U.S.C. §§ 6501–6506).

⁶ Fair Credit Reporting Act of 1970, Pub. L. 91–508; 84 Stat. 1128 (codified in 15 U.S.C. § 1681).

⁷ Richard A. Epstein, *Simple Rules for a Complex World* (1995).

⁸ Quoted in Virginia Postrel, *The Future and Its Enemies: The Growing Conflict Over Creativity, Enterprise, and Progress* at 48 (Touchstone 1998).

⁹ The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* at 23, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

one part of a broader process by which market forces discipline corporations in how they collect, process, use and distribute personal data about us. Together, this layered approach is the best way to maximize the enormous benefits offered by the use of personal data while minimizing its occasional abuse.

III. Market Regulation of Privacy

Companies do not operate in a vacuum. They compete not just for customers, but to protect their good name in the eyes of business partners, shareholders, media watchdogs, potential employees, and citizens themselves. Nowhere in the economy is this more true than online, where companies compete both for consumers' attention and for the trust of business partners, especially advertisers.

The social media revolution has made it possible for anyone concerned about online privacy to blow the whistle on true privacy violations. That whistle may not always be loud enough to be heard, but it's more likely in this sector than any other. Traditional media sources like the *Wall Street Journal* have played a critical role in attracting attention to corporate privacy policies through "What They Know" series,¹⁰ which has been popularized using social media tools. Reporters like Julia Angwin may rightly lament the failure of self-regulation in any particular case, but the very act of their criticism is essential for *market* regulation to function, because they are powerful actors in the marketplaces of ideas and reputation.

Earlier this year, social media tools were directed at Congress—to great effect—to express grassroots concern about the impact of proposed copyright legislation. While some Internet companies certainly helped to promote these messages, even were it not for their involvement, this experience would demonstrate how effective social media activism can be. There is no reason why such techniques cannot be used effectively against major Internet companies themselves, just as Facebook users have used Facebook itself to rally opposition to Facebook on privacy concerns such as its Beacon ad targeting system.¹¹ "The herd will be heard," as Bob Garfield memorably put it in his 2009 book, *The Chaos Scenario: Amid the Ruins of Mass Media*.¹² The Choice for Business Is Stark: Listen or Perish. Among the most important factors driving companies to participate constructively in the multi-stakeholder process, to forge meaningful privacy protections, and to abide by them is the fear of a *Wall Street Journal* article, a social media frenzy, or organized campaign demanding action on a particular privacy problem.

As Wayne Crews of Competitive Enterprise Institute put it in testimony before this committee in 2008:

Businesses are disciplined by responses of their competitors. Political regulation is premature; but "self-regulation" like that described in the FTC principles is a misnomer; it is competitive discipline that market processes impose on vendors. Nobody in a free market is so fortunate as to be able to "self regulate." Apart from the consumer rejection just noted, firms are regulated by the competitive threats posed by rivals, by Wall Street and intolerant investors, indeed by computer science itself.¹³

IV. Enhancing the American Layered Approach to Privacy

As I argued in March in testimony before the House Energy & Commerce Committee's Subcommittee on Commerce & Manufacturing,¹⁴ the FTC could do much more with its existing authority to build an effective quasi-common law of privacy in three ways.

First, Congress should assess whether the FTC has adequate institutional resources and expertise. If the FTC had heeded my fellow panelist Peter Swire's call

¹⁰ See generally *What They Know*, Wall St. J., 2012, <http://blogs.wsj.com/wtk/>.

¹¹ See, e.g., Kirsten E. Marti, Facebook (A): Beacon and Privacy 3 (2010), available at http://www.darden.virginia.edu/corporate-ethics/pdf/Facebook%20A_business_ethics-case_bri-1006a.pdf ("The online community responded immediately to this intrusion. MoveOn.org created a Facebook group "Petition: Facebook, stop invading my privacy!" that stated: "Sites like Facebook must respect my privacy. They should not tell my friends what I buy on other sites—or let companies use my name to endorse their products—without my explicit permission." The Facebook group and petition had 2,000 members within the first 24 hours and eventually grew to over 80,000 names." [internal citations omitted]).

¹² James Cherkoff, "The Joy of a Gated Community," *The Chaos Scenario*, June 1, 2010, <http://thechaosscenario.net/>.

¹³ Wayne Crews, Testimony Before the Senate Committee on Commerce, July 9, 2008, available at <http://cei.org/sites/default/files/Wayne%20Crews%20-%20Senate%20Commerce%20Testimony%20-%20Online%20Advertising,%20July%209%202008.pdf>.

¹⁴ Berin Szoka, Testimony Before the House Energy & Commerce Committee, Subcommittee on Commerce, Manufacturing, and Trade, "Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?", Mar. 29, 2012, available at [http://techfreedom.org/sites/default/files/Szoka%20Privacy%20Testimony%20to%20CMT%203.29.12%20v3%20\(final\)_0.pdf](http://techfreedom.org/sites/default/files/Szoka%20Privacy%20Testimony%20to%20CMT%203.29.12%20v3%20(final)_0.pdf).

for the FTC to build a an office of information technology five years ago,¹⁵ our layered privacy approach would today be far more effective in protecting consumers and ensuring their trust, and less easily dismissed as inadequate by foreign privacy regulators. Chairman Leibowitz deserves credit for appointing the agency's first Chief Technologist. But even with someone as talented as Ed Felten in that position, the FTC is still way behind the curve: His title is not Chief Technology *Officer* because there is no office behind him.

The FTC needs a clear strategic plan outlining (a) how to build the in-house technical expertise it needs (beyond basic IT infrastructure) to identify enforcement actions, support successful litigation, monitor compliance, and conduct long-term planning and policy work, and (b) the resources necessary to achieve that goal through a combination of re-prioritizing current agency spending and additional appropriations. Importantly, this organization should function as a cohesive team that meets the needs for technical expertise of all the FTC's bureaus and offices (including the Bureau of Competition). A stand-alone organization could, like the Bureau of Economics, better attract and retain talent.

Second, the clearer privacy promises are, the more easily the FTC will be able to enforce them. One important way to achieve this goal would be for the FTC to promote the use of "smart disclosure"—the term used by Cass Sunstein, director of the Office of Information and Regulatory Affairs and a close advisor to President Obama, and a widely respected thinker in law, policy and technology. Smart disclosure can empower consumers by letting software do the work for them of reading privacy policies—and then implement their privacy preferences.

For example, users could subscribe to the privacy recommendations of, say, Consumer Reports, or any privacy advocacy group, which in turn could set their phone to warn them if they install an app that does not meet the privacy practices those trusted third parties deem adequate. Or, more simply, such a system could work for communicating whether a site, service or app accedes to a particular self-regulatory code of conduct—and phone privacy controls could be set by default to provide special notices when users attempt to install apps that do not certify compliance with self-regulatory codes of conduct. As the FTC Privacy Report notes, smart disclosure could also "give consumers the ability to compare privacy practices among different companies."¹⁶ An app store might illustrate how such comparisons could work, allowing users trying to choose between several competing apps to compare their privacy practices side by side.

While it would be preferable for smart disclosure to arise through self-regulation, especially given the complexity of crafting disclosure formats, mandating disclosure of privacy practices would generally be a better way for government to address demonstrated market failures than by dictating what constitutes fair information practices—and thus might be an appropriate area for Congress to explore legislation at some point.

Third, the proper measure of the FTC's effectiveness is not how many suits it successfully settles, but how well it contributes to the development of a quasi-common law of privacy that can guide companies pushing the envelope with new data-driven technologies—without stifling innovation that ultimately serves consumers. The chief problem today is that companies have only FTC complaints and consent decrees to guide in predicting the course of the law. These documents offer very little explanation of how the facts of a particular case satisfy the FTC's Policy Statements on unfairness and deception. And these summary assertions are never tested in court, both because of the cost of litigation relative to settlement, and because of the cost to a defendant company of bad publicity from being perceived as anti-privacy exceed the benefits of taking the FTC to court—even when they would likely prevail given the FTC's overreach. While this should reassure us that reputation markets exert far greater pressure to discipline companies on privacy than is commonly appreciated, it also means that we lack the key ingredient for building a true common law: judicial scrutiny in an adversarial process.

The forces that keep privacy adjudication out of the courts and prevent development of privacy common law by judges are not likely to be easily overcome by FTC—or even Congressional—action. So we need to find alternative ways to replicate the adversarial process of careful analysis by which courts build upon simple rules to address the challenges of a complex world. I suggest the following six pos-

¹⁵Peter Swire, *Funding the FTC: Globalization and New Information Technologies Necessitate an Appropriations Boost*, Feb. 26, 2007, <http://www.americanprogress.org/issues/2007/02/ftc.html>.

¹⁶Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* 62 ("FTC Report"), <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>.

sible ways for the FTC to make better use of its existing authority to build a quasi common law:

1. The Commission (or individual Commissioners) should provide greater analysis of its rationale under its Unfairness and Deception Policy Statements for issuing each consent decree.
2. The FTC should, when it closes an investigation by deciding *not* to bring a complaint, issue a “no action” letter explaining why it decided the practice at issue was lawful under Section V.¹⁷ Such letters, issued by other agencies like the Securities and Exchange Commission, provide an invaluable source of guidance to innovators. Congress should even consider whether the FTC should be required to issue such letters.
3. The FTC should consider how it could use advisory opinions more effectively to provide guidance to industry on how the agency might evaluate new privacy practices—especially for companies working on the cutting edge of technology, which are often small. The FTC issues such letters on a wide range of topics,¹⁸ yet does not appear to have issued advisory opinions regarding the application of Section V to privacy.
4. Congress should reassert the vital oversight it exercised in 1980 and 1983 when it ordered the agency to issue the Policy Statements on Unfairness and Deception. At a minimum, the FTC should be required to explain, in detailed analysis, how it has applied those venerable standards in past privacy enforcement cases, and how it plans to do so in the future—again, because it is “easier to learn from history than it is to learn from the future.”¹⁹ Such guidelines are routine in other areas, and provided for in the Commission’s current procedures.²⁰ Indeed, the antitrust guidelines issued by the FTC and DOJ form a key element of the American common law of competition. The FTC has issued a number of Guides²¹ to explain its approach to consumer protection—but none for consumer privacy.²² The FTC’s recently issued privacy report is no substitute for such a Guide—indeed, it has little grounding in the twin Policy Statements that are supposed to be the FTC’s lodestars. To replicate some of the adversarial nature of actual litigation, the process must be the result of a substantive dialogue with affected stakeholders, and it must be subject to involved oversight from the full Commission and from Congress.
5. In particular, the FTC must clarify the boundaries of privacy harm under the Unfairness Doctrine. The FTC’s leadership seems to be trying to have it both ways: playing down publicly what they can do with their existing legal authority (to support their argument for new statutory authority) while, at the same time, making bold claims about the scope of harm in their enforcement actions. If the concept of harm is stretched too far, the Unfairness Doctrine will become again, as it was in the 1970s, a blank check for the FTC to become a second national legislature.²³ I explain my concerns about the potential for the unfairness doctrine to be abused, but also my belief that the doctrine should be used to the greatest extent degree with the 1980 Policy Statement, in my March testimony before the House Energy & Commerce Committee.²⁴

¹⁷ See, e.g., Jodie Bernstein, *Re: Petition Requesting Investigation of, and Enforcement Action Against SpectraCom, Inc.*, <http://www.ftc.gov/os/1997/07/cenmed.htm>.

¹⁸ 16 C.F.R. § 1.1 (2012) (“Any person, partnership, or corporation may request advice from the Commission with respect to a course of action which the requesting party proposes to pursue. The Commission will consider such requests for advice and inform the requesting party of the Commission’s views, where practicable, under the following circumstances . . . (1) The matter involves a substantial or novel question of fact or law and there is no clear Commission or court precedent; or (2) The subject matter of the request and consequent publication of Commission advice is of significant public interest.”); see also Judith A. Moreland, *Overview of the Advisory Opinion Process at the Federal Trade Commission*, available at <http://www.ftc.gov/bc/speech2.shtm>.

¹⁹ See *supra* note 9.

²⁰ Federal Trade Comm’n, FTC Operating Manual § 8, available at <http://www.ftc.gov/foia/ch08industryguidance.pdf>.

²¹ Federal Trade Comm’n, FTC Bureau of Consumer Protection—Resources: Guidance Documents, <http://ftc.gov/bcp/menus/resources/guidance.shtm> (last visited June 26, 2012).

²² Federal Trade Comm’n, Legal Resources/BCP Business Center, <http://business.ftc.gov/legal-resources/48/33> (last visited June 26, 2012).

²³ See generally, Howard Beales, III, *The FTC’s Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, § III, <http://www.ftc.gov/speeches/beales/unfair0603.shtm> [hereinafter *Beales Paper*].

²⁴ See Szoka, *supra* at 15.

6. Congress should ensure the FTC has the resources adequate to engage in this detailed analysis. To dismiss the current legal model as inadequate simply because it has not been fully utilized, and to adopt instead a new legislative framework whose true costs are unknown, would be truly “penny wise, pound foolish.” Given the clear need to reduce Federal spending across the board, and the decidedly mixed record of antitrust law in actually serving consumers, Congress could simply reallocate funding from the FTC’s Bureau of Competition—or, more dramatically, consolidate antitrust enforcement at the DOJ and allocate the cost savings from streamlining to the FTC’s Bureau of Consumer Protection.²⁵

If Congress wants to improve upon the American layered approach to privacy, these suggestions offer concrete steps that could be taken today. Just as Silicon Valley’s motto is “Iterate, iterate, iterate,” the same approach is needed for improving our existing framework.

Only by using the current framework to its fullest capacity will we actually know if there are real gaps the FTC cannot address using its existing authority. In particular, the process of issuing guidelines could identify problems as candidates for appropriately narrow legislation that could build on top of the current baseline as part of an effective layered approach—or for self-regulatory processes akin to those called for by the NTIA. If there are some forms of harm that require government intervention but that cannot fit within an appropriately limited conception of harm under unfairness, it may be better for Congress to address these through carefully tailored legislation, rather than shoehorning them into unfairness. For example, such legislation might be appropriate to prevent employers from pressuring employees into sharing their passwords to Facebook and other social networking sites.

V. The DAA: A Self-Regulatory Success Story

The Digital Advertising Alliance has demonstrated how self-regulation can evolve to provide “the flexibility, speed, and decentralization necessary to address Internet policy challenges”—not perfectly, but better than government. Since my fellow witness Bob Liodice, is representing the DAA today, let me just highlight four areas in which I think DAA has demonstrated the value of self-regulation beyond its additional principles:

- *Transparency*: In April 2010, the industry began including an icon inside targeted ads to raise awareness of the practice and offer consumers an easy opt-out from tailored advertising. That icon is now shown in over a trillion ad impressions each month.
- *Education*: Last January, DAA launched an unprecedented public awareness campaign called “Your AdChoices” to further increase public awareness of the AdChoices Icon, and consumers’ ability to opt-out.
- *Evolving commitments*: In November 2011, the DAA updated its principles to bar data collected for advertising purposes from being used for employment, credit, health care treatment, or insurance eligibility decisions.²⁶
- *Enforcement*: The Better Business Bureau, which administers enforcement of the DAA principles, and has done so for other self-regulatory programs since 1971, has brought a number of enforcement actions,²⁷ demonstrating that it is far from toothless.
- *Do Not Track*: In February, the DAA committed²⁸ to respect Do Not Track (DNT) headers sent by browsers when users visit websites as a (potentially) more consumer-friendly way of implementing DAA’s existing privacy opt-out.

VI. Concerns about Self-Regulatory Processes

The DAA is a good example of self-regulation evolving. But not all self-regulation is created equal. I have previously outlined my concerns about the self-regulatory process the NTIA has proposed to facilitate.²⁹ Chief among those concerns was the

²⁵ See William E. Kovacic, *The Institutions of Antitrust Law: How Structure Shapes Substance*, 110 Mich. L. Rev. 1019, 1034 (2012) (identifying several problems with Federal duality of antitrust jurisdiction).

²⁶ Digital Advertising Alliance, *Self-Regulatory Principles for Multi-Site Data*, Nov. 2011, <http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf>.

²⁷ See Better Business Bureau, *Case Decisions*, <http://www.bbb.org/us/interest-based-advertising/decisions/> (last visited June 26, 2012).

²⁸ Digital Advertising Alliance, *DAA Position on Browser Based Choice Mechanism*, Feb. 22, 2012, http://www.aboutads.info/resource/download/DAA_Commitment.pdf.

²⁹ Berin Szoka, *Comments to the National Telecommunications and Information Administration on the Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct*,

role government play in steering the process through the exercise of “soft power.” My participation in the World Wide Web Consortium (W3C) process as an invited expert (for the last six weeks) has increased that concern dramatically, given the looming presence of the FTC, and to a lesser extent, European governments, behind that process. In particular, I fear that an artificial deadline imposed by the FTC and other global regulators may shape the outcome of the process in ways that prove counter-productive.

More generally, despite my general skepticism of antitrust and belief that market power is best combated with market power, my experience with W3C has made me appreciate better the concerns raised by FCC Commissioner Tom Rosch about manipulation of the self-regulatory process by powerful players—especially where market power is essentially piggybacking on the soft power of government. In his dissent from the FTC’s 2012 privacy report, Rosch asked: “the major browser firms’ interest in developing Do Not Track mechanisms begs the question of whether and to what extent those major browser firms will act strategically and opportunistically (to use privacy to protect their own entrenched interests).”³⁰ And in his concurrence to the draft version of that report released in December 2010, Rosch noted: “the self-regulation that is championed in this area may constitute a way for a powerful, well-entrenched competitor to raise the bar so as to create an entry barrier to a rival that may constrain the exercise of undue power.”³¹

These concerns about power are heightened by concerns about process. The W3C is highly respected as a standard-setting body, but it is not a *policy*-making body. Its first and only other policy-heavy process—to produce the Protocol for Privacy Preferences (P3P), a laudable but highly complex form of smart disclosure—was roundly criticized and never achieved widespread adoption.

Many key players are simply not represented—most notably the publishers, smaller advertising companies and data processors. All of these have a great deal to lose and could be put out of business, or forced to consolidate with larger players, in a Default DNT-On world. In large part, this reflects the high cost of participation, not just in terms of W3C membership,³² but in terms of committing at least one person to engage in the weekly teleconference, the deluge of e-mails on the discussion list and the face-to-face meetings, which run 2.5 days.

It is also possible that the W3C Tracking Protection Working Group, while composed of talented, well-meaning and dedicated people, may simply not reflect the right mix of backgrounds, even among the companies represented. Significantly under-represented are those who could speak with authority to the real world trade-offs inherent in the many complicated decisions being made by the group—not enough business experts, no economists, and too many privacy advocates full of good intentions but lacking in real-world grounding. The stakes could scarcely be higher, with regulator standing ready to implement the outcome of the process, regardless of whether it is well-suited to the problems at hand.

Further, the process has proven highly unwieldy, given the large number of people involved and the large policy implications of the questions being debated—which were amplified considerably by Microsoft’s decision to switch to Default DNT-On.

Still, for all its flaws, it may prove—to paraphrase Winston Churchill on democracy—that the W3C process is the worst possible process—except for all the others. Certainly, it is a better option than having the FTC design a DNT mechanism on its own, as has been proposed in pending legislation.³³

I explain all these concerns in more detail below.

VII. The Dangers of Default DNT-On

Default DNT-On is supposed to empower users but in fact, it simply empowers browser makers to force a fundamental change in the Internet ecosystem, from to-

April 2, 2012, <http://techfreedom.org/sites/default/files/Comments%20to%20NTIA%20on%20Self-Regulatory%20Process%204.2.12.pdf>.

³⁰Dissenting Statement of Commissioner J. Thomas Rosch, Issuance of Federal Trade Commission Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Mar. 26, 2012, at 6, available at <http://www.ftc.gov/speeches/rosch/120326privacyreport.pdf>.

³¹Concurring Statement of Commissioner J. Thomas Rosch, Issuance of Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Dec. 1, 2010, at E-3, available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

³²A U.S. company with over \$50 million in annual revenue must pay \$68,500/year, while smaller companies must pay \$7900, and startups with fewer than ten employees and \$3 million in annual revenue pay \$2250. W3C, Membership Fees, <http://www.w3.org/Consortium/fees?country=United+States&quarter=04-01&year=2012#results> (last visited June 26, 2012).

³³H.R. 654, Do Not Track Me Online Act, available at <http://hdl.loc.gov/loc.uscongress/legislation.112hr654>.

day's low-friction, flat ecosystem of independent sites and services funded by impersonal data collection to one with fewer players who collect more data—"opt-in dystopias."

Since last September, the W3C has been developing a technical standard for Do Not Track (DNT) headers that would "allow a user to express their personal preference regarding cross-site tracking." The W3C process was based on the idea that the DNT mechanism "must reflect the user's preference." Similarly, the DAA commitment was premised on the idea that the user has "affirmatively chosen to exercise a uniform choice with the browser based tool."³⁴ Simply put, users, not browsers, should choose to opt-out of the data collection that creates so much value for consumers.

Microsoft breached this consensus on user choice when it announced last month that its new IE10 browser would send DNT:1 headers by default. This risks derailing the entire W3C process. Just the day before Microsoft's announcement, at the weekly W3C teleconference, privacy researcher Lauren Gelman attempted to allay industry concerns that the spec might go too far by saying: "realistically, majority default DNT is not the world this standard will exist in. DNT is going to be a 10 percent solution"³⁵—a view overwhelmingly shared by participants.

While Microsoft's stated commitment to user empowerment is laudable, Default DNT-On doesn't empower users any more than turning on ad blocking by default would. Anyone who cares can quite easily choose to make that choice. Below a certain threshold of DNT adoption, few sites will find it worthwhile to charge, block or negotiate with those privacy-sensitive users who turn on DNT. But no-cost opt-outs and implicit *quid pro quos* don't scale: beyond a certain point, sites will have to make *quid pro quos* explicit to gain opt-ins (technically, exceptions to DNT). In other words, a significantly higher DNT adoption rate will take us past a tipping point to an opt-in world.

Some downplay the significance of this change, arguing that Default DNT-On will simply force negotiations between sites and users over granting exceptions³⁶—a key part of the DNT spec. But as I explained in my comments on the draft FTC privacy report in February 2011, such negotiations are not costless; they introduce considerable transactions costs ("friction"³⁷) into an ecosystem that currently works because it generated tiny amounts of value from enormous volumes of transactions. Economic theory suggests that forcing today's implicit *quid pro quo* to become explicit (by switching to DNT Default-On) could produce dramatically different outcomes. As I explained:

Much as I enjoy the rich irony of seeing those who are rarely thought of as free-marketeers essentially asserting that "markets" will simply, and quickly, "figure it out," I am less sanguine. The hallmark of a true free-marketeer is not a belief that markets work perfectly; indeed, it is precisely the opposite: an understanding that "failure" occurs all the time, but that government failure is generally worse, in terms of its full consequences, than "market" failure.³⁷

The first part of that lesson comes especially from the work of the economist Ronald Coase. . . who won his Nobel Prize for explaining that the way property rights are allocated and markets are structured determines the outcome of marketplace transactions.³⁸ For example, a rule that farmers bear the cost of stopping rancher's cattle from grazing on their farms by constructing fences will produce different outcomes—not merely different allocations of costs—from the opposite rule.

Coase's key insight was that, in a perfectly efficient market, the outcome would not depend upon such rules: To put this in terms of the privacy debate, the choice between, say, an opt-out rule and an opt-in rule for the collection or use of a particular kind of data (essentially a property right) would have no consequence because the parties to the transaction (say, website users and website owners) would express their "true" preferences perfectly, effortlessly and costlessly. But, of course, such frictionless nirvanas do not exist. The real world is defined by what Coase

³⁴ Digital Advertising Alliance, *supra* note 27.

³⁵ See Lauren Gelman, "Re: tracking-ISSUE-150: DNT conflicts from multiple user agents [Tracking Definitions and Compliance]", *public-tracking@w3.org* mailing list, May 30, 2012, <http://lists.w3.org/Archives/Public/public-tracking/2012May/0341.html>.

³⁶ Jonathan Mayer, "Do Not Track Is No Threat to Ad-Supported Businesses," Jan. 20, 2011, <http://cyberlaw.stanford.edu/node/6592>.

³⁷ Comments of Berin Szoka, on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, A Preliminary FTC Staff Report of the Bureau of Consumer Protection, Federal Trade Commission, February 18, 2011, <http://techfreedom.org/sites/default/files/TechFreedom%20FTC%20filing%202011-02-18.pdf>.

³⁸ Ronald A. Coase, *The Problem of Social Cost*, 3 *J.L. & Econ.* 1 (1960).

called “transactions costs”: search and information costs, bargaining and decision costs, policing and enforcement costs.

The transaction costs of implementing a “Do Not Track” mechanism above an acceptable loss threshold of adoption—where sites must create architectures of negotiation—are considerable: someone must design interfaces that make it clear to the user what their choice means, the user must consume that information and make a choice about tracking, websites must decide how to respond to various possible choices and be able to respond to users in various ways through an interface that is intelligible to users, and so on—all for what might seem like a “simple” negotiation to take place.

These problems are certainly not insurmountable—and, again, with the right engineering and thoughtful user interface design a “Do Not Track” mechanism could well prove a useful tool for expressing user choice. But when we look at the world through Coase’s eyes, we begin to understand how mechanism design can radically alter outcomes (in this case, funding for websites).

Put simply, Default DNT-On could take us from a world in which users can freely browse content and services offered by a thriving ecosystem of publishers to a bordered Internet. Users will either have to pay or opt-in to tracking. In this worst-case opt-in “dystopia,” consumers could be made significantly worse off in three primary ways.

First, to the extent publishers have to rely on micropayments or subscriptions, their revenues will likely drop. Information goods have a marginal cost of zero, and therefore competition tends to drive their marginal cost to zero. Put more simply: unless you have a unique good protected by copyright, it’s hard to charge for it (and charging for many small transactions itself creates high transactions costs). Advertising has always solved this problem by monetizing attention, but advertising online is worth three or more times more when it is tailored to users’ interests.³⁹ Many sites that rely on this revenue will simply disappear, or be consolidated into larger media companies. Consumers will have fewer, poorer choices.

Second, those sites and data companies that are able to obtain opt-ins will likely collect *more* data in ways that are more personal than today. While opt-ins sound great in theory, they simply do not protect privacy in the real world. As Betsy Masiello and Nicklas Lundblad explained in their seminal paper about “Opt-In Dystopias”:

opt-in regimes . . . are invasive and costly for the user and can encourage service providers to minimise the number of times opt-in is requested. This can have at least two adverse effects.

The first is that 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.⁴⁰

The DNT spec allows sites to negotiate with users to grant exceptions to DNT as an explicit *quid pro quo* for access to content or services. But this could rapidly become complex given the need for users to manage exceptions for multiple sites and services:

As this happens we are likely to see demand rise for single identity systems. . . . It is possible that emerging social web services could comply by setting up the opt-in as a part of the account registration process, as discussed earlier. Users have an incentive to opt-in because they want to evaluate the service; after opting-in, a user is able to make an evaluation of the service, but by that point has already completed the negotiation. The service, having already acquired the mandatory opt-in consent, has no incentive to enable users to renegotiate their choice.

The data collection in this instance would all be tied to a central identity and would be likely to have excessive scope and deep use conditions. One unintended consequence of a mandatory opt-in regime might be the emergence of

³⁹See, Howard Beales, *The Value of Behavioral Targeting*, March 2010, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

⁴⁰N Lundblad and B Masiello, “Opt-in Dystopias”, (2010) 7:1 SCRIPTed 155, <http://www.law.ed.ac.uk/ahrc/scripted/vol7-1/lundblad.asp>.

tethered identities, whereby a user's identity is tightly coupled with a particular social platform or service. . . .

From a privacy point of view, tethered identities present many challenges. The concept suggests that all behaviour is tied to a single entry in a database. The ease of executing an overly broad law enforcement request would be far greater than in a regime of fragmented and unauthenticated data collection. The degree of behaviour upon which an advertisement might be targeted would also be far greater. And the threat of exposure posed by a security breach would also increase.

Third, few publishers and data-driven companies will be able to obtain opt-in exceptions to DNT. This will force unprecedented consolidation in the Internet ecosystem, both among publishers and among companies that use and process data for advertising, research and other purposes. As Masiello and Lundblad explain:

A worst-case consequence of widespread opt-in models would be the balkanisation of the web. As already discussed, some degree of data collection is necessary to run many of today's leading web services. Those that require account registration, such as social web services, enjoy an easy mechanism for securing opt-in consent and would be likely to benefit disproportionately from a mandatory opt-in policy.

If we believe that mandatory opt-in policies would disproportionately benefit authenticated services, we might also expect balkanisation of these services to occur. When information services are open and based on opt-out, there are incentives to provide users the best experience possible or they will take their information elsewhere. When these services are closed and based on opt-in, there are incentives to induce lock-in to prevent users from switching services. Users might be reluctant to leave a service they have evaluated and invested in; the more investment made the more likely a user is to stay with the current provider. We might expect mobility to decrease, with negative effects for competition and consumer value.

Simply put, Default DNT-On is likely to drive the adoption of federated content networks, and the evolution of highly decentralized websites and services towards an apps based model—such as on mobile phones and such as Microsoft is introducing in Windows 8—in which advertising is delivered by the app platform operator. This might or might be a good thing on net, but again, the point is that no one really knows, even as we tumble blindly down this path.

With the best of intentions, we are heading towards reshaping the fundamentals of the Internet—in ways that may have serious negative unintended consequences for privacy, the sites and services consumers enjoy, and the health of the ecosystem. But the *way* we're doing it may be even more troubling. This is not the result of a bottom-up evolutionary process, but of collusion between government and powerful market players. In the name of self-regulation, we are essentially moving toward the European model of co-regulation: where governments steer and industry rows, and where powerful incumbents use market power to serve their own agendas, with the blessing of government.

The Federal Trade Commission called for a Do Not Track mechanism in its draft privacy report, issued in December 2010. Chairman Leibowitz and David Vladeck, Director of the FTC's Bureau of Consumer Protection, have taken credit for pressuring industry to come to the table on DNT.⁴¹ The agency has played an active role in the W3C process. FTC Chief Technologist Ed Felten opened day two of the most recent W3C meeting by telling participants what the FTC wanted. Chairman Leibowitz and Commissioner Julie Brill delivered keynote addresses at the two prior meetings. Commissioner Brill, in particular, has pushed the W3C process to change the nature of the DNT spec to limit not just how data can be used, but what data can be collected in the first place. Representatives Ed Markey and Joe Barton have gone even further, sending a letter to the W3C Tracking Protection Working Group during its last meeting urging not only heavy restrictions on collection, but also that DNT:1 be turned on default.⁴²

The FTC has clearly been turning the screws on companies to agree to comply with DNT—even before a standard exists. The FTC showed its hand in Twitter's

⁴¹Federal Trade Commission, FTC Testifies on Do Not Track Legislation, Dec. 2, 2010, <http://www.ftc.gov/opa/2010/12/dnttestimony.shtm>.

⁴²Letter from Congressmen Edward J. Markey and Joe Barton to World Wide Web Consortium Tracking Protection Working Group, June 19, 2012, available at <http://markey.house.gov/sites/markey.house.gov/files/documents/%206-19-12%20Letter%20from%20Rep%20Markey%20and%20Barton%20-%20W3C%20.pdf>.

agreement to recognize DNT in May,⁴³ when FTC Chief Technologist Ed Felten announced the deal himself even before Twitter could do so. Faced with the FTC's open antitrust investigation, and the agency's essentially unchecked ability to bring privacy complaints against the company, at a real cost to its reputation, it's not hard to see why Twitter might be susceptible to . . . encouragement from the well-meaning folks at the FTC.

So one has to wonder what role Chairman Leibowitz, and members of Congress like Representatives Barton and Markey, might have had in convincing Microsoft to break ranks from the W3C process—even if that risked derailing the process itself.

This is, of course, speculative—but not without any basis. At the very least, Congress should ask the FTC to explain exactly what its role has been throughout this process. Further, Congress should call on the agency's leadership to repudiate the disturbing argument made by Tim Wu in defense of “agency threats” as a valid form of extra-legal regulation.

VIII. Conclusion

There are no silver bullets. Neither self-regulation nor relying on Section V is without pitfalls. But together, and working in conjunction with market forces like reputation, with targeted legislative solutions, and with technological change itself, they form a layered approach to dealing with privacy that is more likely to protect us from true privacy harms without killing the goose that laid the golden egg.

Senator KLOBUCHAR. Thank you very much, Mr. Szoka.

Thank you, all of you.

And I just want to clarify something after listening to Mr. Szoka's testimony, maybe with you, Mr. Liodice.

The FTC isn't actually regulating this right now. Is that correct? I mean, what is happening? Because it's my impression that they are allowing the industry to engage in some of this self-regulation and put a policy forward. Could you give me your views on that?

Mr. LIODICE. Sure, yes. Thank you.

We've had many collaborations with the FTC over the past few years. In fact, the FTC has essentially provided the information necessary as to certain directions that we have needed to head in.

So it has been an ongoing collaboration with the FTC. And our self-regulatory mechanisms have evolved appropriately with the encouragement of the FTC.

There admittedly had been times where there has been dissatisfaction. And through their encouragement, we continue to press on, build the technologies, and to complete the system to the current capability that we currently have.

Senator KLOBUCHAR. OK. And I understand that some in the on-line advertising and technology industry, particularly those who have been negotiating at the WC3, believe that industry self-regulation is possible and that the industry can coalesce around an opt-in regime. What do you think the chances are of stakeholders coming together without congressional or FTC action to develop an opt-in regime?

Mr. LIODICE. To develop an opt-in regime we think is against the interest of commerce. We believe that the current opt-out philosophy that we are currently structured around and succeeding with is the right way to go.

We have demonstrated that the industry can come together. We represent a consortium of 5,000 corporations with many different interests, with many different focal points. And to be able to bring

⁴³Michelle Maltais, “Twitter supports ‘do not track’” *Los Angeles Times*, May 17, 2012, available at <http://articles.latimes.com/2012/may/17/business/la-fi-tn-twitter-do-not-track-20120517>.

that level of the business community together to create a system that, in fact, is working, not only for business but, most importantly, for consumers, is something that this industry is extraordinarily proud of.

Senator KLOBUCHAR. Mr. Fowler, both the FTC and the White House reports mention the possibility of privacy practice becoming a consideration actually for consumers deciding between devices and services. And I think that the Microsoft announcement and other things would demonstrate that.

Have you seen significant data suggesting consumers already choose services, particularly online, based on privacy practices?

Mr. FOWLER. I think there is a lot of data that shows that consumers do make decisions based on data practices. I think within our own user base, we are just in the process of completing an analysis of a survey that we did, where we had 10,000 of our users provide input on what they thought about “do not track” and privacy and the types of tools that are available to them.

And what we found was very interesting. And we will be happy to share the results of that analysis once we’ve done our write-up.

But consumers do take privacy seriously. And they do feel that this is an important consideration for them as they browse the Internet, as they use services and applications.

And we found in the context of “do not track” that service providers, browsers, software manufacturers that provide “do not track” features actually lead to greater trust by the consumers who use it.

Senator KLOBUCHAR. Very good.

Privacy policies are important, but I think we all know that consumers don’t necessarily read them all. What efforts are being made to make them more accessible and easier to understand?

Maybe, Mr. Swire, you’d like to answer this as well?

Mr. SWIRE. Well, so privacy policies have another purpose besides the consumers, which is it lays out for all the employees, it lays out for the enforcers, it lays out for the rest of the world, what the privacy rules are going to be. And they also become the basis for how the Federal Trade Commission and the State AGs can step in if they’re breaking their promises.

The financial regulators had a good process to come up with a standard simplified privacy notice for Gramm-Leach-Bliley, much more like the kind of thing you see on the side of a soup can. And I think trying to find ways to have more standardized notices is something that everyone really supports.

Senator KLOBUCHAR. What about considerations for mobile devices that collect data, like smart phones and tablets?

Mr. SWIRE. Well, you know, it’s limited real estate on the smart phone. And I think that for mobile apps, people are really struggling with how to somehow convey it. Maybe over time we’ll see icons used a lot more. Maybe there will be video notice—I mean, audio notices. But I think that’s really something that needs a lot more work.

And they’re talking about mobile privacy as part of the mobile stakeholder process. We need more progress there.

Mr. LIODICE. If I may add to that, Senator?

We are moving very aggressively to adapt or identify principles for mobile. We clearly will need this in the future. We need it now. And so we're moving aggressively to ensure that the principles that we've established for the Internet will extend to the mobile world and ensure that we have absolute enforcement mechanisms in the same way that we currently have in the Internet self-regulatory sphere.

Senator KLOBUCHAR. So you would find some way to extend the opt-out principles and give the same options to those that have the small screens, such as tablets or smart phones—

Mr. LIODICE. Absolutely. Absolutely.

Senator KLOBUCHAR.—as they have on a typical computer?

Mr. LIODICE. There is no question that we're heading in that direction. We have processes underway to make sure that that happens. We will not rest until that does happen.

Senator KLOBUCHAR. OK.

Could anyone fill me in on how that's going to happen, just how you physically do that?

Mr. LIODICE. The technology?

Senator KLOBUCHAR. Yes.

Mr. LIODICE. We haven't developed it at this point in time, but we have developed a group that is examining this in a real-time basis.

The first step, as we did in the self-regulatory process that was established, is to ensure that the principles are appropriately constructed to meet the mobile platform, which is somewhat different than the current Internet digital platform.

Once those principles are established, we will leverage our technology partners that we've used to create the current monitoring, reporting, and accountability systems that will be moving into the unit that is eventually monitored by the Council of Better Business Bureaus.

Senator KLOBUCHAR. One last thing, Mr. Swire, and then I'm going to turn it over to Senate Ayotte.

Mr. SWIRE. So it does show on the mobile how hard it would be to opt out of every single company that maybe places an ad. It's just an awful lot of thumb work.

And having a more simple one way to do it, "do not track" or other expression of preference, becomes even more important, I think, in the mobile space.

Senator KLOBUCHAR. Thank you very much.

Senator Ayotte, and then we're going to Chairman Rockefeller, and then Senator Thune.

Senator AYOTTE. Thank you, Senator Klobuchar.

I wanted to ask Mr. Liodice, and I would like to hear all of your comments on this, certainly, in other contexts before this committee, I have expressed concern about how the FTC interprets its authority under Section V. That said, one thing I would like to hear from each of you on is, can you give me an example of a harm that has taken place regarding privacy that can't be adequately addressed by Section V by the FTC?

And how do you view the current law under Section V, in terms of using that as a mechanism of regulation, rather than creating all new legislation here?

So can you help me on that?

Mr. LIODICE. Sure.

Senator AYOTTE. What is it that Section V isn't protecting now?

Mr. SZOKA. May I jump in, Senator?

Senator AYOTTE. Sure.

Mr. SZOKA. First of all, thank you for your question. This does not get enough attention.

The entire debate, as I emphasize in my testimony, goes on as if we don't already have baseline consumer protection. And as I argue, the trick here is using Section V to its fullest extent and not beyond that.

And the problem, if I may say today, as you'll see if you look at any sort of privacy textbook, is, ultimately, you can look at what the FTC has done. You come up with what my colleague Charlie Kennedy summarizes as saying the list of "dos and don'ts" tell us which practices the FTC has challenged in the past, but does not provide a way of identifying those practices that might be challenged in the future. To me, that's the central problem.

Right now, the problem is not doctrine. It is the fact that the FTC is never challenged in court. And because of that, there are no courts to develop doctrine, and it falls ultimately upon the agency itself to explain its analysis to guide us. And that is precisely what I describe in my testimony as quasi-common law.

Now, to answer your question, I think there are cases that couldn't be dealt with adequately by unfairness, or at least that would stretch unfairness too far.

And just to give you one example, there's talk right now on the Hill of passing legislation that would bar employers from insisting that their employees give them their passwords to their Facebook accounts. I think that's the sort of thing that could actually make a good target for narrow legislation, something I would encourage this committee to look into.

I'm not saying that everything can or should be shoehorned into the unfairness doctrine, but I think unfairness can actually be used to do more today than it is being used without turning unfairness into what it was in the 1970s, which essentially was a blank check for the FTC to become a second national legislature.

Senator AYOTTE. Do other members of the panel have comments on that?

And certainly, Mr. Szoka, that's an issue that I've been concerned about in the past, of a blanket view of Section V.

Mr. SWIRE. Well, the simple point is, if it's not in the privacy policy, there's no deception claim. So a company says, "A, B, and C," and it leaves out the rest of the alphabet. They can do anything with the rest of the alphabet.

And there's no Administrative Procedure Act rulemaking authority in this area, so there's not a chance to get public comments and to have on the record an idea of what the rule should be or not be.

In the absence of that, the FTC, without rulemaking authority, has to go case-by-case, and they have no help on the rest of the alphabet after A, B, and C, if that's all the privacy policy says.

Mr. FOWLER. And if I could just build on that a little bit. I mean, we have a Ford Foundation grant that is a research project looking at first- and third-party tracking online.

The project includes a special add-on for Firefox browser called Collusion. I would encourage you to check out by going to www.mozilla.org/collusion. You or your staff can install it and look at your own webpages to see what kinds of tracking practices are in place.

And what we've found, without fail, is that a lot of organizations really don't have a clear picture of the types of data practices that their sites and applications are engaged in.

And so if you think about this question of Section V and what you've disclosed in your privacy policy, what we're finding is that those privacy policies remain static for too long. They don't reflect necessarily the day-to-day changes that happen in today's dynamic webpage and application environment.

Mr. LIODICE. And if I may build on that, I had to check with counsel, since I'm not a lawyer, to ensure my understanding of it as well.

Part of the beauty of what the self-regulatory mechanism provides is the flexibility to be able to track case-by-case and to be able to link that up with the principles that our marketers have to ascribe to. And if, in fact, they deviate from that, our reporting mechanisms provide the identification to our accountability mechanisms and our self-enforcement mechanism. And if, in fact, those changes or those violations of those principles don't occur, then we reference them back to the FTC.

But with the system that we have, we are able to get at cases and violations of principles that may have escaped the FTC's purview.

Mr. SZOKA. Senator, may I briefly add to that?

Everyone here likes to diminish the importance of case-by-case rulemaking. And I would agree that case-by-case rulemaking doesn't work if you don't explain your analysis. And that is precisely the world we live in today.

All we have is consent decrees that are essentially bald assertions that a company has does something unfair or deceptive. It would be a very simple matter for the FTC to simply do more in its analysis to explain that. If they don't have the resources, I, as somebody who believes in limited government and cutting spending probably more than anybody in this room, would be delighted to give them more funding to do that.

It is pennywise, pound foolish to give up on the existing model simply because the FTC doesn't have the time to explain to us what unfairness means. You could have a meaningful unfairness doctrine to deal with cases beyond what companies have promised if you simply did that.

And I've laid out four ways the FTC could do that. And I think that would be the best thing that this Congress could do to help the agency reach its full potential.

Senator AYOTTE. My time has expired. Appreciate it.

Senator KLOBUCHAR. Thank you. Chairman Rockefeller.

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

The CHAIRMAN [presiding]. Thank you, Madam Chair.

This isn't a question. Mr. Szoka, I have to admit a vast admiration for you. But I have a question at the end.

You're in love with the law. And I think you're in love with yourself. You declare yourself the most conservative person in the room, and I certainly would not argue that.

My question to you is, when you go through your complex legal machinations, for which I'm sure you're very well paid, do you ever think about the effect on consumers? You have not used the word "consumer" once, "user" once.

All you talk about is what works for corporations, what is unfair about FTC.

It's all about legal practices. There's nothing about people. I'm just really curious.

I'm not quite sure how you got on this panel, but you obviously slid by me.

Mr. SZOKA. Sir, I believe that the rule of law protects citizens. It is the bedrock of a free country, and that ultimately having agencies follow the law and work through legal means is something that protects consumers.

I also have explained today that what I admire, what I am in love with, is the idea that we use the law in consumer protection, that we have legal doctrines that do precisely what you're getting at, which is allow us to address real harm to consumers and weigh costs and benefits. That's well-established doctrine. I didn't make that up. The FTC did.

The CHAIRMAN. Thank you.

This is to Mr. Liodice and Mr. Swire. We had a May hearing, and I asked Chairman Leibowitz about the Digital Advertising Alliance's new self-regulatory initiative. And you know, going back to automobiles and all kinds of things, self-regulation is a matter of interest to this committee, because if it doesn't work, then we want to do something about it, at least some of us do.

And the alliances pledged to address the "do not track" request from Web browsers. And he made it very clear, that's Leibowitz, that if the alliance is going to honor a consumer's "do not track" request in a meaningful way, they'll have to stop collecting consumer information, period, except for some limited exceptions.

And I'm going to get into those limited exceptions in this or the next question.

In other words, what Leibowitz was saying was, it made it very clear that you had to do a "do not track," and it should mean "do not collect"—do not collect, do not track.

In other words, don't start. Don't get to the hundred different, you know, exercises of 5,000 different exercises with your thumbs that you have to do to get to what you want.

How do you respond to that?

Mr. LIODICE. Mr. Chairman, the Internet operates on some collection of data. And if a consumer opts out of any kind of information-gathering, there are necessary exceptions in order to be able to ensure that fraud protection, crime prevention, other systems that currently operate on the Internet need to continue to ensure that those law enforcement capabilities continue to exist.

The areas of exception that were noted in terms of market research are those that we had talked to the chairman about before.

And his staff and he believed that that was the right direction to go at that stage.

The one thing that I can say about self-regulation—

The CHAIRMAN. However, I don't think he—he said that these could be expanded almost to the point where the rule would be swallowed up.

Mr. LIODICE. Of course.

The CHAIRMAN. In other words, the definition is so broad, so inexplicably wide, that anything could fit in. So that he liked the concept of it, but there was a large “but”——

Mr. LIODICE. Right.

The CHAIRMAN.—which you have not referred to.

Mr. LIODICE. We would agree that boundaries need to be placed in this arena, because consumers need boundaries in order to understand exactly what their rights are, what their privileges are, and what their decisions need to be based upon.

And that's the reason why we've established the mechanisms for what we already are currently doing. If something is not working or not working as effectively, part of the word that I used before about our system is “evolutionary.” We've continued to evolve to address concerns from the very beginning of our development of the Digital Advertising Alliance self-regulatory system.

For example, on multisite data and mobile, we are evolving, based upon the concerns that have been addressed by legislators or the FTC or others.

The CHAIRMAN. But you would agree, would you not, that if Leibowitz's side concern—and that is that these two phrases could be used to sort of swallow up the whole intent of the rule—that it's better not to fiddle around with that?

Mr. LIODICE. No, what we would do is try to establish——

The CHAIRMAN. You would be——

Mr. LIODICE.—boundaries.

The CHAIRMAN. You're at DAA——

Mr. LIODICE. Yes.

The CHAIRMAN.—with 5,000 people who you say represent all kinds of different interests.

Mr. LIODICE. That's correct.

The CHAIRMAN. You've corralled them, like cats. But at some point, don't you, therefore, have to have something that says “do not track”?

Mr. LIODICE. No, I do not believe that that's the case, sir.

The CHAIRMAN. Why is that? Because that would put you out of business?

Mr. LIODICE. No.

The CHAIRMAN. I'm being a little cynical, but I'm being serious.

Mr. LIODICE. No, I understand. Exactly.

The key here is a question of how we approach limitations on that collection that is responsible, that addresses consumer interests. And as I mentioned before, one of the core interests that we have, in terms of “do not track,” is cybersecurity.

We cannot turn our backs on cybersecurity as an issue, because if, in fact, we do not track completely, and totally stop any type of information-gathering whatsoever, we run into serious problems in the way the Internet is managed.

The CHAIRMAN. I may want to explore that with you. My time is up.

Thank you, Madam Chair.

Senator KLOBUCHAR [presiding]. Thank you.

Senator Thune?

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

Senator THUNE. Thank you, Madam Chair.

And I want to thank our panelists today. I know I always welcome different perspectives. And divergence of opinions is a good thing. I think that benefits all of us as we try to make good and informed decisions, so thank you all for being here today.

Our most innovative companies of all kinds use data to improve their products, gain understanding of their customers, and make better and more informed decisionmaking. Data is behind all sorts of customization, innovation, that benefits consumers.

There was a report commissioned by Interactive Advertising Bureau recently that concluded that the Internet accounted for 15 percent of total U.S. GDP growth. And if the Internet were a national economy, by 2016, it would rank as the fifth largest economy in the world.

The advertisement-supported Internet contributes \$300 billion to the U.S. economy and has created about 3 million American jobs. At a time when we have sustained grim economic news, it has remained a very bright spot in the U.S. economy, and that trend continues.

And my concern is that if we try to rush a quick fix on the issue of privacy, rather than very thoughtfully and carefully dealing with the issue, we could stifle the very important economic advantage that we have in the United States.

My question is a fairly broad one, but I'd like to get your reaction to it. And that is, what are the risks if Congress adopts an overly restrictive European-type approach that stifles U.S. innovation?

Mr. LIODICE. If I may start, Senator Thune, that is, essentially, the core fear, that we lock in place what we currently have and not leave ourselves open to the evolution of technology.

Creativity and innovation is the basis for the Internet. And we recognize that, as part of our self-regulatory principles, we have to allow enough room and flexibility to adopt to a changing economy and rapidly changing technologies.

If we lock ourselves in place too rigidly, we may choke off the kind of innovation and creativity which is the basis for our dynamic U.S. economy, which, in the end, may cost jobs here in the United States and around the world, if, in fact, we don't have that flexible and open society.

Mr. SZOKA. Senator, while Senator Rockefeller might dislike my mentioning another law, let me mention the law of unintended consequences. And that is to say that what you are putting your finger on is that there are many competing values here for consumers.

We can do things that seem to be good for privacy that, in fact, end up hurting privacy, that hurt other values.

And as I explain in my written testimony, that fear is not only in the case of legislation such as you describe, but also in what

Congress and the FTC have been doing to push the “do not track” mechanism to be something other than what it was when it started.

In other words, as Senator Klobuchar suggested, if Congress sits here, and the FTC does, push it toward being an opt-in mechanism, you fundamentally change the nature of the Internet.

“Do not track” was intended to be a solution for people who felt privacy sensitive, who were concerned about that, and wanted to make that tradeoff.

Below a certain threshold, say 10 percent, that can be done for free. No one is going to bother changing mechanisms to negotiate with users.

Above a certain threshold—and that’s where we’re heading now, given Microsoft’s decision—you start to put in place a dynamic that changes what we have today. You start to create, instead of today’s ecosystem where you browse the Internet, you go anywhere you want, and there are no pay walls, there are no pop-ups, you instead have a system of opt-in consent.

And I think if you look at my testimony and if you look at the paper called “Opt-in Dystopias,” you see that, in fact, that’s a very bad world for consumers. It’s one in which there’s likely to be, ironically, more data collected.

Even though we’re intending to reduce data collection, you could have more collected by fewer parties in a less transparent way, while at the same time making the entire ecosystem worse off.

So, yes, I actually care very deeply about consumers. And I worry that we risk all of those things when either we pass legislation that is in the European model or we extort concessions from the private sector, as the FTC and others may be doing. They’re clearly pressuring companies to do things that they never intended to do, and, as Mr. Liodice is saying, have those unintended consequences.

Mr. SWIRE. Senator, last fall I testified in the House Energy and Commerce Committee on the European Union and U.S. and where jobs go. And my testimony concluded that a “we don’t care about privacy” approach, that if the U.S. says we’re not going to do it, that puts a lot of U.S. jobs and global leadership in this area at risk, because we get a risk being treated as locked out from a lot of markets around the world.

India now has privacy rules on the book. Most of Asia does. All of Europe does. And if the U.S. is considered a non-player, we could have U.S. companies shut out of a lot of markets. So we have to face in an international trade setting the reality that if we have a pretty good, credible system here that we can live with, we’ll also have a much better export system. And we have to figure that into the mix.

Mr. FOWLER. If I could just add, as a global software organization with consumers around the world, including Europe, the reality for compliance, the reality for establishing trust, is that we have to address the privacy compliance jurisdictional requirements that exist wherever we do business.

So while we’re not ready to say that we should have a European-style data protection regime in the U.S., we have one anyway, in the sense that we have to comply with that and respect those differences from a legal and cultural perspective when we’re inter-

acting with European customers. And that's true for all the leading Internet companies today.

Senator THUNE. I see my time has expired.

Thanks, Mr. Chairman.

The CHAIRMAN [presiding]. Thank you.

Senator Ayotte?

Senator AYOTTE. I wanted to follow up briefly—thank you, Mr. Chairman—on this idea, Mr. Liodice, that you mentioned about cybersecurity concerns. And if you could describe more where you see those concerns arising, if we were to legislate on the “do not track” issue.

Mr. LIODICE. Sure. It starts with the fundamental fact that the Internet operates on collecting data. And in order to be able to leverage the various components of our economy, of cybersecurity, of the effective management of the Internet, there needs to be appropriate data collection.

Now, the self-regulatory program that we're talking about essentially provides choice for the limitation of data with respect to advertising. But if we are not careful about how far that we extend the reach through legislation of limitations on data, there are law enforcement agencies that currently rely upon data that is collected currently over the Internet.

If we block or limit that ability, the unintended consequences may be the inability to prosecute fraud or not have as robust cybersecurity protections as we have currently at this moment in time.

So the point was that, if in fact legislation does come about, it needs to be done with great care to ensure that the data collection that currently exists for global opportunities, such as cybersecurity, fraud protection, et cetera, must be kept in place, if not become more robust.

Senator AYOTTE. As I hear it, and before I served in the Senate, I was a State attorney general, that you're referring to areas, for example, of sexual predators, identity theft. Are these the areas that you're—you know, when we think about—or are there other broader areas that you're concerned that law enforcement wouldn't be able to access data, because, obviously, in that regard—

Mr. LIODICE. Right.

Senator AYOTTE. I mean, I've worked on those cases. I've worked with the police on those cases. I understand the type of information that is used to hold individuals accountable that are misusing the Internet to commit crimes. And, certainly, that would not be a good consequence, if we were to legislate in that area, so law enforcement couldn't get access or that information wasn't somehow retained.

Mr. Swire?

Mr. SWIRE. So this issue of cybersecurity and information-sharing has been a great big issue in the cybersecurity legislation that this committee and others have been working on.

I had an op-ed in *The Hill* on this subject. And one of the concerns from the privacy side is that definitions are so broad of what counts as cybersecurity that this could be basically all clicks go to government. And some of the proposed language has even been,

notwithstanding all other laws, if it's related to cybersecurity, it goes to the government.

And I think that that's a very broad potential idea of what counts as cybersecurity. And it raises issues about government access to data that are really quite substantial.

Mr. SZOKA. And if I may also respond to this, I've joined forces with groups on the left—the ACLU, the Electronic Frontier Foundation—raising those very concerns about such cybersecurity legislation.

And once again, my concern is that the real harm here comes from government itself. And the way to deal with that is not to cripple law enforcement's access, nor to give it every piece of information it wants.

The solution, as is often the case here, is to ensure the rule of law, which is to say, we have the Fourth Amendment. We have a system for ensuring when government gets access to data, and we should respect that. Those are the values that, unfortunately, get left out of these conversations far too often.

We far too often focus on companies as vehicles for collecting data, fearing the government will get access to it, while doing nothing at all to ensure that government gets access through constitutional procedures.

Mr. FOWLER. If I could just add, I think that before we get too far into this, I think it's important to clarify that in the context of “do not track,” in behavioral advertising, we're not talking about security. We're talking about security of the data related to serving impressions, right? So it's a different type of data. And the security exemptions that are being discussed by the W3C and the DAA are specific and narrow to that type of data.

Senator AYOTTE. One of the concerns that I worry about, regardless of what your view is, whether to legislate or not to legislate in this area, is how we get it right, in the sense that, with the evolving technology. And as I said in my opening statement, as soon as we come up with something that we think solves the problem with the evolving of the technology, you know, that's what I worry so much about. That if we do it, certainly, if we legislate in this area, if we decide to legislate in this area, how do we get it right, so that it doesn't impede our economy or also make it worse for consumers?

Mr. LIODICE. If I may comment on that?

Senator AYOTTE. Thank you, Mr. Chair.

Mr. LIODICE. I'm sorry.

Senator AYOTTE. I think my time is up, so I certainly don't want to—

The CHAIRMAN. Go ahead.

Senator AYOTTE. I'm all set. Thank you.

The CHAIRMAN. OK. Thank you very much.

I just want to sort of declare the cybersecurity argument a total red herring. It has absolutely nothing to do with any of this. And the original cybersecurity bill, it was written by Olympia Snowe and myself and this committee. And that was 3 years ago. It's been negotiated and on and on and on.

The FTC, there are exceptions made that cover any cybersecurity matters, so that any use of that as an argument against “do not track” or whatever else is just off the wall, from my point of view.

Mr. Swire, your written testimony mentions a recent study of the 100 most popular websites that was conducted by researchers at Berkeley. The study found that these websites are collecting an astounding amount of information about their customers.

According to the researchers, 21 of the 100 top websites placed 100 or more cookies—this gets right to you—on users’ computers. That means that when an individual visits one of those websites, 100 or more different companies start to collect information about that person. Therefore, if you have to opt out, you have to do it 100 times. Therefore, why not just “do not track.”

Mr. Swire, do you believe that most consumers know how much information is being collected about them when they visit popular websites?

Mr. SWIRE. We have survey result studies that show that they don’t know, that if you ask them what they think is happening and then you sit them down and tell them, they’re quite surprised by how much more is being collected.

The CHAIRMAN. Wouldn’t it be your view, and maybe yours, too, Mr. Fowler, that the whole history—I mean, we do this with cramming and telephone companies, they all start out—I mean, United Healthcare has now announced grandly that they’re going to continue many of their policies.

Well, their policies happened to have created something called “Ingenix,” which would sort of sets the random market for how much healthcare costs all across the country. And they paid a \$350 million fine in New York State court, which is like admitting they were guilty. It’s a rather bad company. We’ve spent a lot of hearings and have spent a lot of time on them.

In other words, they say they’re going to continue, but you know they’re not. It’s great PR.

Companies say they’re going to crack down. Yes, they do for a period of time. But then as you indicated, at some point, it comes up against their own self-interest. And at that point, they usually crack, in my judgment.

Mr. Swire, tell me why I’m either right or wrong on that, or if I’m close.

Mr. SWIRE. Well, Senator, I’m in a hearing and you’re right. But seriously, the history has been that when you and the government are paying attention to these issues, and the press pays attention to these issues, that companies upgrade their efforts and pay more attention to enforcement.

And then when some different issue becomes the center of attention, these don’t get as much attention. And if you don’t—

The CHAIRMAN. And so answer that in terms of—what we’re talking about is that you don’t sort of have an off and on switch. You do something called legislate “do not track.”

Mr. SWIRE. And that’s what, for instance, has happened for CAN-SPAM and for the Children’s Online Privacy. The Federal Trade Commission got the ability to write rules and everybody got a right to comment on them. And both of those regimes have been pretty steady. Those haven’t been huge flashpoints. We have

COPPA. We have CAN-SPAM. They do what they do, and it's been working reasonably well.

The CHAIRMAN. Reasonably well. On the other hand, Facebook, which is, as I understand, a fairly profitable company, has a rule in which they say that no kid under the age of 13 can be allowed to expose themselves and, you know, all the bullying, sometimes leading to suicides, all kinds of things have happened. On the other hand, they don't stop it.

Mr. SWIRE. Well, then so that's a reason to revisit things. That was a 1998 statute, and so then, periodically, you come back to these things, as you do in lots and lots of other issues.

But if you don't come back ever, then what we've seen is that the level of effort from industry really has fallen down in the periods when attention was elsewhere.

The CHAIRMAN. Yes, sir?

Mr. FOWLER. So if I might add, I think from our perspective and as we look more into consumer values as it relates to personalization, interest-based ads, and so forth, I don't think we're at the point yet where we have the same kind of consumer or public backlash that we've had with CAN-SPAM and Do Not Call. I think there's still an opportunity here.

And some research backs this up, that we have a polarized set of consumers on both ends that are very surprised and uncomfortable by tracking online, and others who are very excited about engaging in personalized content and services. And we have a much larger, in fact, the bulk of the consumer market, that's somewhere in the middle, and, ultimately, will decide based on the value they receive and how transparent those mechanisms are.

So I think we're at a point where the discussions that we're having with the W3C, we have an opportunity to address this through technology and changes in industry practices that create more transparency.

The CHAIRMAN. And then how would you handle the small-print problem?

Mr. FOWLER. Maybe if you could say a little bit more, so I understand exactly the nature of the question?

The CHAIRMAN. You know, people don't read it.

Mr. FOWLER. Oh, small print. OK.

The CHAIRMAN. They don't have the time to read it. And if they read it, they can't understand it.

Mr. FOWLER. Right. In my written—

The CHAIRMAN. If they can see it.

Mr. FOWLER. Yes. In my written testimony, I talk about some of the failures related to the notice and choice model. Again, I feel that there is a lot of innovation that's yet to happen.

From a Mozilla perspective, we're doing a lot of investment in mobile and application notices, looking at in-context notices, as opposed to small print that the consumer has to find and try to understand.

The first time they start to interact with a new feature or they see a particular kind of behavior or conduct happening at a site is, from our perspective, an opportunity to reinforce what choices they have, how to configure the tools that are available to them, and what to ask for from the sites.

So I think that we still have more room for innovation. And I think there's still opportunity to educate consumers. And hopefully, mobile and applications will give us a platform to really see some of that happen.

The CHAIRMAN. This committee really works very hard on consumer protection. I mean, I'm very open about that. It used to be a little bit different. Now it's very clear in its direction.

So naturally, that colors the way we approach things. We really bear in on consumers. What are they capable of doing? What are they capable of understanding? What's beyond their reach? What's not fair? Et cetera, et cetera.

And my sort of favorite example, which we're actually working on quite hard, is moving companies. You decide to move, and you don't particularly look—you just sign a piece paper that says that you accept their contract. But it's kind of a low bid. And because you're not wealthy, you take that low bid because, after all, furniture on a truck trucked to the next destination is not very hard. But what happens so often is that the trucks just stop halfway through and say, if you want your furniture, you've got to pay us another \$2,000.

That's, Mr. Szoka, what I mean when I say that our concern is about consumers.

You have to sometimes go a far piece to make sure that they get the help that they flat out deserve—their lives are far too miserable and difficult these days to possibly figure out for themselves how to protect themselves.

So it does become the role of government. It's like children that are in extreme hunger. There are millions of them across this country. Should the government stay away from that until the free market can sort it out? Or should the government actually say, no, this is something that is not good, this affects the way our future brains will develop and all the rest of that, and we do something about it.

And we have a little bit of that bent in this committee, at least, on this side, a little less on the other side, but surprisingly on the other side, happily on the other side, also.

So let me just thank you all for taking the time to come.

Mr. Szoka, I was very rude to you, and I'll write you a letter of apology, if you wish. I really will.

Mr. SZOKA. Could I just say one final thing, Senator?

The CHAIRMAN. No.

[Laughter.]

The CHAIRMAN. And I'll write a letter of apology for that, too.

[Laughter.]

The CHAIRMAN. But thank you for taking the time, very, very much. We're all sort of focused on what the Supreme Court has just done, which you're all aware of, right?

So this hearing is adjourned. Thank you.

[Whereupon, at 11:10 a.m., the hearing was adjourned.]

A P P E N D I X

STATEMENT OF COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

Self-regulation is a vital part of consumer privacy protection, and the World Wide Web Consortium's current work on a Do Not Track standard, along with the Digital Advertising Alliance's agreement to honor a DNT header, are good examples of the power of this method. The Computer and Communications Industry is a 40 year-old international non-profit trade association dedicated to open markets, open systems, and open networks. CCIA members participate in many sectors of the computer, information technology, and telecommunications industries and range in size from small entrepreneurial firms to some of the largest in the industry. CCIA members employ nearly half a million workers and generate approximately a quarter of a trillion dollars in annual revenue.¹ Our members produce web browsers, operate search engines and e-commerce websites, are Internet advertisers, and offer free web services of many kinds.

Consumer choice regarding the use of personal data is of the utmost importance. Users should have the ability to opt-out of systems that impact their privacy if they're uncomfortable. This is important not just for reasons of pure privacy protection, but also because trust is so essential to the online marketplace. Users who don't trust an online service have many other competitors to choose from and can always take their business to another, more privacy protecting, website.

Do Not Track options are an important part of consumer choice. These options allow users to indicate their preferences with regard to online tracking through a simple browser mechanism that is easy to set, universal, and permanent. A broad coalition of advertisers, brought together by government acting as a convener has agreed to honor the Do Not Track header. The World Wide Web Consortium (W3C), a multi-stakeholder body responsible for Web-wide technical protocols, is in the process of developing the specifications that will underpin the DNT header. This past week the W3C conducted a number of days of meetings surrounding the DNT header, and made progress on some of the remaining issues. A few outstanding questions remain to be answered before the specification is finalized.

As such, the W3C process is an example of a successful self-regulatory program. There are many different voices in the room there, each with strong opinions, but progress is being made and while the outcome is not yet certain, there is some confidence that an eventual agreement may be reached. There may be parties on all sides who are not entirely happy with the final result, but on the whole it will be a product of compromise and be a great step forward for privacy on the Internet.

In a parallel self-regulatory effort, a group of advertisers has come together called the Digital Advertising Alliance (DAA). The DAA has worked with government conveners to reach an agreement, backed by Section 5 of the FTC Act, to respect the DNT header. Self-regulation is alive and well in the tracking space, with companies, government, and civil society all collaborating to develop workable frameworks that protect users.

CCIA has two areas in which we wish to highlight concerns about the Do Not Track conversation. While the ongoing W3C process is a positive one, there are still a few areas where uncertainty remains, and where a wrong decision could have unintended consequences. By mentioning these areas, we hope to help avoid those consequences.

First is the question of exceptions to Do Not Track. The setting of a Do Not Track header, while it is an important consumer protection tool, cannot be a universal sign that a user will never have some traces kept surrounding their use of websites. There are important business reasons to monitor customer use of websites that should not be preempted by a Do Not Track header. For example, a lot of users' actions on websites are stored in order to combat fraud or cheating. Financial

¹For a full CCIA member list, please see <http://www.cciainet.org/index.asp?bid=11>.

websites as well as essentially any online merchant must keep track of a certain amount of information about visitors in order to protect the entirety of their users.

For another example, the vast majority of websites anonymously track how users move around their own website in order to study their layout and usage statistics. We all reap the benefits of this tracking in the form of better website design and navigation, and website operators can improve their businesses by making sure visitors are finding the pages they need easily and quickly. This can be analogized to a retail store studying how anonymous visitors move through the store in order to decide if any changes need to be made to the layout of the products.

The second important aspect of Do Not Track is in user education. Do Not Track's focus is on the privacy implications of what can be collected on the Web while a user browses. That information is of course important to a user and should be a subject of education without a doubt. The problem here stems from what is not being adequately explained to users, and that is the value that comes from anonymized data. Advertising targeted toward what a person likes and enjoys pays for a huge amount of content and services on the World Wide Web that are offered for free to users. Without that source of revenue, innovation in online services would be much harder to come by as the price of starting up a new service and gaining customers willing to pay would be drastically higher.

Data isn't just important for advertising purposes. Collecting large amounts of anonymized data can open up worlds of research that users are not aware of. A famous example is Google's Flu Trends, in computers analyze live queries coming from distinct geographical areas, highlighting people who are searching the Internet for flu symptoms. In this manner, Google can often predict flu outbreaks before even the Centers for Disease Control. Amazon and Netflix each do similar analysis when they help each of us find new books, movies, and music we might like, based on what thousands of other people have also enjoyed. This sort of data collection and analysis poses no real privacy threat, yet provides an invaluable public service.

Users today, however, are not presented with this side of data collection and are making decisions about privacy protection without understand this inherent trade-off. If a user is fully educated and then makes a decision to remove herself from data ecosystem, that is a choice that should be respected, but the education must come first so that decision is informed.

