This is a preliminary transcript of a Committee hearing. It has not yet been subject to a review process to ensure that the statements within are appropriately attributed to the witness or member of Congress who made them, to determine whether there are any inconsistencies between the statement within and what was actually said at the proceeding, or to make any other corrections to ensure the accuracy of the record.

RPTS BLAZEJEWSKI

DCMN SECKMAN

UNDERSTANDING CONSUMER ATTITUDES ABOUT PRIVACY

THURSDAY, OCTOBER 13, 2011

House of Representatives,

Subcommittee on Oversight

and Investigations,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 9:06 a.m., in Room 2123, Rayburn House Office Building, Hon. Cliff Stearns [chairman of the subcommittee] presiding.

Present: Representatives Bono Mack, Blackburn, Stearns, Bass, Harper, Lance, Cassidy, Guthrie, Olson, Pompeo, Kinzinger, Barton, Butterfield, Gonzalez, Matheson, Dingell, and Towns.

Staff Present: Jim Barnette, General Counsel; Brian McCullough, Sr. Professional Staff Member, CMT; Jeff Mortier, Professional Staff Member; Gib Mullan, Chief Counsel, CMT; Andrew Powaleny, Press

Assistant; Brett Scott, Staff Assistant; Shannon Weinberg, Counsel, CMT; Tom Wilbur, Staff Assistant; Alex Yergin, Legislative Clerk; Michelle Ash, Democratic Chief Counsel; Felipe Mendoza, Democratic Counsel; and Will Wallace, Democratic Policy Analyst.

Mrs. Bono Mack. The subcommittee will now come to order. That makes it quiet down real quick.

This is the fourth in our ongoing series of hearings on online privacy. When our work is finally finished, my goal is to point to a better way to protect consumer privacy and to promote e-commerce at the same time. In the end, this will benefit both American consumers and American businesses and preserve a strongly held belief all across our Nation and around the world that the Internet should remain free.

The chair will now recognize herself for an opening statement.

When it comes to online privacy, at least for me, consumer attitudes and expectations are the bits and the bytes that matter the most. Do Americans really believe enough is being done today to protect their online privacy? Are they taking advantage of the many privacy tools currently available to them? Do they even know about these tools? If not, why not? And do these privacy features for the most part really work? Or is it time for Congress to finally legislate in this area? This is a hearing that I have been looking forward to for a very long time because it is the first time we tried to quantify what consumers expect and want. This is where the rubber hits the road with respect to online privacy.

Today there is no single Federal law expressly governing all data collection in the United States. Instead, there is a confusing hodgepodge of more than 300 State and Federal laws. Likewise, there is no single regulator to enforce all these privacy-related laws. Rather, an industry-specific approach has emerged whereby Congress has

restricted consumer data collection and use by subject matter and provided the enforcement authority to the relevant Federal agency.

As it stands today, the Federal Trade Commission arguably has the broadest jurisdiction to enforce general privacy violations under its Section 5 authority, defining unfair or deceptive acts or practices.

Since 2001 the commission has brought 34 cases against companies that failed to protect consumer information, including when companies fail to adhere to their own stated privacy policy. In recent years, both policymakers and stakeholders have expressed increasing concerns regarding the collection and availability of consumers' personal information online. Increased data collection and storage by Web sites, information brokers, direct marketers, ISPs, and advertisers have been driven in large part by the rapid decline of the associated costs of data processing and storage, while at the same time the value of consumer information has increased significantly.

As we know, data about consumers' online behavior is being used today to target ads, increasing the likelihood of a sale of a particular product. Is this bad? Not necessarily. But is this process transparent enough and do consumers have enough information and tools available to them to be able to opt out of having their data collected and shared with unknown parties if they so choose? In many ways, this is the very root of the privacy issue.

In response to growing concerns over online data collection and use, particularly regarding behavioral advertising, the online advertising community developed a self-regulatory model to provide

consumers with notice and choice about advertisements delivered to them through behavioral targeting.

The Digital Advertising Alliance developed and implemented these so-called about ads to provide consumers more information on why they are seeing a particular ad and to provide them a mechanism to opt out of future ads directed at them based on behavioral advertising.

Later, the FTC took things a step further, proposing a number of principles to enhance consumer choices regarding privacy, including the concept of a "do not track" mechanism.

Since the hearing in the last Congress on "do not track" legislation, the two most popular browser developers, Microsoft's Internet Explorer and Mozilla's Firefox, have both designed and incorporated a "do not track" feature into their browsers. These features are user-controlled, so consumers must choose to turn them on to actually prevent tracking.

Internet Explorer blocks content from sites that are on tracking protection lists, and it could otherwise use the content to collect information. Mozilla's Firefox broadcasts its signal to each Web site a consumer actually visits, communicating the consumer's desire not to have his or her information collected.

Clearly, the effectiveness of Mozilla's approach faces significant hurdles because every Web site that receives a signal from the consumer's browser must choose to honor their request, and currently, there is no requirement that Web sites must do so.

So what do consumers think about all of this? And when it comes

to the Internet, how do we, as Congress and as Americans, balance the need to remain innovative with the need to protect privacy? Clearly, the explosive growth of technology has made it possible to collect information about consumers in increasingly sophisticated ways. Sometimes the collection and use of this information is extremely beneficial; other times it is not.

Despite everything that I have heard in our previous hearings, I still remain somewhat skeptical right now of both industry and government. Frankly, I don't believe industry has proven that it is doing enough to protect American consumers, while government, unfortunately, tends to overreach whenever it comes to new regulations.

That is why I am so anxious today to hit the refresh key to learn the latest about consumer attitudes and expectations.

And with that, I am happy to recognize the gentleman from North Carolina, Mr. Butterfield, for his opening statement for 5 minutes.

Mr. Butterfield. Let me thank you, Chairman Bono Mack, for holding this very important hearing today.

This is no doubt a very important issue to all of us. You spoke with me when we first started this subcommittee at the beginning of the session, and you told me of your keen interest in this issue, and I want to thank you for pursuing this hearing today.

This forum provides an opportunity to look at expectations and attitudes about privacy from a consumer's point of view, and these witnesses that we have today, all six of them, will no doubt share with us some very valuable perspectives.

The bottom line is that consumers want and expect privacy. Whether they are online, hopping from one Web site to another, or buying a few things at a chain grocery store, but sometimes, the privacy consumers expect isn't respected. For example, the information collection practices by online tracking firms for purposes of behavioral advertising aren't generally visible to consumers, and with those consumers that know it is happening don't always know how to achieve the level of privacy they want with the tools available to them.

I understand that online advertising is big business. We all know that. Last year revenue from all types of online and advertising totaled $26 billion. This revenue helps to support free access to a lot of the online content consumers have come to expect. A small but growing segment of this revenue is coming from behavioral advertising, and I think most of us by now understand how that works, but let me nonetheless try to describe it in my own way.

Imagine that I am in the market for a new car, let's say a Ford Explorer. Since I drive a 2000 Ford Explorer, let's say I am in the market for another Ford Explorer. I visit some online car comparison Web sites, and there are many. I visit the manufacturer's Web site, and then I decide to put off buying a car for another day or two. I go to the Web site of a daily newspaper, and all of a sudden there are advertisements on some of the pages for, you guessed it, a Ford Explorer.

This happens through the installation of cookies on my computer, although some of the industry have resorted to more persistent and less

visible tracking tools. Those cookies allow an advertiser to track my online activities across multiple Web sites and ultimately serve me up a tailored advertisement for a vehicle that I had previously expressed an interest.

I appreciate the amazing business opportunities made possible by behavioral advertising. I understand that consumers are probably more likely to purchase goods and services after seeing an advertisement if it is relevant to their likes and interests.

However, a leading academic study of consumer attitudes toward behavioral advertising found they don't want it. That study found that 66 percent of survey participants did not want tailored advertising. The number that didn't want tailored advertising jumped to 84 percent when participants were asked if it would be okay to base that tailoring off of tracking a consumer's activities across Web sites. The number jumped to 86 percent when participants were asked if it would be okay to base tailor the advertising on offline activities, like using a discount card at the grocery store.

One thing is clear, consumers aren't clamoring for tailored advertising, and they become more uncomfortable with it when asked about the sorts of tracking activities that enable it. The finding of another study on consumer attitudes sums it up best: 64 percent of participants agreed that someone keeping track of my activities online is invasive, while only 4 percent disagree.

I will be clear. I support the online advertising industry, I have told them that, and respect the central role that ads play in

supporting a free Internet ecosystem. However, I strongly believe that consumers have the right to know upfront when their online activities are being tracked, what activities are being tracked, and what that information will be used for as well as the option to opt out of having their information collected entirely, not just from receiving targeted ads.

The online advertising industry has responded to privacy concerns by creating a self-regulatory program for behavioral advertising that provides consumers with Web sites and that allows them to opt out from receiving behavioral advertising from companies, from participating companies. I appreciate this effort.

I still feel strongly that a national baseline privacy law is the best way to ensure consumers have basic common sense and permanent rights over the collection and use of their information.

Again, thank you, Madam Chair. I yield back.

Mrs. Bono Mack. I thank the gentleman.

And the chair recognizes the gentlelady from Tennessee, Ms. Blackburn, for 5 minutes.

Mrs. Blackburn. Thank you, Madam Chairman.

I want to welcome all of our witnesses here today. We are delighted to have you here to participate in this discussion, and as we talk about tech policy and the virtual marketplace today, we are talking about government regulating the use of data and what that interface is going to be.

As we worked through this issue, as the chairwoman said, this is

our fourth hearing on this, I have decided that this data should be treated as a natural resource and that the DNA of this data is very powerful. It really is the lifeblood of a thriving Internet economy.

So here are some questions for you. Should we allow our free market to explore this natural resource and learn to commercialize it, protect it, and respect it, or are we going to restrict it altogether? Why should government be the decision-maker? Government seems to know so little. It reacts slowly, works poorly, and I was reading a quote from one of my favorite economists, F. A. Hayek, Friedrich Hayek, who wrote the book, "Road to Serfdom," and as I had to remind a college student recently, that is s-e-r-f-d-o-m, not s-u-r-f-d-o-m. Let me give you this quote: It is the curious task of economics is to demonstrate to men how little they really know about what they imagine they can design, end quote. I think that is very relevant to this discussion that we are having about privacy in the virtual marketplace.

We don't know what consumers' true expectations are about online privacy. Consumers are different. Their expectations are not static, whether they are 2 or 20 or 82, and innovation moves 500 times faster than what we see government moving. And we don't need to pretend that government has all the answers.

Our thriving tech and ad industries are infinitely more responsive and better equipped to meet consumer needs than a Federal Government program that is one size fits all.

In my opinion, our foundation for policy should be flexible, encourage beneficial use of data, protect against real harms, empower

people instead of government.

I look forward to your testimony.

And at this time, I yield to Mr. Barton of Texas.

Mr. Barton. Thank you, Ms. Blackburn.

I am going to read the Third Amendment to the Constitution of the United States. It says, no soldier shall in time of peace be quartered in any house without the consent of the owner nor in time of war but in a manner to be prescribed by law. That is the Third Amendment to the Bill of Rights of the Constitution. If the Founding Fathers had had the Internet, instead of saying without the consent of the owner to put soldiers in your home, they would have said without the consent of the Internet user, they couldn't collect data.

I want to put my support to what the ranking member, Mr. Butterfield, just said. I think it is time that the Congress of the United States pass a strong, general, explicit privacy protection law. We have approached the use of the Internet more from a marketing standpoint, that apparently each of us that uses the Internet individually exists to primarily be marketed and not as individuals that have guaranteed rights under the Constitution.

Now, the Constitution does not explicitly guarantee the right to privacy, but they wouldn't have put the Third Amendment about putting soldiers in your home without your consent if they didn't at least implicitly understand that every person in the United States at that time had the right to privacy.

Every week, Madam Chairwoman, we hear some other additional

outrage about the abuse of the Internet, whether it is a super cookie that somebody can put on your computer without your knowledge and you can't get it off. Now, my staff yesterday told me that one of our leading Internet companies, Amazon, is going to create their own server in their own system, and they are going to force everybody that uses Amazon to go through their server, and they are going to collect all this information on each person who does that without that person's knowledge.

I mean, enough is enough, Madam Chairwoman.

We have over 240 million Americans who use the Internet every day. Each of those 240 million Americans are entitled, in my opinion, to the right to privacy.

With that, I want to yield the balance of the time to Mr. Olson of Texas.

Mr. Olson. I thank my colleague, the chairman emeritus from Texas.

I thank the chairwoman.

As we continue our hearings on online privacy issues, we need to ask ourselves two fundamental questions: Number one, when it comes to privacy protections in the online space, is there an issue industry can't correct on their own through self-regulatory initiatives? And, number two, if there is a problem industry can't correct without negatively impacting jobs, our struggling economy, and the growth and innovation we are seeing in the online space, can the government correct these problems?

Today's hearing is important because we will hear directly from industry about what they are doing on their own to better provide transparency and privacy for customers online. One key advantage industry has over government is the ability to quickly adapt to changes in consumer demands and changes in technology.

So I thank the witnesses for being here and look forward to their testimony.

Yield back.

Mrs. Bono Mack. I thank the gentleman, and now we turn our attention to our panel.

STATEMENTS OF BARBARA LAWLER, CHIEF PRIVACY OFFICER, INTUIT; MICHAEL HINTZE, ASSOCIATE GENERAL COUNSEL, MICROSOFT CORPORATION; SCOTT MEYER, CEO, EVIDON; LINDA WOOLLEY, EXECUTIVE VICE PRESIDENT, WASHINGTON OPERATIONS, DIRECT MARKETING ASSOCIATION; ALESSANDRO ACQUISTI, ASSOCIATE PROFESSOR OF INFORMATION TECHNOLOGY AND PUBLIC POLICY, HEINZ COLLEGE, CARNEGIE MELLON UNIVERSITY; AND PAM DIXON, EXECUTIVE DIRECTOR, WORLD PRIVACY FORUM

Mrs. Bono Mack. We have one panel of witnesses joining us today. Each of our witnesses has prepared an opening statement that will be placed into the record. Each of you will have 5 minutes to summarize that statement in your remarks. A special welcome to the Californians on the panel, recognizing it is 6:25 for your body clocks, we have a special appreciation for your appearance here today.

But on our panel, first, we have Barbara Lawler, chief privacy officer at Intuit. Then we have Michael Hintze, associate general counsel at Microsoft. Then we have Scott Meyer, chief executive officer at Evidon. Our fourth witness is Linda Woolley, executive vice president of the Direct Marketing Association. Our fifth witness is Alessandro Acquisti, associate professor of information systems and public policy at Carnegie Mellon University. And our final witness is Pam Dixon, executive director at the World Privacy Forum.

Good morning and thank you all again for coming. You will be recognized for 5 minutes. To keep track of the time, you have the

timers in front of you, and green, yellow, red, self-explanatory, but please try to wrap it up when you get to yellow so when it hits red, your 5 minutes is up.

Ms. Lawler, if you could pull your microphone forward and turn it on, you are recognized for 5 minutes.

STATEMENT OF BARBARA LAWLER

Ms. Lawler. Good morning, Chairman Bono Mack, Ranking Member Butterfield, and members of the committee, thank you for this opportunity to comment on consumer expectations around privacy. I am Barb Lawler, the chief privacy officer at Intuit. I ask that my full statement be put into the record due to the time constraints.

Intuit is well positioned to comment on consumer expectations about privacy. Over 50 million customers entrust us with their most personal financial information. We have been committed to innovating and implementing the safest and most responsible ways to work with consumers' financial information for nearly 30 years. Understanding our customers' expectations about online privacy and earning their trust is a major priority at Intuit.

Intuit recently undertook a comprehensive research program that examined our customers' expectations about privacy. Our customers told us they expect Intuit to be an ethical steward of their information, applying it reasonably and with integrity for their benefit, while keeping it safe and secure. Our research strongly informed the development of our data stewardship principles. The unifying concept is that it is the customer's data, not ours.

Our principles provide our customers with tools to understand how their data is being used and empower them with choices to control the use of their data. These fundamentals were based on a number of key

insights we learned from our customer research project.

First, we learned that data privacy matters to consumers. While many people do not pore over privacy policy statements, they do care deeply about privacy and how their data is used. Customers told us the fine print is often confusing and they prefer simple, easy-to-read explanations of how their data will be applied and used and serviced to their needs.

Second, we found that customers want clear, relevant, and context-based choices that educate and empower them to control the use of their data. When a choice is presented in relevant context and coupled with a simple explanation, most customers felt empowered to make choices and then welcomed the use of their data.

Finally, confidence increases when consumers clearly understand how their data can be applied to benefit them.

In the absence of clear statement and principles, customers can worry that their data will be sold to third parties to benefit someone else or possibly harm them. When data-driven benefits are clearly outlined to consumers in responsible ways, their attitudes toward the use of their data significantly changed.

Data-driven innovations can equip individuals and small business owners with new tools and insights that once were only available to much larger and more powerful companies. Our research showed a tremendous appetite for such products and services amongst both consumers and small business owners. For example, Intuit developed capabilities for small business owners to compare themselves along key

metrics for similarly situated businesses in the same geography. Imagine if your local florist could compare his regular spending trends, soil, marketing or delivery trucks, anonymously with those of other florists in his region of the country. This kind of service involves the use of the customer's own data in a way that brings meaningful value to their lives and financial well-being.

As we move toward a connected services cloud-based economy, it is vital that we develop clear and practical privacy frameworks that answer the concerns and expectations of consumers, regardless of the technology or the device they choose to use. Data stewardship represents our ongoing commitment to act as an accountable organization to our customers and to the public. We see data stewardship as a clear and practical privacy policy framework for the 21st century. We all must work toward the shared goal of protecting consumers while maintaining data-driven innovation that improves consumers' lives in trusted, real, and fundamental ways.

Thank you again for this opportunity. We look forward to working together with you and the committee toward this important goal.

[The prepared statement of Ms. Lawler follows:]

******** INSERT 1-1 ********

Mrs. Bono Mack. Thank you, Ms. Lawler.

Mr. Hintze, you are recognized for 5 minutes.

STATEMENT OF MICHAEL HINTZE

Mr. Hintze. Chairman Bono Mack, Ranking Member Butterfield, and honorable members of the committee, my name is Mike Hintze, and I am an associate general counsel at Microsoft. Thank you for the opportunity to share Microsoft's perspective on the important issue of consumer attitudes about privacy.

We appreciate the leadership the subcommittee has shown on this topic, and we are committed to working with you and others to protect consumer privacy while promoting innovation.

The diverse products and services through which Microsoft engages with consumers gives us a unique perspective on the privacy discussion. We have a strong commitment to privacy because we recognize that consumer trust is critical to the adoption of online services.

Our goal at Microsoft is to build trust with consumers by providing them with information about what data is being collected and how it is being used, offering choices about the collection and use of that data and ensuring that their data is kept secure.

In our experience, there is no silver bullet solution to privacy. This is because privacy means different things to different consumers, and there is a wide range of privacy sensitivities among individuals. Consumers also have different privacy expectations depending on the

context in which their data is collected and used.

Finally, as technology evolves, customer expectations about privacy often evolve with it. These challenges require a multifaceted approach to addressing consumer privacy. In our view, this approach should focus on four key elements.

The first element is company best practices. At Microsoft, we have a deep and longstanding commitment to privacy in how we design our products and services and how we operate our business. We believe in adopting practices that provide consumers with information and choices to enable them to exercise more control over their privacy.

Let me provide some examples of how consumers have responded to that approach. Over the past 5 months, key privacy Web sites offered by just one division of our company averaged over 2 million sessions per month. In an average month, more than 435,000 consumers access our advertisement choice Web site. This site provides information about personalized online advertisements and how consumers can opt out or use other controls. Approximately 20 percent of those consumers perform some action while visiting that site, in most cases opting out of personalized ads. As these numbers make clear, when we provide consumers with information and meaningful controls, many will use them.

The second element is technology tools that empower users to protect themselves as they interact with other sites across the Internet. For example, we were the first major browser manufacturer to respond to the FTC's recent call for a persistent browser-based "do not track" mechanism. In Internet Explorer 9, we offer this feature

which we call tracking protection. It allows consumers to decide which third-party sites can receive their data and filters contents from sites identified as potential privacy threats.

But no company can meet consumer privacy expectations on its own. So the third element that can contribute to the protection of consumer privacy involves baseline rules of the road established by both industry self-regulation and legislation. Industry self-regulation in particular plays an important role in fostering privacy solutions and can offer flexible approaches for protecting privacy in many different contexts. We also have long-supported Federal baseline privacy legislation as a means of setting rules that can protect consumers without hampering innovation.

Nevertheless, self-regulatory efforts are generally better than prescriptive legislation to keep pace with evolving technologies. One recent example of this is the self-regulatory program for online behavioral advertising, which has advanced both transparency and consumer choice. Among other things, this program includes a standard icon that is prominently displayed in or next to online ads. By clicking on the icon, consumers can access information about the delivery of the ad and choose to opt out from receiving behavioral advertising.

Finally, the fourth element is consumer education. In order for all of these elements to work, consumers need to understand the protections and tools available and the practices of companies with which they are interacting. That is why, in addition to providing

information ourselves, we have also partnered with consumer advocates and government agencies to develop educational materials on consumer privacy and data security.

In conclusion, addressing consumer privacy expectations requires the collaborative effort of individual companies, industry groups, consumer and privacy advocates, government, and consumers themselves. We must work together to meet these challenges without hindering innovation.

Thank you, and I look forward to answering your questions.

[The prepared statement of Mr. Hintze follows:]

******** INSERT 1-2 ********

Mrs. Bono Mack. Thank you very much.

Mr. Meyer, you are recognized for 5 minutes.

STATEMENT OF SCOTT MEYER

Mr. Meyer. Thank you, Chairman Bono Mack, and Ranking Member Butterfield, and distinguished members of the subcommittee.

My name is Scott Meyer. I am the CEO and founder of Evidon. I appreciate the opportunity to appear before you today to talk about consumer expectations regarding online interest-based advertising and the important role that my company, Evidon, plays in meeting those expectations.

We founded Evidon specifically to promote transparency, consumer control, and accountability across the online advertising ecosystem. Our technology is at the heart of the industry's self-regulatory program, which is designed to give consumers greater control, transparency, and understanding of interest-based or behavioral ads.

The core component of the program is the display of a distinct advertising option icon on interest-based ads and on Web sites where data is collected and used. Our platform, which is called Evidon InForm, is a leading example of privacy by design in the actual real world. It displays the advertising option icon in ads and on Web pages. When consumers click on the icon, they can easily find out more information about the ad. This includes information about the companies who are involved in delivering the ad to them as well as the

all-important ability to opt out.

I brought some slides with me today which are on the screens and are also in my written testimony, so if I could have the first slide, please, so you can see the platform in action. Here you can see an ad with the advertising option icon along with the text ad choices in the upper left-hand corner. You might also see the same icon in the bottom of a Web page.

When consumers click on the icon, an overlay window appears with more information and the links you see displayed here on the next slide. In the 12 months since the launch of the advertising option icon program, Evidon has delivered over 85 billion of these in-ad notices through our platform. We currently provide notice in nearly 20 billion online ads each month, and on an average day, ads with Evidon-powered notice reach more than 80 million U.S. Internet users.

One click on the more information and opt-out options on the slide takes you to the next page, which is the Evidon Web page shown here. And on this page, consumers can see which companies have been able, which companies have been involved in the data collection and use, and they have the ability to find out more as well as, importantly, to opt out.

Evidon InForm also provides reporting to the companies to show them how consumers have interacted with this platform, and those reports are endorsed as a standard method for providing evidence of compliance with the industry's self-regulatory program.

Though Evidon itself does not collect any consumer information,

our anonymous logs show that the advertising option icon has been clicked 4.5 million times since the launch of the program. That has resulted in 730,000 opt-out requests being sent through the Evidon platform alone.

In 2010, we commissioned a study by Millward Brown to better understand what consumers want and what they expect when they click on the icon. We found that 76 percent of consumers who clicked on the icon and interacted with the Evidon notice experience that you see here wanted to see all of the companies involved in targeting ads to them and find out more information. We also found that this was good for business, that 67 percent of consumers when they went through the Evidon notice experience felt more positive and in greater control of their advertising and felt more positive toward the brands that were involved in these ads.

Together these metrics support the proposition that consumers want more than a simple on or off switch, and they want substantive notice and control regarding the companies responsible for targeting the ads to them.

Finally, if I could go to the next slide, in addition to implementing the advertising option icon, we have led the way with the creation of the Open Data Partnership. Open Data, a key feature is the preference manager you see here and in my written testimony which enables consumers to see and edit the information that companies have collected about them as well as the all-important ability to opt out.

The metrics I have laid out today and more fully developed in my

testimony reflect an order of magnitude shift in the availability of how information is used and collected and the choices that consumers are able to make. This is important because the information is no longer buried in privacy policies. Now it is presented to the consumer in clear, specific, and easily understood ways directly at the point of engagement. And ultimately, the success of this program should be judged by the degree to which these access tools are produced in a credible fashion and the extent to which these tools are offered to the consumer and not simply the rate at which consumers opt out.

One last point I will make is that this hearing is all about consumer expectations. The one thing I think everyone here can agree on is that consumers have come to expect free online content. The targeted advertising that we are talking about today plays an essential role in supporting the vibrant, free, and open Internet that consumers have come to expect and to enjoy.

Thank you again for inviting me to testify, and I look forward to answering your questions.

[The prepared statement of Mr. Mr. Meyer follows:]

******** INSERT 1-3 ********

Mrs. Bono Mack. Thank you, Mr. Meyer.

Ms. Woolley, you are recognized for 5 minutes, and please make sure your microphone is on and close to you.

STATEMENT OF LINDA WOOLLEY

Ms. Woolley. Thank you, Madam Chairman.

Ranking Member Butterfield and members of the committee, thank you for the opportunity to speak.

My name is Linda Woolley, and I am executive vice president of Washington operations for the Direct Marketing Association, a global trade association of thousands of businesses and nonprofit organizations that use and support multi-channel direct marketing tools and techniques.

Today, however, I am pleased to testify on behalf of the Digital Advertising Alliance, known as DAA, and to report to the subcommittee on the substantial progress of our self-regulatory program for online behavioral advertising. The program which you heard about from previous witnesses builds on a long tradition of successful self-regulation in marketing and advertising and provides transparency and controls so that consumers can exercise their individual choices regarding online behavioral advertising.

It is appropriate that the subcommittee is devoting a series of hearings to online issues because it is impossible to overstate the economic importance of the Internet today. I think one of your

members, I think Mr. Butterfield actually, mentioned earlier that the online behavioral advertising industry in this year alone represents a $30 billion economy, and that is growing.

Advertising helps to fuel the Internet economic engine. According to a new report from the Direct Marketing Association, based on the results of the first half of this year, expenditures in 2011 on online marketing in the United States are expected to total over $30 billion. These revenues support e-commerce and subsidize a rich variety of content and services that consumers and businesses rely upon and value.

Behavioral or interest-based advertising is an essential form of online advertising. It delivers content to consumers based on interests that are inferred from data about online activities. Consumers are likely to find interest-based advertisements much more relevant than the random messages that they would otherwise receive, and advertisers and publishers also derive great value from relevant advertising.

In general, the data used for interest-based advertising is not personally identifiable, except when consumers choose to share personally identifiable information. Nevertheless, the advertising industry recognizes and respects that some consumers prefer not to receive such advertising.

In 2009, as was already mentioned, the Federal Trade Commission endorsed industry self-regulation for online interest-based advertising. Following the road map that was set out by the

commission, the online advertising industry, on its own initiative, developed a self-regulatory principles for online behavioral advertising that cover consumer education, enhanced notice of data practices, innovative mechanisms, choice mechanisms, data security, sensitive data protection, consent for retroactive material changes, and enforcement.

Our self-regulatory principles are comprehensive, but yet they are flexible enough to respond to the complex and ever-evolving online advertising ecosystem. More importantly, they represent consensus in the online advertising community and are supported by all of the major industry stakeholders in the Internet ecosystem, as my colleague from Microsoft previously mentioned.

Since publishing the principles, the advertising industry has put its money where its mouth is and developed a program that is second to none. Hundreds of companies have invested now millions of dollars to give consumers transparency about online data collection practices and meaningful choices about how data is collected and used.

I want to mention that the DAA program includes all 15 largest online advertising networks and that the brands that participate in this program are household names. To mention a few: Google, Microsoft, Yahoo!, GM, American Express, Bank of America, Disney, Procter & Gamble, Target, Wal-Mart, AT&T, Verizon, Comcast, Time Warner Cable, Honda, Hyundai, Toyota, Dell, HP, the list goes on, but I think you get the sense of how all of these companies understand that this is a critical program, a critical and credible program that they, too,

want to be part of.

My written testimony describes our achievements in greater detail, but I would like to highlight a few key elements for the subcommittee. First, the advertising option icon shown in this program is a key feature of the program, and as mentioned earlier, this is what consumers see if they click on it, they get in one or two clicks are able to opt out.

The self-regulatory program: Second, the DAA program is effective and easy to use for consumers. When the ad is delivered is at the exact moment that consumers are likely to want to take action and make a choice about their preferences, and finally, the program is backed up by strong enforcement, managed through both DMA and the Council of Better Business Bureau. Thank you very much for the opportunity to testify.

[The prepared statement of Ms. Woolley follows:]

******** INSERT 1-4 ********

Mrs. Bono Mack. Thank you, Ms. Woolley.

Dr. Acquisti, you are recognized for 5 minutes.

STATEMENT OF ALESSANDRO ACQUISTI

Mr. Acquisti. Thank you, Chairman Bono Mack, Ranking Member Butterfield, and members of the subcommittee, it is my honor to be here today.

My name is Alessandro Acquisti. I am an associate professor at the Heinz College, Carnegie Mellon University. I have been studying the economics of privacy for about 10 years.

Surveys have found repeatedly evidence of widespread privacy concerns among U.S. consumers. Most Americans believe that privacy is a right, and this right is under threat. They express concerns over the way businesses collect personal information and favor government intervention over self-regulation as a means to protect privacy.

Consumers are especially troubled by tracking technologies. A vast majority of individuals express elevated concerns about the usage of their location data and significant distrust towards targeted advertising.

However, other studies have found discrepancies between privacy attitudes, what people say in surveys, and actual behavior. Individuals like sharing information online with friends and seem willing to trade privacy for convenience and personalized services.

Now, consumers' willingness to share personal information is not

in contradiction with their desire for privacy. However, behavioral research has shown that consumers face significant challenges in navigating complex privacy trade-offs in the marketplace in ways which reflect their self-interests.

One problem highlighted by research is that consumers often do not know what happens to their data or are provided confusing, sometimes even misleading information about their data. Choice and notification regimes are unlikely to solve the problem. By the time the consumer learns how to deal with a privacy sensitive technology, often a new and more intrusive technology has already appeared, catching the consumer unprepared.

Furthermore, if we assume that consumers will actually read the privacy policies, studies have shown that the opportunity costs for the U.S. economy or the time spent actually reading those policies will be about two-thirds of a trillion dollars a year.

These problems are magnified by the proliferation of consumer tracking across multiple sites and progresses in data mining, which make it possible to re-identify individuals and make sensitive inferences from data which seemed anonymous. In a recent experiment at Carnegie Mellon, we predicted individuals' Social Security numbers simply starting from their faces. Individuals and consumers are at a loss here because they cannot predict how the innocuous information they reveal today will be combined to produce more sensitive inferences tomorrow.

A second problem relates to systematic biases, mistakes people

make when trading off privacy and disclosure. Consider instant gratification bias. Human beings tend to value the present more than the future and therefore underappreciate the negative consequences of current actions. While the benefits of information disclosure are often immediate, the costs of disclosures happen in the future. Therefore consumers may disclose data today that puts them at great risk tomorrow.

Consider also the paradox of control. At CMU, we did experiments and found that increasing control of a person's information can decrease concern about privacy but paradoxically increases individuals' propensity to disclose sensitive information to strangers, even when the objective risks are actually increasing. So, in a way, more control, less privacy.

In other experiments, we found that individuals can be manipulated to disclose more or less information with subtle changes to the interfaces of Internet services. There is evidence that online companies have used similar strategies to nudge users toward more disclosure. So self-regulatory solutions are unlikely to solve this kind of a problem.

In a way, this research indicates that there is no complete free choice on the Internet. What I mean is that even before the first visitor has arrived to a Web site, the engineers of the Web site have made design decisions that will impact the future behavior of the visitor and in fact also how much the person will reveal.

So privacy is becoming less about control over your information

and more about the control that others can have over you if they have your information. In economic terms, the notion that as consumers, we receive free online services is only partially accurate. The other side is that in reality information doesn't pay the bills at the end of the month. The free services consumers get are paid by consumers by purchasing goods at prices which they are nudged to accept based on information firms have about them.

Now for the good news. Industry and academic laboratories across the United States have also developed other technologies which can protect privacy without sacrificing firms' ability to innovate. I am referring to privacy enhancing technologies, in particular through the type of technologies which work by anonymizing individual data in ways which are both effective, in the sense that reidentification becomes very hard, and efficient, in the sense that transactions can still be completed.

This means that we can still tap economics as a natural resource without sacrificing consumer privacy. Therefore, a critical question for Congress is how to create incentives so that we can foster the progress and the deployment of those technologies.

Thank you, and I look forward to answering any questions.

[The prepared statement of Mr. Acquisti follows:]

******** INSERT 1-5 ********

Mrs. Bono Mack. Thank you very much.

And Ms. Dixon, you are now recognized for 5 minutes.

STATEMENT OF PAM DIXON

Ms. Dixon. Thank you.

Thank you for the invitation to come here today. I appreciate it very much. Just three quick things. First, I think we have heard today that from industry and academics, that consumers just don't know what the risks are out there, and we all drive cars, but we are not all mechanics. Likewise, consumers are on the Internet, but they are not all technical experts. This is not a surprise to any of us.

It is so frustrating when we get consumer phone calls, and there is a solution for them, but they don't know about it. And we talk to them about it, but that is just one consumer that we have helped. There are millions and millions of consumers in this particular boat.

How do we help all these consumers who are unaware of these technical risks that we face online? It is a very difficult challenge, but the one thing that surveys are very clear on is that consumers are completely almost unaware of the risks they face. It would be very challenging for a consumer to simply keep up with everything that is going on between a tracking cookie and a this and a that.

But secondly, as Alessandro has talked about, consumers do not understand the privacy trade-offs that they are looking at, when they are looking at privacy policies and icons. This is a deep problem that

is not going to be solved by pretty much anything. This is a human nature problem.

So a consumer goes to a Web site, they see a privacy policy or they see a seal or an icon. What do they think? They think that their information is not collected, that their information is not sold, bartered, et cetera. This is simply not usually the case, but this is what consumers believe. This is a fundamental perception issue that is going to need to shift for consumers to be able to take adequate protective actions for themselves.

So, as a result of these structural imbalances on the Web, we support legislation that will protect consumers. However, the reality check is that we don't see any likelihood of that happening in the near future.

So what is a consumer to do? What is to happen now? What are we faced with here? I think that what we need to do is look at self-regulation. If self-regulation is going to be the way forward, we need to reform it. There are a lot of structural issues with self-regulation today. Self-regulation today bears many of the hallmarks that self-regulatory efforts for privacy in the past have also shared.

I have included a checklist of 15 items that a credible self-regulatory regime should have. Among these include greater transparency; a defined and permanent role for consumers; composition of a board, a governing board that includes a majority of consumer involvement. All of these things would go far to improve the current

self-regulatory schemes in play today. So we advocate for greatly improved and reformed self-regulation. I think it is an important thing to look at.

The second thing is that we think that there needs to be a broader scope of discussion. It is very frustrating for me when I hear discussions about online advertising because when we get calls from consumers, they are not talking about what ads they have been shown, not usually; it is pretty rare. They are talking about their health data that has been used against them, that an employer has found. They are talking about when they have gone to a Web site, they have signed up for a survey, and then they found out later that that information was sold because they just didn't read the privacy policy.

We have got to look at the broader array of privacy issues. Some of these issues do include advertising because advertisings are part of the collection mechanism online. That is the role we need to look at. So when we are talking about opt-outs, it is great that there is so much more activity with opt-out and that the opt-out is better. We support that, and I think it is terrific. It is. It really is. It is much, much better than it was even 2 years ago.

But what are consumers getting the right to opt out of? Are they getting the right to opt out of tracking or being shown an ad? We need to deliver opt-outs that confer fundamental choices to consumers, like opting out of tracking. So this is what we think is really important to focus on.

And then just a quick word. Many of the self-regulatory regimes

today focus on very narrow aspects of online privacy. So, for example, if a consumer with a health condition was to go to a Web site to research AIDS or cancer or Alzheimer's for an aging parent, that consumer's information can be tracked and then used in ways that may be counter to their expectations. This is exactly the kind of thing that we need to work with. Does it harm a person to be shown an ad about Alzheimer's? That is debatable. In some cases, I think young teen girls being shown weight loss ads; that can be harmful. But other, you know, a red car or a blue car; I am not so worried about that. I am worried about the collection of the data, the tracking, and the reuse. So that is my statement, and thank you for your time and attention.

[The prepared statement of Ms. Dixon follows:]

******** INSERT 1-6 ********

Mrs. Bono Mack. Thank you, Ms. Dixon.

And now I will recognize myself for 5 minutes for questioning. I would like to start with Mr. Meyer.

In your testimony, you state that since October 2010, your icon has been featured in over 85 billion ads, that consumers have clicked the icon 4.5 million times, and that consumers have submitted 730,000 opt-out requests. That is not a real high success rate I would think.

On your slide, I noticed the icon, and I toured Intuit a little while ago, and they had some pretty fantastic technology that tracked the eyeballs as they followed around the screen. What kind of testing did you do of your icon and clicking on that icon, is that evident enough for the consumers, or is this not quite there yet as being as obvious to consumers as it could be?

Mr. Meyer. Sure. So I think that we do a lot of testing, and the challenge with the size of the icon in the ad is that we are working with a small amount of real estate, and we have to balance the notification about online tracking with the ability for the ad to actually perform, and we have to enable marketers to continue to meet their needs. The icon was created through a cross-industry and cross-functional group that included academics and industry, and it was tested reasonably well.

And very importantly, I would end with the icon is not an opt-out mechanism. The icon is an education mechanism. One of the important features is the ability to opt out, and in terms of the performance rates in terms of the clicks relative to the performance of overall

on an advertising, it is very consistent; general online advertising ads click rates generally are under 1 percent anyhow.

Mrs. Bono Mack. Can you -- and let me clarify a little bit about what I am saying about the success rate of that, whether that is driven by your design or whether it is driven by consumer expectations is, I think, the point of the whole hearing, but on all of these different cookies, can you briefly explain the difference between tracking, session, persistent, flash cookie, super cookie, and if there is absolutely no technological answer on the horizon that could wipe all of those things out?

Mr. Meyer. So the technological answers exist today for almost all the different types of cookies.

Mrs. Bono Mack. Even a super cookie?

Mr. Meyer. Super cookies are the one piece that we at Evidon think should not be used for any form of online advertising. That is not what they are designed for. We don't think there is any legitimate purpose in online advertising for super cookies.

All the other forms of cookies that you allude to, that you mention, are easily accessible. The most basic are HTML cookies that are used for what are called session and permanent cookies, and those can be erased through the opt-out mechanism that we provide. We also own and operate a service called Ghostery, which is one of the most popular privacy protection tools for consumers. More than 4 million people have downloaded it. That completely blocks advertising. It essentially creates the on-off switch that is envisioned by "do not

track."

Mrs. Bono Mack. So Ghostery is a lot stronger than if I just go into my own browser and I hit delete cookies?

Mr. Meyer. That is true.

Mrs. Bono Mack. If I can go to Ms. Lawler, thank you for your testimony, and for me, something that has struck me over all of these years is the migration of what the content industry has been faced with, that it is impossible to compete against free. And I know that Intuit has tried, they have now Mint.com, so you have both the Quicken and the Mint. Can you explain, are consumers understanding the difference? Are they enjoying the free program better? Are they migrating to free because they are getting some trade-offs? Can you explain briefly your experiences with the two?

Ms. Lawler. Yes. So let me start and say there is -- Quicken is actually our flagship product. That is where Intuit started nearly 30 years ago, and so that is downloadable software or CD-based software that you run on your desktop, so you pay for that.

I think what you are asking is where the business model goes and where consumers are going is to an online-based service. In the case of Mint.com, Mint is free, and so you are not paying for that. You can actually use some of the tools on Mint without even signing up for it. When you go to the Mint page, it is very simple, easy, clear to understand what the value is, what you can do in terms of managing your budget, tracking expenses.

How that gets paid for is through the option for you to get offers.

Mrs. Bono Mack. But my question specifically is, are you finding that consumers are going toward the free site rather than the -- either the downloading, you buy the CD-ROM at --

Ms. Lawler. They are moving over time. I don't have the specific numbers with me. I would be happy to go find that information for you and bring it back to the committee at a later date. What we are finding is that there is a gradual move to online. Some of that is technology based, so those who are more comfortable with mobile technologies. It is also somewhat generational, so as we see young people more comfortable with using free online services or any online service, there is definitely a trend toward online, but it is very slow and gradual, so small percentages over the years.

Mrs. Bono Mack. All right, thank you.

My time has expired.

Mr. Towns, you are recognized for 5 minutes.

Mr. Towns. Thank you very much, Madam Chair.

Let me begin with you, Ms. Dixon. I understand that there was a study in California of Internet users, and of course, could you please talk about that just for a moment in terms of what happened?

Ms. Dixon. Yes, I believe you are referring to the Chris Hoofnagle and Jennifer King study that --

Mr. Towns. In 2008?

Ms. Dixon. Yes.

Mr. Towns. Yeah, right.

Ms. Dixon. It was a groundbreaking study. What they did was

they went and surveyed online users and asked them what they perceived when they saw privacy policies online. And their findings were remarkable because the misperceptions were just profound. So, for example, a majority of consumers, when they saw a privacy policy, believed that that meant that the site would not collect information about them, even collect. Users also believed that they would have the right to sue if the site did things with their data that they did not want, and these were just among a few of the many misperceptions that consumers had about privacy policies when they saw them, and consumers, very few consumers understood that when, for example, they opted out -- there were questions about, you know, various cookies and what not. Consumers just did not understand that when they opted out with an opt-out cookie, that it didn't mean that they were not going to be tracked; it just meant that they were not going to be given display ads based on tracking. So there was a profound, deep, serious misunderstanding and misperception of what privacy policies actually mean when they are on a site.

Mr. Towns. Thank you very much.

Dr. Acquisti, do you think privacy policies serve any useful purpose for the consumers?

Mr. Acquisti. They do. I see them as necessary, not sufficient, conditions, in the sense that we do need privacy policies because we need to inform and educate the consumers. They are not sufficient, however, because of the type of challenges I was describing in my testimony.

Mrs. Bono Mack. Excuse me one second, if the gentleman will suspend. I am asked to notify you, while there are protestors in the hallway, we don't expect it to get out of hand, but if it does, please exit that door.

Mr. Towns. You don't have to worry about it, I am here. I am here, don't worry about it.

Mrs. Bono Mack. There you go. I feel so comfortable now. Thank you, please continue.

Mr. Towns. Yes, you may continue.

Mr. Acquisti. So the challenges I was mentioning, just to summarize, are, one, the problem of -- economists call it bounded rationality. We don't have unlimited time to think about all the possible consequences. Even if we read a policy, we may not think through what it really implies. Some policies are written in ways which are not easily understood. One study a few years ago reported that half of privacy policies on the Internet are not understood by about 60 percent of Internet users. Plus there is also this additional challenge that if we take these policies seriously, and we really believe that users, after reading privacy policies, do not know what happens to their data, the opportunity cost is enormous.

Mr. Towns. Thank you very much.

Mr. Hintze, I followed your company in terms of I know you have a privacy officer. Basically what is the role of that privacy officer?

Mr. Hintze. Well, we have a number of people at Microsoft focused on privacy. We have got our chief privacy officer, who is responsible

for the overall governance of privacy programs within Microsoft, and that includes training for our employees, whether they are developers or marketers or human resources folks. It includes the development of our standards and guidelines that we provide around marketing, around product development, et cetera. It includes building in privacy checkpoints and privacy training and privacy standards into our business processes. So our chief privacy officer oversees all of that.

He also oversees, not necessarily direct reporting relationships, but kind of a dotted-line relationship to all the people in Microsoft who are focused on privacy, and we have over 40 full-time people focused on privacy and another 400 who have it as a defined part of their job, and those people are embedded in every business and operations unit of the company.

RPTS THOMAS

DCMN SECKMAN

[10:05 a.m.]

Mr. Towns. Short of strongly regulating business, which would probably do more harm than good, what can we do to encourage other companies to consider privacy issues very carefully.

Mr. Hintze. As I mentioned in my testimony, I think that there are roles for multiple entities in protecting privacy from government, individual companies, to academics and privacy advocates as we have represented on the panel here today. I think individual companies like ourselves can lead by example by adopting strong privacy practices. We have made those internal standards that I talked about for developing products and services and building privacy protections into those; we have made those publicly available so that others can see them and take advantage of the work that we have done over the years in developing those.

Privacy advocates clearly have a role in helping to educate consumers and bring to the attention issues that come up and nudging industry in appropriate ways to do the right thing. And government has a role through enforcement when people are breaking existing laws through using your own bully pulpit to educate your constituents and playing the oversight role that this committee has done so well for so many years.

Mr. Towns. Thank you so much. We salute you and your company.

Mrs. Bono Mack. The Chair now recognizes Mr. Blackburn for 5 minutes.

Mrs. Blackburn. Mr. Meyer, I want to come to you.

I know that Evidon is partnering with Akamai? Am I saying that correctly?

There was a Wall Street Journal article on it saying that you would handle, what is it, trillions of interactions, a trillion interactions a day. So let's talk about the consumer.

Now, with your platform, tell me what this means for the consumer. How does it empower them? How does it allow them to continue to protect or have the ability to protect what I term the virtual you, their presence online?

So just in about 15, 20 seconds, can you give me that synopsis?

Mr. Meyer. I will do my best.

So Akamai powers more than a trillion Internet transactions every day. The Evidon technology, which you saw in my slides and in my testimony, will now be built directly into that platform, which will take the process of Web site operators of all forms, and it will take the process of complying with the program and giving consumers that view into their virtual you. It will take what is now a reasonably complex legal and technical process, and it will simplify to literally a few clicks and a short one.

Mrs. Blackburn. So you are saying your ability is simplicity and transparency and access. Is that what I am hearing you say?

Mr. Meyer. That is the goal of us and Akamai getting together

for this.

Mrs. Blackburn. That is what I wanted to know. I was unclear. The B2B is fine, but I want to know what you are going to do for the consumer. How are you going be able to protect their privacy?

Ms. Woolley, I want to ask you pretty much the same thing. Do you think that industry can do a better job than government in addressing these privacy concerns that you all have rolled out with the Ad Choice campaign?

Ms. Woolley. Yes, I absolutely think that industry can do a better job than government. The main reason is that we are nimble, and we can move quickly. We have rolled out this program in a year. And we are now rolling out further iterations of the program, which include migration of that icon overseas and migration of that icon to mobile devices. To do that in less than a year is something that government could not go.

Mrs. Blackburn. In your testimony, you mentioned protecting data in terms of the cost to jobs, cost to the economy. And would you just elaborate on that just a tiny bit?

Ms. Woolley. Sure. There have been several studies that show that if the United States were to adopt a privacy regime along the lines of what Europe has adopted that the cost --

Mrs. Blackburn. "Do not track."

Ms. Woolley. "Do not track." And do not use cookies. The cost to our economy would be about $33 billion a year.

Mrs. Blackburn. Okay. Thank you.

I have a series of yes-and-no questions that I wanted to go through. So if you all will listen, and I will have you raise your hand for yes and your hand for no.

Okay. Do you believe that a government mandated "do not track" as the FTC has endorsed has gone too far and would be too much to address the privacy problem? Yes, if you believe "do not track" goes too far, raise your hands. Okay. So I have got four on that.

And no. One no. And the rest abstain. So you are going to be a no, too.

Do you believe that government regulations on commercial use of de-identified metadata or anonymous data sets pose significant challenges to the First Amendment? So do you believe that government regulations on commercial uses of de-identified metadata or anonymous data sets pose significant challenges to the first amendment. Yes? Okay. We have got two yeses.

No? We have got two noes. And the rest are thinking.

Congress and the Federal Government in general have a low approval rating. We admit that. Yes or no, do you think consumers -- here is the question, yes or no, this is what I want to hear from you all: Do you think consumers trust government to know best how to protect their privacy through rules, mandates, legislation, or no? Do they trust the government to do it, or do they trust you?

Yes, if they trust government. Just two of you would trust the government.

No, they don't trust the government. They would trust industry,

one. Like these hands kind of waving out there.

Do you believe that new privacy regulations could have an adverse impact on industry competition that would hinder smaller firms, some of the innovative firms?

Yes.

Do you believe new privacy regulations could have an adverse impact on industry competition that would hinder smaller firms or no?

Yes if you believe?

We have got two on the yes side.

No, not going to impact.

One no.

I am going to let you off the hook because my time has expired.

Mrs. Bono Mack. Mr. Lance for 5 minutes.

Mr. Lance. Good morning to all. This is very interesting, and I have learned a great deal.

To Ms. Lawler, do you know what percentage of your customers view and manipulate the privacy options that you offer them?

Ms. Lawler. We have a couple of different ways that we approach privacy choices. If you think about the traditional choices that most companies have offered for the last several years, which would be in the marketing space -- so around phone calls, e-mails, snail mail and so on -- it is a fairly small percentage. I don't have all of the numbers with me. I can tell you that in our email marketing, specifically that our opt-out rates are at about the industry average, but I would be happy to research that more with our technicians.

Mr. Lance. What is the industry average?

Ms. Lawler. It is about 0.05 to 0.1. It depends upon the type of ad and the context.

Mr. Lance. Thank you. Thank you very much.

To Professor Acquisti, your testimony includes an interesting point that I am not sure has been raised before. You call it the paradox of control. In other words, the more privacy choices a consumer has, the more likely that consumer is to have a false sense of security. Does this argue against more granular controls, or if you would elaborate on your views on that?

Mr. Acquisti. It was a paradoxical result. To explain it with an analogy, other studies have shown that when you ask people to wear seatbelts, they -- some of them may start driving faster. It is probably overconfidence. You feel more protected, you end up taking more risks.

So we believe that this is what is happening in the results we found is you make consumers feel more in control, the ones deciding with the agency of deciding whether or not to disburse information, which in a normative sense is a good thing, the unexpected consequence can be that this overconfidence can lead to the consumer taking more risk.

What I mean by more risk, and I have to be very careful, is compared to a condition where there was no such feeling of control, the subjects in the control ended up revealing more sensitive information to more strangers.

Mr. Lance. So how would you overcome that challenge?

Mr. Acquisti. Well, it is central what kind of control do we give, and whether control solves all of the problems. So the results of the study suggest that merely giving granular control may not solve consumer decision-making problems if the control leads to bad decisions later on.

It is not a statement about we should never give control, of course. It is about what matter, what type of control we give and whether by giving control, do we feel that we have solved privacy problems.

The results of the experiment, such as the answer to the last question, is no

Mr. Lance. Thank you very much.

To Mr. Hintze from Microsoft, you state that consumer attitudes to privacy can evolve over time -- I am sure that is true -- noting how consumers were originally hesitant to share photos and videos online, but now regularly do so. Have you seen any evidence where consumers are evolving in the opposite direction to restrict the collection and sharing of their information online with commercial operators.

Mr. Hintze. I am not sure I can point to any particular statistics that would show that, but I certainly think that we see more of an awareness of privacy than we did a few years ago.

I agree with the comments that Ms. Dixon made that people don't always fully understand all of what is going on, and it is always a

challenge to get the right information in front of consumers, but you do see a heightened awareness, and that is in large part due to the work of privacy advocates and many of the journalists. And we have all seen the Wall Street Journal series of articles and other publications that have been focused on privacy.

Whether that translates into people making different choices, that is hard to quantify, and I am not quite sure how we would do that. But we certainly see more people looking at our privacy Web pages now than we have in the past, and it is certainly something that we are cognizant of and want to make sure we are responsive to those concerns.

Mr. Lance. Thank you very much. My thanks to the panel.

I yield back the remainder of my time.

Mrs. Bono Mack. The chair now recognizes Mr. Gonzalez for 5 minutes.

Mr. Gonzalez. Thank you very much. I appreciate it.

I apologize for not being here for the testimony. I had the opportunity to review written statements that were submitted. Again, I wish I could have been here for the testimony because it is incredibly important to have you here today and to share your viewpoints and your own experiences.

My first observation, of course, is information gathering, dissemination, protection of same and so on, and how important that is to different industries.

So I guess I want to acknowledge that in this informational age and how we market, how we promote products and services in our system

is incredibly important, and things have been revolutionized. And the fact that you can now target audiences, which I think is a tremendous advantage -- it makes a more effective way for those individuals in this country that have different business enterprises to reach their customers. And you know what happens when we reach customers? And that means we in fact do create wealth for many, and we create jobs in this country.

So I want to acknowledge the importance of information gathering, what it means, and that many of the services that are provided today, as we say free, really constitute a trade. You will receive some sort of service through the Internet one way or another in return for allowing the person that is providing you this service or benefit the opportunity to basically establish some sort of consumer DNA. And that is the world that we live in.

And I think, as I came in, one of the things that Mr. Hintze was pointing out is really whether the consumer is aware of the information that they are providing and its use.

And we have struggled with this in the past, even years ago when I was on financial services, as to what an affiliate would share.

But what it comes down to -- Mr. Hintze, I was reading your testimony, and it is very interesting because you have different points. But one of them of course is technological tools. And that is that you, with Microsoft, could provide the consumer and the user of the Internet with the ability to basically not allow any kind of tracking to establish this consumer identity or DNA. Is that correct?

Mr. Hintze. That is right. In the testimony, I briefly mentioned the features we built into Internet Explorer 9 in response to the call for "do not tracking" mechanisms that are browser-based.

And if I could expand on that slightly, what Internet Explorer 9 does with the tracking protection feature is that it allows consumers to turn on this feature and import any tracking protection lists that they want, which would be a list of third party sites that may be tracking individuals across the Internet. And when you turn this on, it blocks those connections to those third parties.

So, for example, if you went to a major news site and there were 10 third parties providing content on that site, which is not an uncommon scenario -- a couple of them may be advertising networks. One may be a stock ticker; one may be an embedded video, all coming from different sites. If one or more of those sites were listed on a tracking protection list that a user had installed through this feature, that call just wouldn't be made, and that would cut off any ability for that third party to collect any information because it is blocking the content coming down, and it is blocking any other connection going back up to that third party. So the nice thing about that is it is technology neutral. It doesn't matter if they are tracking through a cookie or through logging IP addresses, or even one of these super cookie mechanisms, the connection just isn't made.

It is kind of a sledgehammer approach. It blocks the content, too, but it is very effective.

In contrast to some of the other "do not track" mechanisms that

have been mentioned during the opening statement of Ms. Bono Mack, she mentioned that the Mozilla approach sends a signal to the receiving Web site that says "do not track." The problem is there has been no definition or common understanding as to what a Web site is supposed to do in response to that signal. And we are working with the World Wide Web consortium and with Mozilla and with privacy advocates to try to provide some definition around that, so that there are additional choices for consumers that we support.

But in the interim, the approach that we have taken is effective and doesn't rely on the receiving third party to make any choices or decisions.

Mr. Gonzalez. Technology has created, we want to say it the dilemma or the challenge, so technology would be the answer. And I only have a few seconds. But let me get this straight.

What you are able to provide the Internet user is going to be where they select the third party sites. This is not going to be a generic or universal application where I, Charley Gonzalez, I could just have this feature, and I don't have to identify a particular third party; it would just be all encompassing. It doesn't matter what contact or who I contact or who I connect with, I wouldn't have the ability to have that feature. It is all contingent on identifying the third party site.

Mr. Hintze. You can download a list from an entity you trust; a privacy advocacy organization could publish a tracking protection list. Any organization could publish one. You could create one

yourself, but as you mentioned, you would have to know. But you can rely on an organization to do that. And there are some out there that are very comprehensive. They have many, many third parties on there, that if you import that, it would block those third parties. So you don't have to do that sort of leg work yourself. You could rely on a trusted entity that you trust.

Mr. Gonzalez. You are on the right track.

Again -- Madam Chair, if I could have a few extra seconds --

Mrs. Bono Mack. There will be a second round if we can.

Mr. Gonzalez. I think we are going to have a second round, so if you can wait my turn again.

Mrs. Bono Mack. The chair now recognizes Mr. Guthrie for 5 minutes.

Mr. Guthrie. Thank you, Madam Chair.

Thank you for coming. Thank you for being here today.

Just a couple of questions as we move forward.

Advertising has always been about behavior. All of us are behavior advertisers. I want to send pieces of mail to people who vote. So we always get the voter rolls out, and we go through. I know it is a public record, but it is private behavior that is made public for us to move forward and see.

But what we have to do is to try to balance now that things are in hypermode with the technology. If you make a phone call, somebody knows where you are, they can find out where you are at all times. If you use your discount card, that is why they give you a discount; they

want you to swipe it so they can track your behavior shopping so they know how things are going.

But the question is we have got to try to balance.

I know that Bing, Yahoo, Google, any search engine wants to outdo the other one. They want to be faster, better because they want me to go to it, because the more people that go to it, the more valuable their advertising space is, just like if I want to watch a Kentucky basketball game for free, they have got to take a break every 8 minutes to show a commercial, so I can watch it for free. And that has happened on the Internet, but the difference is they can individualize it, I guess.

So I guess my point is, and I guess Dr. Acquisti, since you studied this -- and you said you didn't think it would affect the economic behavior of this; we talked about the $33 billion of job loss. Ms. Blackburn asked a question. You said you didn't think it would affect it.

If the search engines aren't getting the revenue from the advertising to let me to use it for free and they are competing against each other to make it better, so it is far better than it was a year ago, what is going to drive that innovation if the advertising dollars -- if we follow the European model, what is going to drive the innovation or continue to be free to me, or will we have to start paying for it like when we did debit cards? We took a vote here to change the debit cards. Now the people who voted for it are complaining about the fact that banks are charging for it. So, I mean, that is the

question what I want to ask you. How is it not going to affect -- how is it going to work economically if we do the European style system?

Mr. Acquisti. Definitely. So to clarify the point I was making in the testimony was not that there will be no effects, but rather I was pointing out that the so-called free goods we get online are free only if you don't consider the fact that we end up paying for them as consumers through a different channel as we purchase the goods, which are offered online.

Mr. Guthrie. Like watching a sports game on television for free. You have got to sit through the commercial to watch it.

Mr. Acquisti. That was the point I was trying to make.

Mr. Guthrie. Or you can do Pay-Per-View and watch it without commercials. But a lot of us don't want to pay for a search engine. We just want it. And so who is going to pay for it if we don't do it? Is the model that you have to pay individually, like you have to sign up for a search engine, like $10 a month or something as opposed to getting it for free? How is it going to work if we don't have advertising?

Mr. Acquisti. Actually, if I may, the alternative I don't believe is between no advertising and advertising. First of all, this is in parentheses, free content existed even before the age of behavior advertising. In fact, we don't know exactly how much of the free content now available online is due to behavior advertising versus quote-unquote more traditional.

Mr. Guthrie. I only have a minute and a half. So maybe we can

catch you in the second round.

I wanted to ask Ms. Dixon. I had an uncle or great uncle who had early-onset Alzheimer's. He died in his 50s. I am 47 now. So if I go online and maybe I don't know this and I Google early-onset Alzheimer's, what do I need to fear that I don't know, because if I Google that right now, what could happen -- because you were saying that -- I mean what would happen if I went in and search-engined that, what could happen to me that I don't know about?

Ms. Dixon. In a search engine, I don't think you have so much trouble because most of the ads are contextual, and it is really not that big of a deal. Maybe you will find a rogue actor advertiser, who is kind of a low-hanging fruit and out of the ballpark and not playing by the rules.

But in general, where you really need to be concerned is when you go to -- a couple of different things. There are three scenarios. One, you go to a scammy site that is just built based on fear, and someone slapped up a Web site, and there are all sets of third parties on it, and they are gathering up any information you are filling into a form, and they are selling it on to a direct marketing list. That happens more often than I even want to describe. It is a terrible thing when it happens to anyone. That is what you need to fear.

The second thing would be if you go to let's say a very legitimate Web site. It is a legitimate business. There are some very large Web sites that you could go to that focus on health care and type in your query. What can happen is that you simply begin to see advertisements

that are focused on early Alzheimer's. That is really not that big of an outcome in my book. That doesn't bother me that much.

What bothers me more is that there may be a number of third party entities on that page. It could be advertisers; it could be other kinds of third parties. It could be Facebook. It could be all sorts of different third parties now in this new kind of digital technology.

Mr. Guthrie. What can they do to me?

Ms. Dixon. Well, that is the thing. What they can do is they can take that information that you have given and merge it with other information, and that becomes a part of a profile about you or the computer you are using. If you have registered for the site, it becomes part of your profile.

Mr. Guthrie. And somebody would use that to do what that would be negative?

Ms. Dixon. They can sell it. They can sell it outright. It happens every day.

Mr. Guthrie. So somebody can say, "He must have Alzheimer's" because you Google that?

Ms. Dixon. Or he is interested in Alzheimer's information.

Mr. Guthrie. And that is bad. Okay.

Ms. Dixon. Or has Alzheimer's, correct.

Mrs. Bono Mack. The gentleman's time has expired.

The chair recognizes Mr. Butterfield for 5 minutes.

Mr. Butterfield. I think we are all well aware that a lot of free content available on the Internet is made possible by advertising, all

types of advertising, not just behaviorally targeted advertising. I think consumers understand that they get free content thanks to the ads that surround that content.

But what they often don't understand is that the spaces where those ads are placed might sometimes be watching them.

As one privacy expert who has looked at consumer attitudes and behavior regarding privacy has put it, consumers accept the idea that ads support free Internet content but do not expect data to be part of that exchange. Many in the Internet tracking industry argue that steps to empower consumers to decide for themselves whether they want to allow tracking of their online activity will kill free Internet content. I, for one, do not buy this argument. I don't buy it because reported advertising revenue numbers don't support it.

The last figure that we have been able to track showed that revenue from behaviorally targeted ads was $925 million in 2009. That is almost a billion dollars. This figure was reported in a large 2010 marketing industry blog post. This is the only easily accessible piece of information that we have been able to find that specifically breaks out revenue from these ads. In 2009, overall revenue from every type of Internet advertising was $22 billion, almost $23 billion.

Now, the first question is open to anyone who wishes to respond. Can any of you provide more recent figures that clearly break out the amount spent on behaviorally targeted ads last year, not on display advertising generally or all online advertising, but specifically on behaviorally targeted ads? Do any of you have any data that you feel

you can provide.

As I used to say when I was a judge, let the record show that no one responded.

Ms. Woolley. Let me just respond that according to the FTC's definition of what online behavioral advertising is, one of our partner trade associations in the DAA, the Internet Advertising Bureau, found that over 80 percent of the ads that are delivered are OBA or online behavioral advertising. And actually, I think, sir, the revenue number is significantly higher than the blog post that you cited. DMA has done several studies more recent than 2009 with global insight, and I think the number is actually substantially higher.

Mr. Meyer. If I can add to that, I can follow up and get you the specific estimates. I think it is in the several billion dollars. And the other important thing to think about, there are two other important points.

The first one is the definition of what is behavioral, and that is why a legislative approach could be so dangerous, because it could be anywhere from a reasonably small percentage to a number as high as 70 to 80 percent. That is the first piece.

And the second one is that this is the fastest growing part of the online advertising industry. So if you break out the different pieces, the data-driven behavioral and network advertising is growing at the fastest rate inside of an overall very fast-growing industry, along with video advertising.

Ms. Woolley. I guess one other point I would like to make here,

too, is that there was a conversation about targeting individuals. I represent the Direct Marketing Association. Targeting individuals is not a new phenomenon. It is something that -- the Direct Marketing Association is close to 100 years old. That is something that has gone on for close to 100 years. And direct marketing methods and techniques are part of the curriculum of almost every university that has a direct marketing program. So these are actual techniques and methodologies that are taught in university.

So the thing that the Internet has done is make the process faster and more nimble. But the techniques and the methods are not knew.

Mr. Butterfield. All right. That is helpful.

Thank you. I yield back.

Mrs. Bono Mack. I thank the gentleman.

The chair recognizes Mr. Kinzinger for 5 minutes.

Mr. Kinzinger. Thank you, Madam Chair.

Thank you all for coming out and for participating.

I will be the first to say that I think government needs to put an end to needless regulations that do little to protect the consumer or protect jobs.

But I am not convinced personally that "do not track" legislation is the right approach. I do have some serious concerns that without privacy protection, consumers can lose confidence in the online free market.

Each of you represents responsible companies that are working to inform consumers in their privacy choices online. But in the end, you

don't represent the bad actors that could potentially come and undermine your efforts.

So my first question is to all of you, and we can do the hand raise thing. You all basically answered this, but I want to see for myself: Do you think the committee should pass privacy legislation to ensure the bad actors don't undermine your efforts?

Who is a yes on that?

And who is a no?

So two noes.

I am also deeply concerned by what a Stanford study that appeared in the National Journal yesterday said. The study shows that Web sites are unknowingly leaking email addresses, user names, and other personal information to ad networks. If consumers had the choice and were aware of this transfer of personal data, I don't believe the mass majority of consumers would support Web sites selling this personal information to outside parties. Should consumers be required to opt-in to allow Web sites to share this personal information?

And let me also expand on that. I am not talking about a 30-page privacy statement that nobody reads. I don't think I have ever read a 30-page privacy statement in my life. Something that should clearly be presented before it is being shared.

So should opt-in be a requirement? I guess we can start right to left --

Ms. Dixon. It is really complicated.

Mr. Kinzinger. Well, let's try to keep it very short if we can.

Ms. Dixon. It is a challenging question to answer in a black-and-white manner. If there is a first party relationship, that is on thing, but if we are using first fair definitions of first party, first party fine. Third party, that is a whole different thing. It really needs to opt-in for third party.

Mr. Kinzinger. Doctor?

Mr. Acquisti. I actually agree exactly with the statement.

Mr. Kinzinger. Anybody else have anything?

Ms. Woolley. I have an opinion, and it is a complicated question.

The wonderful thing about the icon is that -- which is over there; I don't think you were in the room when I mentioned that -- is that it gives the consumers a choice about opting out of those third parties who are on a site and not allowing collection and use of the data. And it is easy. It is transparent. It is ubiquitous at this point. You can't be on the Internet without seeing the icon.

Mr. Kinzinger. You are more of an opt-out versus an opt-in.

Ms. Woolley. Well, there are lots of reasons that -- the Stanford -- and I don't even want to call it a study. It was the musings of a graduate student. It was not peer-reviewed. There was no methodology. That is all that it was. There are great reputable studies out there, but that was not one of them.

As my colleague from Microsoft mentioned earlier, there are lots and lots of reasons why third parties are on Web sites. Some of them are there to serve ads. Some of them are there to collect information, but others are there to deliver content, like sport scores and stock

scores. So if you are absolutely blocking third parties or you are collecting opt-ins for absolutely everything for third parties, the consumer has no -- I mean, we go to CNN.com. We know what we want. And if I have to permit every single one of them, I don't know what I don't know.

Mr. Kinzinger. Any of the other three of you?

Mr. Meyer. I would like to go back to something you said about "do not track" and the need for legislation. The reason I said no is because it already exists in the form of the Federal Trade Commission Act. Just this morning, the Federal Trade Commission settled with a company for deceptive trade practice. And the situation you described tends to be firmly in line with those deceptive trade practices, and that is the right role of government --

Mr. Kinzinger. Thank you. I am going to have to cut you guys off because I have one more question.

I have an update from a major telecom provider which says they are going to start sharing user information with local companies based on their physical address on an opt-out. They are also going to start recording and sharing URLs of Web sites visited with actual, physical locations of that users wireless device. It does say there will be no information that is personally identifiable, but after seeing the study, which you call into question but I have some interest in, I am not sure that it is possible. Should sharing a user's geolocation data with ad networks require a clear concise opt-in from the consumer? If we could go -- do you three have anything, first?

Mr. Hintze. I would be happy to address that.

We operate a phone operating system as well as many of our other things in addition to our ad business, and our approach has been that we believe that the collection of precise geolocation information should require an affirmative consent on behalf of the user.

Mr. Kinzinger. Does anyone disagree with that?

Ms. Woolley. The one thing I do want to say is if information as you are describing it right here is aggregated, that geolocation that is aggregated and not specific to an individual could be used for all sorts of business decisions, not --

Mr. Kinzinger. We are talking about marrying that with a specific individual, though, in this case.

But thank you all for your generosity.

I yield back.

Mrs. Bono Mack. The chair recognizes Mr. Dingell for 5 minutes.

Mr. Dingell. Madam Chairman, thank you. I commend you for this hearing.

These questions are yes-or-no questions.

To all witnesses, starting at your left -- rather at your right and my left, is it your understanding that interest-based advertising supports much of the free content of the Internet, yes or no? Beginning with Ms. Lawler.

Ms. Lawler. Yes.

Mr. Hintze. Yes.

Mr. Meyer. Yes.

Ms. Woolley. Yes.

Ms. Dixon. Yes.

Mr. Dingell. No disagreement.

Further, is it your understanding that the consumers expect much of the content they consume online to be free, yes or no?

Ms. Lawler. Yes.

Mr. Hintze. Yes.

Mr. Meyer. Yes.

Ms. Woolley. Yes.

Mr. Acquisti. No.

Mr. Dingell. So no disagreement on that.

Do you believe that all consumers have the same view of interest-based advertising, yes or no?

Ms. Lawler. No.

Mr. Hintze. No.

Mr. Meyer. No.

Ms. Woolley. No.

Mr. Acquisti. No.

Mr. Dingell. So we have agreement there.

To all witnesses, is it fair to say that imposing ridged privacy requirements on interest-based advertising would have a drastic effect on the way consumers currently experience the Internet, yes or no?

Ms. Lawler. Can you ask the question again, please?

Mr. Dingell. Is it fair to say that then imposing rigid privacy requirements on interest-based advertising would have a drastic effect

on the way consumers currently experience the Internet, yes or no?

Ms. Lawler. I am going to say probably.

Mr. Hintze. I know you asked for a yes or no, but I think it depends on what you mean by rigid. We think there can be some baseline privacy requirements that are perfectly consistent with the business models and innovation that we are talking about.

Mr. Dingell. I will not object to any of you panel members giving additional response for the purposes of the record because that is fair to you.

Mr. Meyer.

Mr. Meyer. I would agree with Mr. Hintze that it depends on the level of the ridgedness, but the potential for it having a negative impact is unnecessarily high in my opinion.

Mr. Dingell. Ma'am?

Ms. Woolley. Well, I have to give you the lawyer answer, too, which is, it depends. Because I think our program imposes very rigid requirements, and I think the way we have done it does not adversely affect the Internet.

Mr. Dingell. Our next two panel members, please?

Mr. Acquisti. My answer is not necessarily.

Ms. Dixon. My answer is not necessarily. However, I am not sure that is the only thing we should be focusing on.

Mr. Dingell. So I guess that is a maybe.

To all witnesses, do you believe that the current industry efforts to protect consumer data privacy are sufficient, yes or no.

Ms. Lawler. Yes, but we can do more.

Mr. Hintze. Generally, yes.

Mr. Dingell. If you please, Mr. Meyer?

Mr. Meyer. We are off to a very good start, but we need to support of, in particular, of this committee and the Federal Trade Commission to accelerate the acceptance.

Ms. Woolley. Could you repeat the question?

Mr. Dingell. Do you believe that current industry efforts to protect consumer privacy are sufficient?

Ms. Woolley. I believe that they are sufficient, but I also know that our program is evolving, so we have the ability to evolve and get stricter as times change.

Mr. Acquisti. Unfortunately not, but I believe there are industries, privacy technologies which could definitely help.

Ms. Dixon. At the current time no, however I believe that the efforts could be improved through self-regulatory reform, such as involving consumers, having independent bodies overseeing the efforts and other things that would --

Mr. Dingell. I have a minute and 3 seconds left. Do you believe that such efforts can be improved, or do you believe that Congress should pass data privacy legislation?

Ms. Lawler. We believe that there is a significant opportunity for businesses to come together and lead more and do more in a self-regulatory approach. If Congress were to act, it would need to be a principle-based approach that is flexible and nimble and is not

overly prescriptive.

Mr. Hintze. I think current efforts can be improved, and they are being improved, and I think that there is also a role for baseline privacy legislation.

Mr. Meyer. I don't think it is necessary, but if there were any type of legislation, it would need to provide safe harbor for existing problems.

Ms. Woolley. I do not think that legislation is necessary, and I think our table includes many wonderful American companies, including GM, and I would invite everybody here to be part of that program because our table is open.

Mr. Dingell. Sir?

Mr. Acquisti. I believe it can be improved and the legislation can foster the deployment of technologies based on public/privacy interaction focused on privacy and data sharing.

Ms. Dixon. Legislation will help and improvement of the current regimes will help as well.

Mr. Dingell. Now, again, to all witnesses. I am intrigued by the concept of "do not track" list. Is it advisable for the Federal Government to mandate a "do not track" solution that prevents people from being tracked by the multiple devices that they use to access the Internet, yes or no? Starting with you Ms. Lawler.

Ms. Lawler. We don't believe that it makes sense for the government to mandate a "do not track" approach. We think it needs to evolve in terms of tools and technology.

Mr. Hintze. We agree with the comments of Ms. Lawler. The FTC's done a good job of encouraging industry to move forward, but the industry has responded in an active way.

Mr. Meyer. Legislative mandates for technology we don't think are the right approach, especially because it would extinguish a very vibrant competitive entrepreneurial market that provides these tools today that continue to evolve and compete with each other.

Ms. Woolley. People need education. They need to know what is going on. They need to be make their own choices.

Mr. Acquisti. It may not be the ideal solution, but it is better than no solution

Ms. Dixon. We do support "do not track" legislation.

Mr. Dingell. I note I am out of time, Madam Chair.

Mrs. Bono Mack. The chair recognizes Mr. Olson for 5 minutes.

Mr. Olson. I thank the chairwoman.

And I want to welcome the witnesses and giving us your expertise. And just for the record, my neighbors' kids were not out in the lobby early this morning. They are still back home in Texas as far as I can tell.

And my first set of questions are going to be for you, Ms. Woolley, and I want to follow up on the line of questions from Ms. Blackburn from Tennessee about the economics of privacy. And I am familiar with the Digital Advertising Alliance's effort to develop the advertising icon so proudly displayed over here, which provides consumers with notice and choice about ads being delivered to them through behavioral

targeting.

Many of the big companies have adopted the icon, but as you know, small business drives job creation in our economy. So can you elaborate more on how you have made the icon available to our small businesses for free?

Ms. Woolley. Thank you for raising that. It is actually a great story. We have made the icon available for free. If you have less than $2 million of revenue that is derived from online behavioral advertising and you are a small business, you can get the icon for free. We also have a program with one of the ad networks that deploys the icon on small business Web sites.

And the thing that that does is it enables those small businesses to get revenue from the ad networks because their ads are -- they are now targeted ads. So it enables small businesses not only to get revenue from the businesses that they are in but from the advertising world as well. So it is actually a great program.

Mr. Olson. That is my feeling as well.

Would you say that the icon provides a competitive advantage to companies that adopt it? To put it another way, are companies competing for business based on privacy features?

Ms. Woolley. Actually, it is very interesting. When we launched the icon, we did not anticipate it being a trust seal of sorts. We thought that it was really just a consumer notice and choice mechanism, but it has actually wound up being a trust seal. And companies are competing based on the fact that this is a symbol that

consumers can see; they know, they know that there are principles and enforcement behind it, and they wind up trusting that site much more than they would have otherwise.

Mr. Olson. So it actually is becoming competitive and driving --

Ms. Woolley. Absolutely.

Mr. Olson. Finally, in your testimony, you mentioned one of the major benefits of industry self-regulation is its ability to respond quickly to changes in technology and business practices. And some have raised concern that data collected for advertising purposes could be hypothetically used as a basis for health insurance or credit eligibility decisions, but we don't have any actual examples or cases of this happening, but DAA is still going to address these concerns and help to expand your guidelines to clarify these kinds of practices that would be prohibited. Can you elaborate more on that initiative?

Ms. Woolley. Yes, sir. You actually have stolen a little bit of our thunder, because in a couple of weeks, we are going to be making the announcements that all of the companies that comply with the DAA program will be prohibited from making eligibility decisions, any kinds of eligibility decisions based on data that is advertising and marketing data.

So I know that the chairman of the Federal Trade Commission is fond of saying, if you buy a deep fryer online, then you will be denied health insurance. And we want to make it abundantly clear that that kind of decision is not acceptable. It is not part of the program. If you do that and you are part of the program, you will be thrown out

of the program and referred to the FTC.

Mr. Olson. I didn't mean to steel your thunder. That is not what I intended to do.

This is a final question for all witnesses. Because of my time, I will probably have to make it yes or no questions.

It is my understanding that the FTC has received a very wide range of comments concerning consumer attitudes and behavior when it comes to privacy. My interpretation of that wide range in comments, there is no clear consensus. Some consumers feel more strongly than others about online protections.

And so my question for all of you, starting to the left and work to the right there, is there any hard data that you are aware of that demonstrates the level of discomfort or the percentage of consumers who are willing to forego the benefits of free content online in order to avoid being tracked, yes or no? Starting at the end with you, Ms. Lawler.

Ms. Lawler. I don't have any specific information from our consumer or customer studies that would indicate that particular type of action.

Mr. Hintze. It is hard to interpret a lot of the studies out there because, as Dr. Acquisti pointed out, there is a discrepancy between what people say and what they do. So you can find a lot of studies that say people are very concerned about privacy, and I believe there is something behind that.

But in terms of the tradeoffs, that is harder to quantify.

Mr. Meyer. We haven't seen that research. It is the same juxtaposition between what consumers say and what they do. But it is something we are actually looking at Evidon right now.

Ms. Woolley. People vote with their feet or with their pocketbooks. And I think it is accurate to say that people are concerned about privacy, because they are. And I think it is also accurate to say that people are not afraid to use technology, and they are not afraid to use the Internet. Sales on the Internet have gone up exponentially in the last 3 years, and new devices come out. People love them. They buy them. They down load apps. They are very willing to adopt all of these new things as they come out. They love them.

And we are very mindful of the fact that as an industry, we are the ones providing all of these great and wonderful and engaging things to people, but we have to take into consideration their desire for privacy. And that is the main reason that we have created this entire program.

Mr. Olson. You have met my 14-year-old daughter.

Mrs. Bono Mack. The gentleman's time has expired. And there will be a an opportunity for a second round, but there are still some other members needing to ask questions.

The chair recognizes Mr. Stearns for his 5 minutes.

Mr. Stearns. Thank you, Madam Chair, and let me compliment you. This is a great hearing, and I am glad to have all of these witnesses here.

Ms. Woolley, let me say that I think that your logo and what you

are doing I think is terrific, and I think it goes a long way toward this self-regulatory behavior and program. And we have just got to educate the consumers what it means when they see your logo. And hitting that logo, when I look at your slides, it starts to move into a little complication. And had you thought about perhaps even simplifying it even further, or do you think you are at the point where it is pretty well understood by consumers?

Ms. Woolley. I don't think it is at the point where it is understood by consumers. We are actually later in the fall going to be launching an education campaign just to get at that point. We really hope that over time consumers will look at this symbol and know exactly what it means, kind of the way consumers look at the recycling symbol. Fifteen years ago, nobody really knew what the recycling symbol was and how they do it.

Mr. Stearns. This Good Housekeeping Seal, which everybody recognizes, is universally accepted.

Ms. Woolley. Exactly.

To answer your question about whether the program is where it needs to be, we launched this program a year ago, and we are constantly looking for suggestions about evolving the program, making it more consumer-friendly and making it do really what all of you want it to do. So I welcome that input.

Mr. Stearns. When I look through your slides, it is almost as a consumer, I just want one big button, can I opt out, and that is it, and it is done.

Ms. Woolley. There are two ways that you can get to our opt-out. You can get to it from the icon that is on ads. The other way that you can get to it directly is if you go to www.aboutads.info, and if you go to that site, in the middle of that site is a huge check mark, and it says, for consumers, if you check on it, you can opt-out right there.

Mr. Stearns. That opt-out, when you do that, does that apply to all of your companies, or does i apply to --

Ms. Woolley. The first thing that happens is you will see your computer churning away, and it will tell you the ad networks that are operating on your browser on that computer. And you can opt-out of all of them if you want to. Immediately behind it is a screen that tells you all of the ad networks that exist, and you can opt-out of all of those if you want.

Mr. Stearns. I think it is a credit to what you are doing. When you see the European Union's privacy policy and then you see a lot of Latin America and a lot of Asian American countries have stopped -- India is starting to include a privacy policy adopted after the European Union, we are almost going to be sitting here with a self-regulatory type of operation compared with everybody else.

Do you feel there is any Federal baseline legislation that is needed at all for privacy?

Ms. Woolley. Not at this time. We have got some great privacy laws in the area of HIPAA and Gramm-Leach-Bliley --

Mr. Stearns. Dealing with financial and health care --

Ms. Woolley. Exactly.

Mr. Stearns. So you don't think there is any other area that is as sensitive?

Ms. Woolley. I don't.

Mr. Stearns. Do you think that there is any need for Federal baseline legislation for any aspect of personal privacy on the Internet? Just yes or no.

Ms. Lawler. I need to say more than yes.

Mr. Stearns. Just yes or no. If you have to check off whether we need Federal baseline legislation for any aspect of personal privacy on the Internet?

Ms. Lawler. As a company that is already regulated by some of the laws just mentioned, if there were a Federal baseline approach, we would want to see something that is principle-based. So we think that there's a potential for an appropriate baseline in place --

Mr. Stearns. I have a bill H.R. 1528. It is a privacy bill that Mr. Matheson and I both dropped.

Ms. Lawler. Yes. I have looked at that.

Mr. Stearns. Do you think there is anything in there that you think should be needed? You won't offend me if you say no. Doesn't bother me at all. I have nothing tied to my legislation.

Ms. Lawler. I think there are some things there that are workable.

Mr. Stearns. Let me go down and ask you if you think there is any Federal baseline legislation, Yes or no?

Mr. Hintze. Yes, we have been on record for a number of years.

Mr. Stearns. I know. I thought you had.

Mr. Meyer. We don't support any new baseline legislation, but having read your bill, the piece that we do like is the provision for safe harbor for self -- existing self-regulatory.

Mr. Stearns. Using the Federal Trade Commission.

Ms. Woolley. Ditto with that.

Mr. Acquisti. Yes, we do. Self-regulatory solutions tend to fail under pressure, and the recent studies have shown that there is a frequent non-compliance with NAA and the DAA initiatives among the top 100 Web sites --

Mr. Stearns. So your answer is yes, there needs to be some type?

Mr. Acquisti. Yes.

Mr. Stearns. Ms. Dixon, I assume you are a strong yes.

Ms. Dixon. Yes, and we would still like to see reforms of existing self-regulatory programs to include consumers in other reforms.

Mr. Stearns. Let me ask this last question and just ask one person, so it won't take too much time. What benchmarks are needed for self-regulation? Could you say from your experience what benchmarks are needed, since you represent the digital alliance?

Ms. Woolley. Thank you. I think the right benchmark is not how many people opt-out. I think the right benchmark is how many people are seeing icons, and do they know what it means? So I think education is the right measure.

Mrs. Bono Mack. Thank the gentleman.

The chair recognizes Dr. Cassidy for 5 minutes.

Dr. Cassidy. Thank you.

I am never quite sure I understand this issue as much as I try and understand it.

Ms. Lawler, did I hear you say that only 0.05 percent of people actually opt out?

Ms. Lawler. Here is what I was saying is, we were talking about the opt-out rates for email marketing, which is different than the discussion that the majority has focused on today around online behavioral advertising. So what I was actually listing was kind of a range of industry standard, which is 0.1 to 0.05. That is a different kind of data than what we are talking about with opt-out for behavioral advertising.

Dr. Cassidy. Ms. Woolley, Ms. Dixon raises some troubling things in their testimony. She speaks of how AOL once released some data sets; New York Times was able to track backward from these compressed data sets, supposedly disjointed, to find out where somebody lived. Now, do current self-regulating processes prevent that from happening again? Because that would certainly spook me if the New York Times was knocking on my door hey, Bill, what is happening? So you see my question?

Ms. Woolley. I am not familiar with the point that was raised.

Dr. Cassidy. Ms. Dixon, will you mention to her what your testimony said?

Ms. Dixon. In the testimony, I was talking about that we needed a larger vocabulary when we are talking about online privacy. And I mentioned the AOL data breach in 2006. What happened is researchers at the company released data sets that were anonymized information about users, supposedly, and after it was released, a New York Times reporter went through and was easily able to look at little bits and pieces of scattered information that consumers had typed into search engines, and they identified people.

Dr. Cassidy. So that said, that is troubling.

Ms. Woolley. Yes, it is troubling. And the whole issue of data breach is very troubling. And I think that we need to be very careful about separating out privacy issues from data breaches. And the data breach issues I think require some significant action by Congress.

Dr. Cassidy. Ms. Dixon, would that answer satisfy you?

Ms. Dixon. I think that what happened at AOL was part of an environment where there is not a clear idea of what privacy benchmarks and standards there are.

Dr. Cassidy. Yeah, but that was a data breach?

Ms. Dixon. I am not so sure that it was a data breach. I think that it can't easily be defined that way. Because when consumers type their search queries

into that search engine, they relied on that AOL privacy policy that says, hey, we are going to do X, Y, and Z.

Dr. Cassidy. Let me move on.

Mr. Hintze, when I log on to MSN and I put in my user ID and then

I hit in private browsing, does MSN or Bing still track me, even though Fox Sports may not or --

Mr. Hintze. The in private browsing feature in our Internet Explorer browser blocks third parties who are present on the Web site you have gone to. But when you have gone to a Web site -- say you have gone to MSN. In that case, MSN would be the first party. That is the company, that is the Web site you chose to interact with. So it doesn't block the connection to that first party.

Dr. Cassidy. So does MSN then track me across the Internet --

Mr. Hintze. No. The in private browsing, it prevents anybody who, other than the site you have chosen to go to -- so when you go to MSN, MSN knows you are there. When you go to Amazon, Amazon knows you are there. But if there were a common third party, they would not be able to track you across those two sites because you blocked them.

Dr. Cassidy. So for my home page for MSN, I have a Web site from Home Depot. Home Depot would not know, but MSN still knows. Is that correct?

Mr. Hintze. Correct. If you type www.MSN.com into your Web site.

Dr. Cassidy. Now I think I understand now how data is anonymized and theoretically, if you will, I am protected, but I gather that if you are MSN, Yahoo, or Google and I log in, that is not anonymous. That is actually me. Now, so, again, I am trying to understand this. I apologize if I sound stupid, but you can take, unlike everybody else who is anonymous, you actually know it is me. Now to what degree can

you collate that with other information from other third parties?

RPTS BLAZEJEWSKI

DCMN NORMAN

[11:04 a.m.]

Mr. Hintze. You are correct that when you sign into a site you have self-identified yourself to them. You have said, hey, it is me; you have a billing relationship with them, for example. There are different methods used within the industry to anonymize data. Some are stronger than others.

Dr. Cassidy. Does MSN anonymize my data once I have signed in, or do they keep it much as apparently AOL did, as a dataset which could be leaked and which could then be tracked back to my home address?

Mr. Hintze. For search data, we store search queries, for our Bing search engine, we store search queries in association with a unique identifier which we put technical controls, including one-way cryptographic hashing, to prevent that data from being associated with identifiable data that you may have provided to another one of our sites.

So, for example, if you had a Hotmail account and you had given us your name and your city, we would have that in one database, and we put in measures to make sure that when you put in your search query, that data is not associated, it is in different buckets.

Dr. Cassidy. I am out of time, but I may hang for the second round. Thank you, I yield back.

Mrs. Bono Mack. I thank the gentleman, and a few of us have stuck

around for a second round. So I am going to begin with 5 minutes for myself, and the question -- I don't know if it would be better for Mr. Hintze or Mr. Meyer or who. Anybody can take a crack at this. Something that just popped into my brain was deep packet inspection, and we haven't talked about that at all today. But my example is the other day I received an email from a friend of 40 years ago who I did gymnastics with. The message said "gymnastics" somewhere in there, and sure enough, for the first time ever, I received a bunch of ads about buying tumbling mats. I never, ever have gone online to look for tumbling mats.

Deep packet inspection, is it a part of your thinking here, or is it as troubling to you as that glaring example was to me?

Mr. Hintze. I will just briefly respond and then let others. We don't engage in it. It is not how we run our ad network. Even within our own email online service Hotmail, we do not base advertising based on the content of your email. Other companies do that; we do not.

Mrs. Bono Mack. Have you supported in the baseline legislation, you have said you supported in the past, something that --

Mr. Hintze. We have supported Federal baseline privacy legislation. Like others on the panel, we think it should work in conjunction with self-regulatory initiatives with safe-harbor provisions, but it is something we have supported

Mrs. Bono Mack. And DPI, would you support throwing that in there, then? Deep packet inspection, would you support putting that in there?

Mr. Hintze. You know, I think that one of the challenges with legislation is that when you get into particular technologies and try to ban technologies or methods, that can have unintended consequences.

Mrs. Bono Mack. Thank you.

Mr. Hintze. You talk about deep packet inspection, you talk about supercookies, there are certainly uses where we think those methodologies are inappropriate and invasive and not consistent with consumer expectations or choices they have made. But one can imagine that those kinds of technologies would be put to very beneficial uses, and so I think we have to be very careful about trying to regulate specific technologies.

Mrs. Bono Mack. Thank you. Mr. Meyer?

Mr. Meyer. I agree with Mr. Hintze. I think that Evidon's purview doesn't expand out into deep packet inspection, but our opinion is similar to the opinion on supercookies, that right now we don't see it as a good use in online marketing, but legislation carries with it a lot of risks around legislating a technology when things are evolving this quickly.

Mrs. Bono Mack. Thank you. I really enjoyed Mr. Guthrie's questioning earlier. He really got to the crux of the whole matter, what does this mean.

Miss Dixon, you took a crack at the answer, but it is the reputational harm that we are all concerned about, and then I am also concerned about a bridge too far. When does reputational harm then translate into physical harm? And those are the questions that I think

we need to grapple with as policymakers. But I have also -- and I keep going back to how the content, we had, you know, P2P, we had Kazaa, and Napster, and some things come up, and then i-Tunes came on the scene to deal with peer-to-peer, and now we are back to like a Spotify method where content is all free again. You can download 3,000 songs for free.

So it is still evolving, and the business models are evolving. But really, me perhaps jumping ahead here to Intuit. Reputational harm for consumers is one thing, but I know that Intuit, the reputational harm that could happen to a company should they breach consumers' confidence is also something worth considering.

And I think, Ms. Woolley and Ms. Lawler, if you would like to take the next minute and 45 to talk about your version of what would happen to your company if you lost consumer confidence by breaching what consumers believe you do to protect them.

Ms. Lawler. When we conducted our customer research to understand their attitudes about privacy and how data was used, our customers were very clear that as long as we were open and honest and clear with them about what we were doing and giving them choices, that they would trust us, continue to trust us. So they said things like, "I will continue to use your products because of the data stewardship principles that you are showing us; I feel safer in an unsafe world."

Conversely, what we saw, because we did quantitative research where we got a lot of verbatims that I have just mentioned, but we also did qualitative studies where we talked one on one and in small groups, and in those sessions, I think our customers -- and I think it is a

proxy just for consumers at large -- when you are dealing with unique data about me that is sensitive to my life or my business, I want control, I want to know what is going on, and if you screw that up, I am certainly going to consider going somewhere else.

And to the point someone made earlier, consumers make choices with their feet and with their wallets. They also make choices in the online world essentially with their fingers and eyeballs. So that is why being as open and clear and transparent, starting with this idea that it is the customers' data, not ours, and putting them as much in control as possible, is just critical to our success. It enables us to actually innovate and use their data to benefit them in ways that improve their lives.

Mrs. Bono Mack. Thank you. Ms. Woolley, if you would like to.

Ms. Woolley. Thank you. One of the things that is great about the DAA program is that in order to get the principles in the first place, thousands of companies participated in that process, and the six trade associations that developed it also represent thousands of companies, so it really is a consensus-based program. And the reason that so many companies came to the program and came to the table was because they are all intent on doing the right thing. Obviously there are outliers out there who may or may not be as interested in doing the right thing, but the goal of the program is to get as many companies into the program as possible, and so the issue of reputational harm is clearly front and center for all of them.

Mrs. Bono Mack. Thank you, and my time has expired. And I

recognize Mr. Butterfield for 5 minutes.

Mr. Butterfield. Thank you. Social networking sites like Facebook have made it possible for Internet users to share the details of their lives. The things users share can include seemingly mundane and harmless things like where they were born, or head shots and picture profiles. It can also include more intimate and personal details, like how they are feeling physically or mentally, their relationships, their political leanings, or even their work history or other affiliations. Some choose to put all of this out there for the whole wide world to see -- I am not one of those, but some do -- while some choose to make only the barest of details available to the world and selectively share based on their preferences.

Professor, in your testimony you discuss briefly a couple of studies you have contributed that support the view that consumers' ability to make rational and fully informed decisions about their privacy preferences are constrained, constrained both by our limited ability to process information available to us, and advances in technology whose implications can't be understood or predicted by consumers. Specifically, you mentioned a study in which you were able to identify individuals and infer personal information about them using facial recognition technology in photos they had posted online on sites like Facebook. That is absolutely incredible.

Can you please discuss this study a bit more, briefly describe what you did, what bits of information you used, how easily available it was to you, and what further information you were able to infer?

Mr. Acquisti. Certainly. Indeed, our study was about finding out what happens when you combine publicly available information with off-the-shelf technology such as face recognition and cloud computing, and you put them together and you try to identify individuals online and offline and then infer more sensitive information. What we did, we started from images of faces of people that I could call them anonymous in the sense that we didn't have a name when we started the experiment. These images either came from online environments such as dating sites or from the State, students on the CMU campus. We used face recognition and cloud computing to compare these images to images we had downloaded from publicly available data, profiles on popular social networking sites, and when we found matches between a face in the first group and a face in the second group, we could then infer probabilistically the name of the person, up until then anonymous. With the name, we could then search for personal demographic information.

For instance, from Facebook profiles we can find often the hometown where the person was born and the date of birth, and then with the hometown and the date of birth, using an algorithm we developed 2 years ago, we ended up predicting the Social Security number. So the sequence is start from a face, find a name online associated with the face, find publicly available information, not sensitive, but demographics for instance for the person, and with that information infer something more sensitive. It is a process of data accretion which shows the challenges we face in protecting privacy.

Mr. Butterfield. You mentioned Social Security numbers, and that is somewhat intriguing. Are you saying that you are able to possibly predict Social Security numbers based on simple demographic data put up by individuals on Facebook?

Mr. Acquisti. Yes. When I say "predict," I stress that I am talking about a probabilistic prediction, not deterministic. What I mean is that a Social Security number has nine digits, and we would not be able to predict with a single attempt all nine digits at the same time, so our degree of accuracy changed, depending on whether we consider only the first five digits or all nine. But the stories that -- and we showed this 2 years ago, because data about Social Security numbers is already publicly available -- it is called the so-called death master file. It is a public database of all Social Security numbers of people who are dead, and because we have so much demographic data for people who are alive, we can interpolate, combine the two datasets and end up predictions as a sense for alive individuals.

Mr. Butterfield. Let me yield to the chairman.

Mrs. Bono Mack. I appreciate that very much. I think this is an important point that needs serious clarification. You can find all of that data on any public figure right now by going to a bio. You can open a book, somebody has written their life story. You don't need to create an algorithm, you can just do that.

Why aren't people just creating, I mean other than creating the Social Security number, but you are trying to protect people from -- for

example, any Member of Congress, all that data is out there. So how is it different?

Mr. Acquisti. So, indeed, there are two points to make here, one specific to as a sense. In recent years the regulatory approach has been towards making Social Security numbers less available, because we know they are so sensitive. And in a way that is well intended, a good meaning; but the challenge we show with our results is that even if you make Social Security numbers less available in public documents, they can still be predicted from otherwise publicly available data.

Mr. Butterfield. Thank you.

Mrs. Bono Mack. Thank you so much, Mr. Butterfield.

Mr. Butterfield. Uh-huh.

Mrs. Bono Mack. But your point that you began with, I think facial recognition technology is troubling for everybody, but your point was you are not critical of Social Security numbers. You are talking about how easy it is to search because, you know, we could be taking a picture of any of you and suddenly by tomorrow have your Social Security number.

Mr. Acquisti. This is absolutely correct.

Mrs. Bono Mack. This is a privacy debate. On the online world we are asking for more than perhaps has been out there for years, and these things aren't happening. So I just want to point that out, and I have overexhausted his time, so I need to -- okay, yes, if you can respond briefly.

Mr. Acquisti. The Social Security number prediction is just an

example what can be done. The story we were telling with this recent study is that we are now close to a point where you can start from an anonymous face in the street and predict sensitive, not publicly available, but sensitive information about the person.

Mrs. Bono Mack. I thank the panel and the gentleman for yielding to me, and I am happy to now recognize Mr. Stearns for 5 minutes.

Mr. Stearns. Thank you, Madam Chair. We hear from consumers and from researchers like the professor today, and even from Intuit's own research, that privacy policies are too complicated and consumers don't bother to read them. And myself, if it is one or two pages I don't go further. And so I think most consumers just don't take the time. And then, of course, if the privacy is on the thin side and they are just -- such that they don't advocate enough, enough protection.

So I guess, how do we bridge the gap and provide full disclosure without alienating the average consumer who is not a privacy professional? It seems to me that is about where we are. If we are talking about self-regulatory incentives, then you have got to have some kind of policy which bridges this gap and provides the information without confusing the consumer. So I thought I would just go from my left to my right, and maybe some ideas of how we could do this so that consumers are educated, for one; and two, that the privacies are not complicated and maybe design work or something like that, some ideas.

Ms. Lawler. We are experimenting with different types of what I would call explanations to customers, and that is really out of our research -- and some of our early findings suggest similar to what we

have heard a little bit about today, a simple, plain English explanation in context. So you can't offer big blanket opt-in or opt-out or whatever kind of choice at the beginning of something where it is not relevant to me. I don't understand it. Customers have been very clear about that. And I think there are probably other studies that validate that, but in context.

So we are actually running tests right now. We don't have the data yet. We would be happy to come back and share that at a future time.

Mr. Stearns. Okay.

Ms. Lawler. One of the other things that we did that I think -- just a couple of other quick thoughts, sir -- is if we stopped thinking about privacy policies and privacy statements and put it in this framework and this idea that is plain, simple, short explanations, you have to have a policy somewhere, but really what consumers want is something that is simple, easy to understand, real-time. And if companies haven't done it, what I would suggest they do, which we did recently and have made improvements significantly, is run your policy statements, your explanations, through a grade-level analyzer. So we did that, and we have simplified our language so that it was closer to a 9th grade level rather than where we started a couple years ago at a 13th grade level.

Mr. Stearns. Okay. Let me go through the panel here. I have only got about 2-1/2 minutes left.

Mr. Hintze. Yeah. To cut this short, I agree with everything

Ms. Lawler said. I think that in our experience the challenge is to get information in front of people when you are most likely to capture their eyeballs and their attention, and sometimes that means at the point of a decision making, when they are making a particular decision. Sometimes that can be too disruptive because they are so anxious to get the thing done that they are trying to get done, that if you put something in front of them, they are just going to hit "cancel" or "yes" or whatever the default is. So sometimes it is at the time you are installing a product. Sometimes it really sort of varies and you get there with a little bit of trial and error.

Mr. Stearns. But the point at which you get their attention is what you are saying.

Mr. Hintze. Yes, yes.

Mr. Stearns. Mr. Meyer.

Mr. Meyer. That is our business to figure this out, and the key thing I would add to the discussion is --

Mr. Stearns. Why, Mr. Meyer, don't you have privacy with a video, just a quick -- I never see anybody have a video for privacy.

Mr. Meyer. Some companies, some of our clients, do have videos in their privacy policy.

Mr. Stearns. Somebody would say do this, do that.

Mr. Meyer. Yeah, it all depends on the segment. It is very hard to know which type of user is showing up in which particular experience, and the key is to create a layered experience so that it can stand up to the scrutiny of, you know, privacy advocates and academics, and as

well as be simple enough for someone to get through it in a few clicks. And that is part of the reason we did this partnership with Akamai, to get the first layer as close to the point of engagement as possible, and then allow consumers who want more detailed information to dig through it, but not force them to read through a whole complex policy.

Mr. Stearns. Gotcha. Ms. Woolley.

Ms. Woolley. The goal that you mentioned is exactly the goal of the program, the advertising option icon program. It is in one or two clicks a simple explanation about what is going on, not --

Mr. Stearns. Have you thought about using video on it?

Ms. Woolley. -- a deep privacy policy, and also you can opt out.

Mr. Stearns. Instead of a narrative do you think a video would be better?

Ms. Woolley. There is not a video, but good idea. I mean, it is something we may try and do.

Mr. Stearns. Because you see, across these Web sites, the ones who are most successful have the videos instead of the narrative. Anyway, Professor?

Mr. Acquisti. Two solutions which need to complement each other; one is standardize the starting line of privacy policies, which are common in form across Web sites. This decreases the cognitive costs for the consumer. And the second, a baseline level of protection further through regulation.

Mr. Stearns. Would that come from that baseline from the Federal Trade Commission? Where would that baseline come from?

Mr. Acquisti. For instance, from the Federal Trade Commission.

Mr. Stearns. Oh, okay. Ms. Dixon?

Ms. Dixon. I agree with Professor Acquisti's remarks. I would just add one thing. We are talking about improving self-regulation of consumers. I think we ought to hear from the consumers, and the consumers ought to be part of that self-regulatory process and have a permanent and defined role in that process so they can give us direct feedback.

Mr. Stearns. Good. All right. Thank you, Madam Chair.

Mrs. Bono Mack. Thank you, Mr. Stearns. The chair is happy to recognize Dr. Cassidy for 5 minutes.

Dr. Cassidy. Mr. Hintze, okay, somebody -- you have a phone, right? You have a phone system? So Microsoft does. If I log on my phone, I register my phone, I pull it out of the box and I register it, it says hey, I am Bill Cassidy, I am da-da-da, and I also again have MSN. You spoke about this kind of firewall, if you will, between my Hotmail account and my MSN activities. But what if Apple or Google or Yahoo! or you -- I have a phone and either I have the phone which your company provides, or I am using the operating system that your company provides, or I am plugged into my browser on the phone; is that data correlated with my desktop browsing?

Mr. Hintze. No, and --

Dr. Cassidy. And do you speak just for Microsoft or do you speak for an industry standard?

Mr. Hintze. I am speaking for Microsoft. I am speaking for

Microsoft. Well, it depends. It depends on the scenario you are talking about. If you log in to your Hotmail account on a PC and then you log into your Hotmail account on your phone, it is the same account; that data is connected on the back end. The problem is there are many different scenarios we can go through.

If you are using a location-based service, where we as the operating service on the phone is providing this location service, that location data comes up without any identifying information. It comes up only so that it can send back location information so that an application can take advantage of that. And then on our back end, we don't store any unique IDs at all associated with the hardware or a user, and so, you know, it really depends on the scenario. In a logged-in scenario is the one scenario where, yes, there would be a linkage across the PC and --

Dr. Cassidy. Now, would this data be, could this data be or is this data, when it is connected, is it collated, correlated, da-da-da dated, in order to further target me in a more sophisticated fashion?

Mr. Hintze. We are just moving into mobile ads, and so in the future I think the answer will be yes. But, again, we would do that in a way that takes into account our own privacy standards, the standards that are being developed by the self-regulatory initiatives, et cetera. So yes, but people will have choices about that.

Dr. Cassidy. Okay. Ms. Dixon, what are your thoughts about that, because you seem to kind of come from the most sort of we-have-to-be-concerned perspective?

Ms. Dixon. Yeah, the tethered applications, mobile phones that are -- there is certain hard encoding that Mike could tell you more about, that links that phone directly to a person's identity in different ways than Web browsing does. So when we are talking about linking ads to phone technologies, I think that we are entering a new arena. The self-regulatory regime in place for that is a code of conduct by the Mobile Marketing Association, and the codes are profoundly general. They are so general it is unbelievable, and they are not protective at all. So a great deal of work would have to be done to reform this space or to regulate the space in order to provide baseline consumer protection.

Dr. Cassidy. Ms. Woolley, what are your thoughts about that? And, again, I am going to cut you off in a second because I have one more question for Mr. Hintze.

Ms. Woolley. Thanks. We are in the process of developing a program, building up a program where this icon will migrate to ads that are served on mobile devices. So a consumer will be able to not only see an ad on a mobile device, but he or she will be able to see the icon and opt out on that mobile device. And those choices, as we develop that program, expand that program to a mobile device, those choices must be honored by everybody in the chain of delivering that ad on a mobile device, the same way that the choices have to be honored.

Dr. Cassidy. So you agree with Ms. Dixon, but you feel as if that work, that hard work is being done, if you will?

Ms. Woolley. Absolutely.

Dr. Cassidy. Okay. Now, Mr. Hintze, in your testimony, reference 19 -- reference, I should say comments -- you say that even if responsible companies adopt strong practices and participate in self-regulatory initiatives, bad apples can spoil the whole bunch. Michael Jackson's redux. And government can play a role by setting baseline standards.

Now, that is a little bit less libertarian than I think some of the others on the panel. So you do see a role for government setting baseline standards. Mr. Stearns has legislation which, frankly, I haven't read, but he referenced it earlier. Have you read it, and if so -- if not, confess; but if so, what are your thoughts on it?

Mr. Hintze. We have read it and we have been on record for I think about 6 years now of supporting baseline Federal privacy legislation, that again it would be principles-based, not technologies-based. It would have to be flexible and incorporate safe harbors for effective self-regulatory initiatives. But there are a lot of things in Mr. Stearns' bill that we are supportive of, and we are, you know, happy to work with this committee and your office, Mr. Stearns, on that as well, going forward.

Dr. Cassidy. Okay. I am out of time. I yield back, and I thank you.

Mrs. Bono Mack. Thank the gentleman, and we would like to thank our panel very much for being with us today. You have been quite gracious with your time, and I look forward to working with all of you again as we get closer to making some important decisions about the

best ways to protect the online privacy of American consumers.

I thank Mr. Butterfield and all of the members and staff of this terrific subcommittee for their participation.

This was the fourth in our series of online privacy hearings so far this year. As the bits and bytes begin to add up, I think that we are getting closer and closer to understanding what the American consumers really want with respect to online privacy.

I remind members that they have 10 business days to submit statements and questions for the record and ask the witnesses to please respond promptly to any questions they receive.

[The information follows:]

******** COMMITTEE INSERT ********

Mrs. Bono Mack. The hearing is now adjourned.

[Whereupon, at 11:29 a.m., the subcommittee was adjourned.]