AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

UNDERSTANDING CONSUMER ATTITUDES ABOUT PRIVACY

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

OCTOBER 13, 2011

Serial No. 112–96

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

U.S. GOVERNMENT PRINTING OFFICE
74–605 PDF WASHINGTON : 2012

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

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
CLIFF STEARNS, Florida
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
Vice Chairman
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
CHARLES F. BASS, New Hampshire
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

MARY BONO MACK, California
Chairman

MARSHA BLACKBURN, Tennessee
Vice Chairman
CLIFF STEARNS, Florida
CHARLES F. BASS, New Hampshire
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

G.K. BUTTERFIELD, North Carolina
Ranking Member
CHARLES A. GONZALEZ, Texas
JIM MATHESON, Utah
JOHN D. DINGELL, Michigan
EDOLPHUS TOWNS, New York
BOBBY L. RUSH, Illinois
JANICE D. SCHAKOWSKY, Illinois
MIKE ROSS, Arkansas
HENRY A. WAXMAN, California *(ex officio)*

C O N T E N T S

	Page
Hon. Mary Bono Mack, a Representative in Congress from the State of California, opening statement	1
Prepared statement	4
Hon. G.K. Butterfield, a Representative in Congress from the State of North Carolina, opening statement	6
Hon. Marsha Blackburn, a Representative in Congress from the State of Tennessee, opening statement	7
Prepared statement	9
Hon. Joe Barton, a Representative in Congress from the State of Texas, opening statement	10
Prepared statement	11
Hon. Pete Olson, a Representative in Congress from the State of Texas, opening statement	13
Hon. Cliff Stearns, a Representative in Congress from the State of Florida, prepared statement	190
Hon. Henry A. Waxman, a Representative in Congress from the State of California, prepared statement	191
Hon. John D. Dingell, a Representative in Congress from the State of Michigan, prepared statement	196

WITNESSES

Barbara Lawler, Chief Privacy Officer, Intuit	14
Prepared statement	16
Answers to submitted questions	201
Mike Hintze, Associate General Counsel, Microsoft Corporation	30
Prepared statement	32
Answers to submitted questions	203
Scott Meyer, CEO, Evidon	56
Prepared statement	58
Answers to submitted questions	206
Linda Woolley, Executive Vice President, Washington Operations, Direct Marketing Association, on behalf of Digital Advertising Alliance	75
Prepared statement	77
Answers to submitted questions	209
Allessandro Acquisti, Associate Professor of Information Technology and Public Policy, Heinz College, Carnegie Mellon University	97
Prepared statement	99
Answers to submitted questions	214
Pam Dixon, Executive Director, World Privacy Forum	112
Prepared statement	114

SUBMITTED MATERIAL

Majority memorandum, dated October 13, 2011, submitted by Mrs. Bono Mack	197

UNDERSTANDING CONSUMER ATTITUDES ABOUT PRIVACY

THURSDAY, OCTOBER 13, 2011

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

The subcommittee met, pursuant to call, at 9:06 a.m., in room 2123, Rayburn House Office Building, Hon. Mary Bono Mack (chairman of the subcommittee) presiding.

Members 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, Senior 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.

OPENING STATEMENT OF HON. MARY BONO MACK, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

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 that 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.

[The prepared statement of Mrs. Bono Mack follows:]

Opening Statement of the Honorable Mary Bono Mack
Subcommittee on Commerce, Manufacturing, and Trade
"Understanding Consumer Attitudes About Privacy"
October 13, 2011
(As Prepared for Delivery)

When it comes to online privacy – at least for me – consumer attitudes and expectations are the bits and 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, then 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 long time, because it's the first time we have 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 hodge-podge of more than 300 state and federal laws. Likewise, there is no single regulator to enforce all of 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 websites, 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 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 the 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 a 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 that could otherwise use the content to collect information, while Mozilla's Firefox broadcasts a signal to each website 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 website that receives the signal from the consumer's browser must choose to honor the request, and currently there is no requirement that websites 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's 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's doing enough to protect American consumers, while government, unfortunately, tends to overreach whenever it comes to new regulations.

That's why I'm so anxious today to hit the "refresh key" to learn the latest about consumer attitudes and expectations.

###

OPENING STATEMENT OF HON. G.K. BUTTERFIELD, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA

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 OK 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 OK to base tailored 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 that allow 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.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

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.

[The prepared statement of Mrs. Blackburn follows:]

Rep. Blackburn's Opening Statement for CMT Subcommittee Hearing on Consumers' Online Privacy Expectations

Today we're talking about government regulating the use of data.

Electronic data is a natural resource. The DNA of data is powerful – it's the lifeblood of our thriving Internet economy.

Should we allow our free-market to explore this natural resource, learn to commercialize it, protect it and respect it? Or will we restrict it all together?

Why should government be the decision-maker? Government knows so little, reacts to slowly and works so poorly.

Economist F. A. Hayek once said, "The curious task of economics is to demonstrate to men how little they really know about what they imagine they can design." His wisdom is especially relevant to this discussion.

We don't know what consumer's true expectations are about online privacy. Consumers are different and expectations aren't static. And innovation moves 500 times faster than the detached delusions that dominate the executive agencies.

We don't need government to pretend it has all the answers.

Our thriving tech and advertising industries are infinitely more responsive and better equipped to meet consumer demands than the federal government. The last thing we need is another "federal, one-size-fits-all" approach to an issue that affects such a huge part of our economy.

Congress must be flexible. Encourage beneficial uses of data. Protect against real harms. Empower people instead of government.

I look forward to your testimony and thank the chair for yielding.

OPENING STATEMENT OF HON. JOE BARTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE 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.

[The prepared statement of Mr. Barton follows:]

Opening Statement of the Honorable Joe Barton
Chairman Emeritus, Committee on Energy and Commerce
Subcommittee on Consumer, Manufacturing, and Trade
"Understanding Consumer Attitudes about Privacy"
October 13, 2011

The Third Amendment of the Constitution reads, " 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." This clearly protects the privacy of American citizens and explicitly calls for consent of the Owner. While the Founding Fathers were not talking about the internet specifically, I believe that they would have applied the same principle to the internet world.

I was recently informed by my staff that Amazon has created a new browser that would use its own servers to provide faster internet to their users. This would allow Amazon to collect data on all online activity of their users, and I believe that this is completely out of line. It seems like every day I hear of something new from some company who is trying to find more ways to track its users. Enough is enough.

In the United States, there were 124 million people on the internet in the year 2000 compared to over 240 million who use the internet today [1]. Because our country has roughly 300 million citizens, this means that over 70 percent of Americans are using the internet.

---

[1] See http://www.internetworldstats.com/am/us.htm

With this in mind, more and more companies are conducting business online and now more Americans are indeed giving their home phone numbers, home addresses, credit card numbers, and even social security numbers to numerous internet vendors. In some cases, companies mandate that this information be given electronically otherwise a consumer's quality of service is decreased.

I believe what businesses fail to consider when creating new mechanisms to offer more efficient services, is the monumental risks that come along with handling, managing, and protecting consumer data. When personally identifiable information gets into the wrong hands, it is the consumer, not the company, that suffers the harm.

As Co-Chair of the Bipartisan Privacy Caucus, I am committed to protecting current and future Americans from online abusers. While not every website operator is a bad actor, there are many out there that are. I believe that it is time for Congress to pass a law that safeguards every American's right to have control over their personal information.

OPENING STATEMENT OF HON. PETE OLSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE 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, ON BEHALF OF DIGITAL ADVERTISING ALLIANCE; 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:]

Testimony of

Barbara Lawler
Chief Privacy Officer
Intuit

Before the Subcommittee on Commerce,
Manufacturing, and Trade
House of Representatives
Understanding Consumer Attitudes About Privacy

Thursday, October 13, 2011
9:00 AM
2123 Rayburn House
Office Building

Good morning and thank you Chairwoman Bono Mack, Ranking Member Butterfield and members of the Committee for providing Intuit the opportunity to be here today. We applaud the Committee's interest in online privacy issues, and in particular the focus on consumers' expectations about their online privacy.

Intuit is in a unique position to comment on this subject. Today, over 50 million customers entrust Intuit with their most personal financial information. As more and more of Intuit's products and services are accessed online, understanding our customers' expectations regarding their online privacy and earning their trust has been a major priority at Intuit.

At Intuit, customers are at the heart of everything we do. We were founded on the idea of customer-driven innovation, a mindset and methodology to uncover consumers' important, unsolved problems and then develop innovative products and services that meet and surpass those needs. Many companies talk about customer focus, but the level of commitment to understanding our customers' point of view, and the rigor we put behind it, differentiates us.

Towards that end, Intuit recently undertook comprehensive research that examined our customers' expectations about privacy, including data security and the use of their own specific data. Through the research, our customers explicitly told us that they expect us to be ethical stewards of their data, using it responsibly and with integrity, for their benefit, while keeping it safe and secure.

The research clearly demonstrated the high value our customers place on responsible use of their data. More so, the findings were a central element in the development of Intuit's Data Stewardship Principles, a framework that clearly communicates to our consumers exactly what we will and will not do with their data. Our Data Stewardship principles are included below. To, us, they represent our commitment to be an Accountable organization, to our customers, the public, and to the government. Our Principles align with the "elements of Accountability" framework.

We welcome the opportunity to share some of our insights from that research with you today.

About Intuit:

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

We started small with Quicken personal finance software, which simplified the common household dilemma of balancing the family checkbook. Today, we are one of the nation's leading providers of tax, financial management and online banking solutions for consumers and small businesses, and the accountants, financial institutions and healthcare providers that serve them. We employ nearly 8,000 people, our revenues

top 3.5 billion and we're recognized by Fortune Magazine as one of America's most-admired software companies and one of the country's best places to work.

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

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

Privacy is not a new issue to us at Intuit. We've been committed to continually innovating and implementing the safest and most responsible ways to work with consumers' intimate financial information for nearly 30 years, and we have a dedicated team of privacy professionals with over 70 years of combined experience.

Experience has taught us that consumer trust is a key component of customer satisfaction and long term growth. Without earning and keeping that trust, our customers will not continue to use our products and services. Trust that Intuit handles vital personal information in an ethical and responsible fashion is a founding element of Intuit's relationship with its customers.

As technology products and services transition to online, always-available, connected services, including Intuit's offerings, we believe the same values of trust and transparency will spur continued growth of the U.S. and global economy. We do not

view privacy and security as an exercise in compliance, but as a key part of the value we deliver to customers. Our customers see it that way too.

Intuit's Research Initiative:

As our business evolves and we continue to innovate with online connected products and services, often referred to as 'cloud services', more and more of our customers entrust Intuit to hold their most sensitive data for them. In order for us to provide our customers with the sense of trust that they have come to expect from Intuit, it was important for us to clearly understand our customers' feelings and attitudes about how their data is used, especially in a cloud-based services environment.

Intuit developed Data Stewardship Principles in order to provide customers and the general marketplace with a clear and simple framework to understand how we safeguard and manage customers' data.

To help us develop our Data Stewardship framework and ensure that it addressed the priorities of our customers, Intuit recently undertook an intensive research initiative that sought to understand consumer attitudes towards privacy and the use of their data.

Intuit's research was conducted in late 2010 and early 2011. It was both qualitative and quantitative, employing in depth interviews as well as broad surveys. Intuit conducted two rounds of quantitative, statistically valid surveys that cut across our multiple customer bases and product lines to get feedback and learn what mattered most to our customers; about 2000 for each cycle of research. We also conducted multiple rounds of qualitative customer focus group and one-on-one sessions in order to dive deeper into customer feelings regarding transparency, choice, data use cases and security.

This research is unique. To our knowledge, Intuit is one of the few private-sector companies to invest in a broad and in-depth study that asked its customers about their perceptions regarding privacy and the use of their data.

The findings from this research were instrumental in helping shape Intuit's Data Stewardship Principles. Through the research, we discussed, iterated and reviewed the evolving Data Stewardship principles with our customers in order to make sure we understood their priorities and developed a final set of Principles that were clear, concise and meaningful to them.

Data Stewardship Principles

What we stand for:

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

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

We will not:

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

We will:

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

Intuit Proprietary & Confidential

intuit

The central concept of Data Stewardship is that it is the customer's data, not ours. The Principles assure our customers that Intuit will not sell, publish, or share data entrusted to us that identifies the customer or any person without explicit permission. Data

Stewardship also provides our customers tools to understand how their data is being used and empowers them with choices to control the use of their specific data.

Data Stewardship is designed to enable Intuit to continue to innovate and grow by reinforcing the trust our customers have in us, through ensuring transparency and providing clear choices about the use of their data. The Principles are written clearly to state that we will use our customers' data to help them save time and money.

The research we conducted strongly informed Data Stewardship and provided Intuit with three key insights that I would like to share with you today:

- One: Customers care deeply about how their data is used.

- Two: Customers want clear explanations and relevant choices about the use of their data when it is contextually relevant to them.

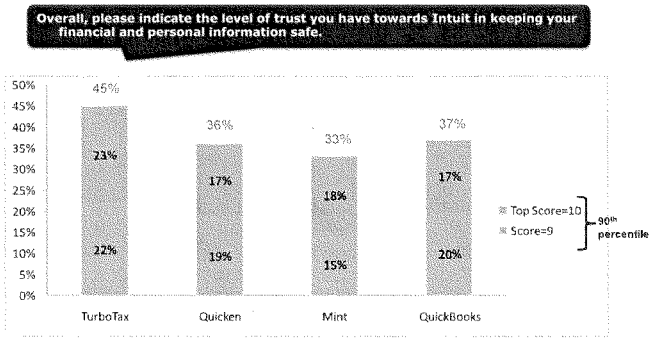
- Three: Customers welcome and want data-driven innovation when the benefits to them are clear.

Data Privacy Matters:

What came across loud and clear in the research was that people care deeply about privacy and how their data is used. As more and more of our lives are conducted online, personal privacy is an increasingly important issue for consumers in the here and now.

As they participated in the quantitative research, customers indicated their initial trust level in Intuit.

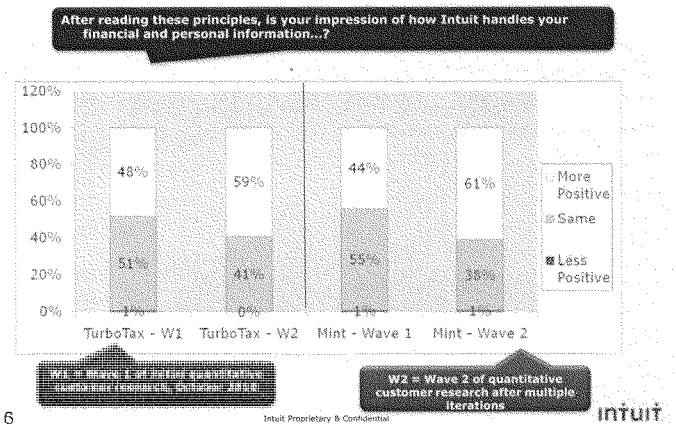
Baseline: Overall Level of Trust
(Before Exposure to Data Stewardship Principles)



5 Intuit Proprietary & Confidential intuit

Nearly sixty percent (60%) of our customers said they felt more positive about Intuit after they read our proposed Data Stewardship Principles that outlined Intuit's ethical use of their data. This is a striking number – and speaks to the importance people place on how their personal data is used, and that clear, simply-stated Principles enhance trust and confidence. One customer stated, *"As a leader in the industry, this statement only reinforces the high regard in which I hold the company."*

Impression of Intuit
(After Exposure to Data Stewardship Principles)



The importance customers place on data privacy should not be confused because of a lack of engagement in reading privacy statements. Our research showed that even though people are very invested in the use of their data, many customers feel overwhelmed by the fine print of lengthy privacy statements used today and do not feel empowered to have much control over how their personal data is used. In reviewing the Principles, customers commented that they liked them because they are, *"clear, concise and focus on top concerns"* and valued their *"brevity, directness, and assurance."*

Throughout our qualitative research – both focus groups and individual interviews – it became clear that although people do not always read a company's privacy policy or notice, they do care deeply about their data and how it is used. This sentiment was echoed in the written statements and comments provided by people participating in the quantitative studies as well. Customers often made strong, evocative statements about the Principles, such as *"A little safer in an unsafe world"* and *"Because of these principles, I will continue to use their products"*.

The research also showed that customers' number one concern in regards to online privacy is the potential loss of control over their data. When asked to rank Intuit's Data Stewardship principles, 85 percent of customers ranked the principle of Intuit NOT selling their personal data without their explicit permission as the most important principle.

It was abundantly clear to us from the research that our customers felt very strongly about how their data was handled, used and safeguarded. Evolving our privacy framework to a Data Stewardship approach that addressed this core concern while maintaining trust was vital to continuing Intuit's longstanding, trust-based relationship with its customers.

Relevant Choices.

The research also demonstrated that customers want clear and relevant, context-based choices that educate and empower them in regards to controlling the use of data specific to them.

Many customers told us that they often got lost in the fine print and felt overwhelmed by the dense language being used in many privacy policies. They felt that unrestrained use of their personal data was the default setting for most agreements and that they had to swim upstream in order to control their own data.

Instead of long, detailed privacy notices, what customers said they wanted were simple, easy-to-read explanations of how their data would be used. The more words they saw on a page, the more confidence appeared to diminish among our customers. They also wanted to have user-friendly choices about uses that would be specific to them. In other words, less is more.

They also wanted these choices to be presented in context, when the choice was relevant and they could clearly understand the benefit being offered to them based on the use of their data. They did not want to have to go look for their choices somewhere else, such as in a longer privacy statement or a license agreement. When choice is presented in a relevant context, and coupled with a simple explanation, we found that most customers felt empowered to make a choice, and many wanted and welcomed the use of the data.

And they want the choices they make to matter. While they were very receptive to Data Stewardship, customers also expect us to follow through with these Principles and ensure they are not just empty phrases. Customers want proof and not just promises from companies. As part of this research, customers were given the opportunity to provide feedback on several potential data use cases. First and foremost, they want proof that their data will be used to benefit them.

Moving forward, we believe Data Stewardship Principles must be implemented and communicated clearly and consistently across appropriate consumer interactions to become meaningful. We continually strive to introduce new ways to prove our accountability to our customers. Because consumers expect us to be accountable for the promises we make to them, Intuit continues to research the best means to provide data use-related information to our customers in a timely and relevant manner.

Customers also expect us to educate our employees about proper privacy and data security. Nearly 80 percent of our customers said that it was important that employees be trained in how to responsibly handle their data. At Intuit privacy and security training are required for all employees. Additionally, they expressed appreciation that we provide educational resources to customers so they can learn how to safeguard their data, which can be found at security.intuit.com.

In summary, customers want the principles of Data Stewardship to be meaningful and real. In other words, they want to shift the balance of the data privacy relationship with companies as they currently perceive it. Instead of consumers feeling that it is their responsibility to weed through the fine print of privacy statements, they want the private sector to work with them by articulating clear policies and practices, offering relevant choices, and following through on clearly stated data privacy principles.

Demonstrating the Benefits of Data-Driven Innovation:

Our research also demonstrated that consumer confidence increases when consumers clearly see how their personal data can be used to benefit them.

During the research project, some customers stated their belief that if they allow their data to be used by companies, it will not benefit them. They believe that 'data use' meant their data would be sold, leading to an increase in unwanted marketing, predatory data mining schemes, and unwanted spam. They believe their data will be used against them and not for them.

However, when the potential benefits of data-driven innovation were clearly outlined to customers, their attitude towards use of their data changed. Consumers are extremely open to the responsible use of their data if it provides them with direct and tangible benefits.

At Intuit, we have begun to demonstrate to customers how our customer-driven approach to innovation can unleash the power of the customer's own data, and empower consumers and small businesses to have new insights and make decisions that improve their financial lives. For example, Intuit has recently developed capabilities for small business owners to compare themselves along key business metrics to other businesses similar to them in the same geography. Imagine if your local florist could

compare his regular spending trends (on potsoil, marketing, or delivery trucks) with those of other florists in his region of the country? We have also developed a service that helps to identify savings on items commonly purchased by small business owners. Both of these services involve the use of the customer's own data in a way that brings meaningful value to them.

Data-driven innovations, at their best, can empower 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.

Our research also shows that we, as an industry, must do better in articulating and demonstrating the benefits that data-driven innovation can provide to customers. If we develop clear, principles-based data frameworks, simply described, and demonstrate the real-world benefits for consumers – we will generate trust, fuel economic growth, and deliver astounding new benefits and services to customers.

Conclusion:

As we move forward toward a connected-services, cloud-based economy, Intuit believes it is vital that we develop clear and practical privacy frameworks that answer the concerns and expectations of consumers. *"Customer focused, protecting my data and interests, holding themselves accountable,"* are the core elements that mean the most to customers. So, Data Stewardship represents our ongoing commitment to be an Accountable organization, and the Principles align with the "elements of Accountability" framework.

At Intuit, we used the insights from our recent research as a key element in developing our Data Stewardship Principles. We took our customers along with us on the journey to define our principles about the use of data in order to generate a set of principles

that reflects their needs, values and concerns. One customer observed, *"I'm happy that Intuit cares enough about privacy issues to seek customer feedback."*

Intuit's Data Stewardship Principles express how we think about data and offer clear guardrails to guide our judgment. Data Stewardship is derived directly from Intuit's core operating values – especially Integrity Without Compromise – and is intended to guide our mindset and behavior in all we do. It reflects and reinforces that we are an organization that is accountable for our actions, and for the responsible use of customer data entrusted to us.

Data Stewardship supports Intuit's growth strategies and also meets our customers' expectations about being transparent in how Intuit uses their data to deliver better products, services and features to serve them.

The business world is quickly shifting to one where the center of gravity is now centered on the cloud and connected software, platforms and services. Innovative data use lies at the heart of many new products and services for customers.

As we enter this new environment, we believe a key aspect for fueling economic growth will be understanding and respecting the expectations of consumers in regard to data privacy. At Intuit, we believe one of the key drivers for future business success will come from maintaining and earning the trust of consumers.

Once again Madame Chairwoman, Representative Butterfield and members of the Committee, thank you for giving Intuit the opportunity to share some of our insights from our recent research initiative.

Only by learning directly from consumers what they really want and what is important to them, will we be able to develop the clear and practical data frameworks needed for

the 21st century. We all must work towards the shared goal of protecting consumers while maintaining data-driven innovation that improves consumers' lives in trusted, real and fundamental ways.

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

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:]

MIKE HINTZE
ASSOCIATE GENERAL COUNSEL
MICROSOFT CORPORATION

SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE
COMMITTEE ON ENERGY & COMMERCE
U.S. HOUSE OF REPRESENTATIVES

SUMMARY OF TESTIMONY
HEARING ON "UNDERSTANDING CONSUMER ATTITUDES ABOUT PRIVACY"
OCTOBER 13, 2011

Microsoft engages with consumers in multiple contexts — as a website publisher, an operator of an ad network, a provider of cloud computing and other online services, and as a developer of PC and mobile operating systems, a leading web browser and other software applications — and therefore offers a unique perspective on the privacy discussion.

There is no single, "silver bullet" solution to privacy, principally because privacy means different things to different consumers; depends on the context in which data is collected and used; and is subject to a rapid pace of change in technology. Consumer sensitivities and expectations regarding privacy therefore are evolving constantly.

This necessitates a multi-factored approach to addressing consumer privacy that includes: (1) company best practices, such as privacy by design, transparency, and security; (2) technology tools, such as the browser-based "Do Not Track" mechanism that we incorporated into Internet Explorer 9 to allow consumers to make informed privacy choices for themselves; (3) industry self-regulation, such as the Self-Regulatory Program for Online Behavioral Advertising, which employs a universally-recognizable "Advertising Option" icon that consumers can access to learn about and opt out of online ads; and (4) consumer education, which equips consumers to make choices that align to their own privacy needs and helps protect them from harm.

In Microsoft's experience, consumers are using the privacy tools and information we make available to make informed privacy choices for themselves. For example:

- Over the past five months, key privacy websites offered by just one division of our company averaged over two million sessions per month.
- In an average month, more than 435,000 consumers access our "Advertisement Choice" webpage, which is the website that explains how a user can opt-out of personalized online advertisements and provides information about how and why

such advertisements are delivered. Approximately 20 percent of those consumers perform some action while visiting that web page, in most cases opting out of personalized ads.

- In an average month, approximately 16,000 U.S. consumers visit their Personal Data Dashboards, which provide a centralized location for consumers to view and manage their online information. In August 2011 alone, these visits increased to more than 22,000.

STATEMENT OF MIKE HINTZE
ASSOCIATE GENERAL COUNSEL
MICROSOFT CORPORATION

BEFORE THE
SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE
COMMITTEE ON ENERGY & COMMERCE
U.S. HOUSE OF REPRESENTATIVES

HEARING ON "UNDERSTANDING CONSUMER ATTITUDES ABOUT PRIVACY"

OCTOBER 13, 2011

Chairman Bono Mack, Ranking Member Butterfield, and honorable members of the Committee, my name is Mike Hintze, and I am an Associate General Counsel of Microsoft Corporation. Thank you for the opportunity to share Microsoft's perspective on the important issue of consumer privacy. We appreciate the leadership that the Subcommittee has shown on privacy issues, and we are committed to working collaboratively with you, the Federal Trade Commission ("FTC"), the Department of Commerce, consumer groups, and other stakeholders on ways to protect consumer privacy while promoting innovation. The multiple contexts in which we engage with consumers gives us a unique perspective on the privacy discussion. As a website publisher, an operator of an ad network, a provider of cloud computing and other online services, and as a developer of PC and mobile operating systems, a leading web browser and other software applications, Microsoft has a deep understanding of the roles that different participants play in the digital ecosystem and in safeguarding consumer privacy.

Microsoft embraces a commitment to consumer privacy because we recognize that consumer trust is critical to the adoption of online and cloud computing services that Microsoft and others in our industry offer. 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, choices about the collection and use of that data, and confidence that their data is secure. As I will describe in greater detail in my remarks, these three principles — transparency, control, and security — underpin Microsoft's approach to privacy. They are essential components of the privacy frameworks advanced by the FTC and the Department of Commerce, and we believe they represent what users have come to expect from their online experience.[1]

---

[1] *See generally* Fed. Trade Comm'n, Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010) ("FTC Staff Report"); Internet Policy Task Force, Dep't of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 16, 2010).

In our experience, there is no single, "silver bullet" solution to privacy. There are several reasons for this conclusion. First, privacy means different things to different consumers, and research has shown that there is a wide range of privacy sensitivities among individuals.[2] Second, we believe that consumers often have different privacy expectations depending on the context in which their data is collected and used; for example, their expectations can differ when they interact with retailers, social media platforms, online games, search engines, or Internet service providers. To meet these differing needs and expectations, Microsoft strives to offer meaningful privacy choices in its service offerings, recognizing that informed consumers will make personal privacy choices and adopt a wide range of privacy preferences.

The challenges of crafting effective privacy solutions also are rendered complex by the rapid pace of change in technology, business models, and consumer adoption rates for online services. Within this rapidly evolving environment, user sensitivities and expectations regarding privacy also can evolve over time in particular contexts. Not too long ago, few consumers were sharing their personal photographs and home videos publicly; today, consumers regularly post these and other materials on social networking and online video websites without hesitation because they find value in these services.

---

[2] For instance, Alan Westin, a well-known privacy researcher, has concluded that individuals can be segmented into three separate groups based on their attitudes toward privacy: privacy fundamentalists, privacy pragmatists, and privacy unconcerned. *See What Consumers Have To Say About Information Privacy: Hearing before the House Subcommittee on Commerce, Trade, and Consumer Protection*, 107th Cong. 15-16 (2001) (testimony of Alan K. Westin, Professor Emeritus, Columbia University). According to Professor Westin, at one end of the spectrum, some consumers are privacy fundamentalists, meaning they are "intensely concerned about privacy" and "generally will reject benefits offered to them by a business." At the other end of the spectrum are consumers that are "privacy unconcerned," who "[don't] know what the 'privacy fuss' is all about" and "[have] little problem with supplying their personal information to government authorities or businesses." *Id.* The majority of consumers fall into the "privacy pragmatist" category; they "weigh[] the value to them and society of various business or government programs calling for personal information, examines the relevance and social propriety of the information sought, look[] to see whether fair information practices are being widely enough observed, and then decide[] whether they will agree or disagree with specific information activities." *Id.*

These challenges necessitate a multi-factored approach to addressing consumer expectations about privacy that includes (1) company best practices, (2) technology tools, (3) rules of the road established through both industry self-regulation and legislation, and (4) consumer education. Today, I will describe the steps Microsoft has taken and continues to take to protect privacy and advance these objectives. These steps demonstrate Microsoft's deep commitment to privacy, particularly in its own product design, and highlight the important role that company best practices and technology play in addressing consumer privacy and meeting consumer expectations. They also help highlight the importance of fostering an environment that will lead to appropriate privacy protections without impeding innovation. It is important to acknowledge at the outset, however, that no one company alone can fulfill all of these objectives. Addressing consumer privacy expectations often requires the collaborative effort of individual companies, industry groups, consumer and privacy advocates, government, and consumers themselves.

I. Microsoft's Commitment to Privacy in Product Design and Business Practices

Individual companies play an important role in protecting consumer privacy. At Microsoft, we have a deep and long-standing commitment to our privacy by design approach. It defines not only how we build products, but also how we design and operate our services and how we conduct our business. Microsoft was one of the first companies to appoint a chief privacy officer, an action we took over a decade ago, and we currently employ over 40 employees who focus on privacy full time and another 400 employees who focus on privacy as part of their jobs. In addition, we have adopted robust policies and standards to ensure that we do business and design our products and services in a way that respects and protects consumer privacy. For years, we have built privacy standards and checkpoints into our product development processes. Doing so helps us ensure that we engineer privacy into our products and online services at the earliest stages of their development and foster the continued consideration of privacy throughout the product lifecycle, including after the release of the product or

service into the market. We have continued to refine and develop these standards and processes over time. We have even made some of these standards available publicly to help others in the online industry adopt high standards for privacy.[3]

Microsoft also has been a leader and innovator in increased transparency by, for example, developing and being one of the first companies to adopt "layered" privacy notices. The Microsoft Online Privacy Statement provides consumers with the most important information about our privacy practices in a concise, one-page upfront summary with links to additional layers that describe in more detail our data collection and use practices.[4] We also provide information about our privacy practices and access to user controls on dedicated web pages and know that consumers are viewing this information. For example, over the past five months, key privacy websites offered by just one division of our company averaged over two million sessions per month.[5]

Microsoft's online advertising business provides illustrative examples of how we also provide consumers with meaningful choices about how their information is used. Several years ago, Microsoft decided to address a weakness inherent in offering consumers the ability to "opt out" of behavioral advertising solely via an "opt-out cookie." At the time, opt-out choices not only were wiped

---

[3] For example, Microsoft's Privacy Guidelines for Developing Software Products and Services, which are based on our internal privacy standards, are posted publicly at http://www.microsoft.com/privacy. We make these standards publicly available for other organizations to use to develop and guide their own product development processes. And our privacy guidelines are recognized by the International Association of Privacy Professional's privacy certification program – the Certified Information Privacy Professional for IT (CIPP/IT). *See* https://www.privacyassociation.org/images/uploads/CIPP_IT_Reading_List_0909.pdf.

[4] *See* http://privacy.microsoft.com/en-us/default.mspx.

[5] These key privacy websites include choice.live.com, where consumers can learn more about the online advertising process, opt out of personalized ads, and access their personal data dashboard (provided at Appendix 1); the "Advertisement Choice" website, which contains information about personalized advertising and provides an opt out option (provided at Appendix 2); and the Personal Data Dashboard website, which provides access to all of these key privacy controls in a centralized location (provided at Appendix 3). In August 2011, traffic to these privacy websites totaled 2,405,702 sessions, or approximately 1 million distinct users.

clean each time a user deleted the cookies for his or her machine,[6] but the opt-out cookies also were computer specific. To address these limitations, Microsoft began offering users the ability to tie their opt-out choices to their Windows Live ID — the credentialing protocol that consumers use to sign in to our online services. As a consequence, if a user today deletes the cookies on his or her machine, when the user signs back in with his or her Windows Live ID, that opt-out selection will persist. It also means that a user's opt-out choices can apply across multiple computers (*e.g.*, home and work computers) when the user signs in on them.

As an alternative to opting out, we also allow users to influence the ads they see by signing in through their Windows Live ID and selecting their interests. This means that users will be more likely to see ads over time that reflect their own preferences. In an average month, more than 435,000 consumers access our "Advertisement Choice" webpage, which is the website that explains how a user can opt out of personalized online advertisements and provides information about how and why such advertisements are delivered.[7] Approximately 20 percent of users that access this web page (and similar Microsoft web pages) perform some action while visiting them, in most cases opting out of personalized ads. In an average month, approximately 16,000 U.S. consumers also visit their Personal Data Dashboards, which is a new feature that we have developed to provide a centralized location for consumers to view and manage their online information. In August 2011 alone, these visits increased to more than 22,000. These company-specific efforts are, of course, in addition to the joint efforts we have undertaken with other stakeholders in the online advertising industry, which I describe in greater detail below.

---

[6] Relying solely on a cookie to store the opt-out choice was in tension with the common advice to consumers that one way to help protect privacy was to periodically clear their cookies. The result was that when a consumer cleared his or her cookies, the opt-out choice also would disappear.

[7] *See* http://choice.live.com/Default.aspx.

In short, by building transparency, choice, and security into its products from the earliest stages of design, Microsoft fosters consumer trust in its products and in the online environment and empowers users to control their personal information and make appropriate privacy choices for themselves.

II. Microsoft's Development of Technology Tools

As a technology company, we naturally believe that technology has a key role to play in protecting privacy, particularly with respect to providing consumers with a variety of choices and tools to help put them in control as they interact with sites and services across the Internet. In our capacity as a browser vendor, for example, Microsoft has developed and supported a number of innovative tools that give consumers greater control over the collection and use of information about their online actions. For example, with Internet Explorer 8, we introduced InPrivate Browsing, a feature that prevents a consumer's browsing history, temporary Internet files, form data, cookies, and usernames and passwords from being retained by the browser after the consumer closes the InPrivate Browsing window.[8] This helps consumers keep their browsing history private on shared computers such as at home, in an Internet café, or at a public kiosk. Another feature introduced in Internet Explorer 8, InPrivate Filtering, analyzes third-party content and provides users with options to block third-party content providers from collecting information about users' browsing activities.[9]

Microsoft also was the first of the major browser manufacturers to respond to the FTC's recent call for a persistent, browser-based "Do Not Track" mechanism.[10] Specifically, Internet Explorer 9 offers an innovative new feature, "Tracking Protection," that allows consumers to decide which third-party sites can receive their data and filters content from third-party sites identified as potential privacy threats. When a consumer visits a website, his or her computer automatically shares information with

[8] *See* http://windows.microsoft.com/en-US/windows-vista/What-is-InPrivate-Browsing.

[9] *See* http://windows.microsoft.com/en-US/Windows7/InPrivate-frequently-asked-questions.

[10] *See* FTC Staff Report at 66.

that website, such as cookies, IP address, and other standard computer information. If the website contains content provided by a third-party website (for example, a map, advertisement, or any web measurement tools, such as a web beacon or scripts), some information about the consumer may be sent automatically to the third-party content provider.[11] Users who activate the Tracking Protection feature can create or download Tracking Protection Lists that identify third-party websites or content that are, in the view of the list creator, trustworthy or untrustworthy.[12] If a third party site is listed as a "do not track" site on a Tracking Protection List, Internet Explorer 9 will block the websites a consumer visits from making "calls" to that third party site.[13] By limiting calls to third-party websites, Internet Explorer 9 blocks these third-party sites from collecting information from users – without relying on these third-party sites to read, interpret, and honor a do-not-track signal.[14]

The Tracking Protection feature is highly customizable and can be adapted to specific user preferences because anyone on the Web (including consumer groups and privacy advocates and security firms) can create and publish Tracking Protection Lists – they simply are files that can be uploaded to a website and made available to others via a link. Consumers can create or subscribe to a list or lists as they see fit.

III. Microsoft's Support for Baseline Rules of the Road

In addition to company-specific efforts, Microsoft believes that there is need for baseline rules of the road. These rules may best be established by a combination of federal privacy

---

[11] This type of arrangement can have several benefits. For example, it enables consumers to access third-party content conveniently, and the presence of advertising may make it possible for the website to provide access to premium content at no charge. There can, however, be an impact to consumer privacy as a result because it is possible for the content providers to track individual consumers across multiple websites.

[12] *See* http://www.iegallery.com/en/trackingprotectionlists/.

[13] Information can be sent to a site listed as "do not track" on a Tracking Protection list if the user chooses to visit that site directly by clicking on a link or typing its web address.

[14] As an additional measure, if the user has installed a Tracking Protection List, Internet Explorer 9 will send a do-not-track signal or preference to all the websites the user visits.

legislation that establishes baseline principles (discussed below) and industry self-regulation that would build on those basic principles to create effective privacy protections that take into account consumers' reasonable expectations of privacy in different contexts. Industry self-regulation can and should establish minimum standards and best practices across an industry, and foster industry-wide privacy solutions. As I mentioned at the outset, consumers can have different privacy expectations depending on whether they are interacting with retailers, application developers, social media platforms, online games, search engines, Internet service providers, publishers, advertisers, or ad networks, and industry self-regulation can offer flexible tools for addressing privacy issues in these many different contexts. In addition, self-regulatory efforts are generally better able than prescriptive legislation to keep pace with evolving technologies and business models.

Microsoft has a history of working collaboratively with other companies to develop and support appropriate solutions that build on the principles of transparency, control, and security. For example, Microsoft is a strong supporter of, and is implementing, the Self-Regulatory Program for Online Behavioral Advertising, which includes the prominent display of text or a universally-recognizable "Advertising Option" icon in or next to online ads.[15] By clicking on the text or icon, consumers can easily access and learn about online behavioral advertising and the privacy practices associated with online advertising, and, with a single click, consumers can choose to opt out of receiving tailored advertising from all participating companies, if they choose. This program, which facilitates both transparency and consumer choice, also includes an educational website where consumers can learn about online advertising and choose not to have their information used for behavioral advertising.[16]

Data security also is among the focal points of the Self-Regulatory Program for Online Behavioral Advertising: participating organizations must agree to provide appropriate security for, and

---

[15] *See* http://www.aboutads.info/.

[16] *See id.*; *see also* http://www.aboutads.info/consumers/.

limit their retention of, data collected and used for behavioral advertising. In our multiple roles as a browser manufacturer, ad network, and website operator, for example, we are coordinating with the Interactive Advertising Bureau and other participants in the Self-Regulatory Program to ensure that this important initiative is effective, enforceable, and broadly accepted. Consistent with our commitment to responsible industry leadership, we also are working at the World Wide Web Consortium, the standards-setting body for the Web, to develop an industry consensus about technical standards that can be implemented across browsers to enable common tools for consumers to control tracking by third parties.[17] As a result of these self-regulatory initiatives, we believe that the online advertising industry is taking important and effective steps toward improving consumer privacy.

While the efforts of individual companies and industry self-regulatory initiatives play key roles in protecting consumer privacy, baseline federal privacy legislation could serve as an effective complement to industry efforts. The current sectoral approach to privacy regulation makes compliance a complex and costly task for many organizations. According to one estimate, by 2009 there were more than 300 federal and state laws relating to privacy.[18] The sector-specific approach also creates confusion among consumers and can result in gaps in the law for emerging sectors or business models. By contrast, baseline privacy protections that apply across sectors could provide more consistent protections for consumers and simplify compliance for businesses that increasingly operate across those sectors. Baseline privacy protections also could promote accountability by ensuring that all businesses use, store, and share commercial data in responsible ways, while still encouraging companies to

[17] *See* http://www.w3.org/2011/tracking-protection/charter-draft.html.

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

compete on the basis of more robust privacy practices.[19] In addition, baseline federal privacy legislation could foster greater legal certainty by preempting state laws that are inconsistent with federal policy.[20]

If Congress pursues legislation, however, it should be crafted carefully and with two goals in mind. First, it must protect consumers' privacy and data security while enabling innovation and facilitating the productivity and cost-efficiency that new business models and computing paradigms offer. Second, it should create privacy protections that can withstand the rapid pace of technological change so that consumer data is protected not only today, but also in the decades to come. To achieve these two ends, any proposed legislation should be tested against certain fundamental criteria, among them:

- Flexibility. Legislation should permit businesses to adapt their policies and practices to match the contexts in which consumer data is used and shared and be sufficiently flexible to allow technological innovation to flourish. Instead of imposing prescriptive rules, the legislation should establish baseline principles, then permit businesses to adopt methods and practices to achieve those principles in a manner that best serves their business models, technologies, and the demands of their customers.

- Certainty. Legislation should provide businesses with certainty about whether their privacy policies and practices comply with legal requirements. Government-recognized safe harbor programs are one way in which the framework can remain flexible but also provide businesses the certainty necessary to encourage the development of innovative privacy protections and new products and services.

- Simplified Data Flow Standards. Legislation should seek to facilitate the interstate and international data flows that are necessary to enable more efficient, reliable, and secure delivery of services, including through harmonizing international privacy regimes and preempting a patchwork of state privacy laws.

- Technology neutrality. Legislation should avoid preferences for particular services, solutions, or mechanisms to provide notice, obtain choice, or protect consumer data.

---

[19] Even if responsible companies adopt strong practices and participate in self-regulatory initiatives, one bad apple could potentially spoil the whole bunch and undermine trust in online commerce and cloud computing generally. That is where government can play a key role by setting baseline standards and taking enforcement action against bad actors who do not take privacy seriously. Government-recognized safe harbor programs are another way the government can play a critical enforcement role, yet at the same time preserve flexibility and provide businesses with the certainty they need to encourage the development of innovative privacy protections and new products and services.

[20] See., e.g., Remarks of Brad Smith to the Congressional Internet Caucus, November 3, 2005, available at http://www.netcaucus.org/speakers/2005/smith/.

Online advertising is a good example of the need for flexible and technology-neutral baseline principles within a framework that allows for specific self-regulatory initiatives that co-exist with, or build on top of, the baseline obligations of the law. The technologies and business models have been evolving very quickly and will likely continue to change in the coming years. Adopting very specific law based on what online advertising looks like in late 2011 likely would be dated in just a year or two, and could significantly hinder innovation. Instead, a federal privacy law might embody baseline principles of transparency, control and security. But how those are implemented with respect to current technologies and online advertising business models is more appropriately addressed through industry self-regulation and innovative technology tools than prescriptive rules that try to impose a static and one-size-fits-all set of rules on a dynamic and multi-faceted industry.

IV. Microsoft's Support For Consumer Education Efforts

While I have focused my remarks thus far on company best practices, technology tools, and baseline rules of the road established through both self-regulatory efforts and legislation, that focus should not minimize the importance of ensuring that consumers understand data practices and their privacy implications. Indeed, it would be impossible to meet consumer expectations if there were no effort to inform consumers of the protections available, the controls and tools at their disposal, and the practices of the companies with which they are interacting. Informed and educated consumers are much better able to make choices that align to their own privacy needs and sensitivities and to take steps to help protect themselves from harm. That is why we provide consumers with clear information about our own practices and, where appropriate, offer choices about what data will be collected and how it will be used. Additionally, we provide to consumers general educational materials about how to protect their privacy and security and how to stay safe online.[21] We also have partnered with consumer advocates and government agencies to develop educational materials on consumer privacy and data

[21] See, e.g., http://www.microsoft.com/security/default.aspx.

security,[22] and we believe that such initiatives are important for ensuring that consumers understand the importance of protecting their privacy and security online — and that they are equipped with the information and tools with which to do so.

V. Conclusion

Thank you for extending us an invitation to share our experiences and thoughts with you. We commend the Subcommittee for holding this hearing today, and we are committed to continuing to work collaboratively with you, other government stakeholders, members of industry, privacy advocates, and consumers to advance consumer privacy and promote trust in online services. Privacy is a moving target and a complex challenge, but we believe that it is possible to honor individuals' privacy expectations without compromising the nation's strong record of — and ongoing need for — technological innovation.

---

[22] *See, e.g.,* National Cyber Security Alliance (NCSA), *available at* http://www.staysafeonline.org/; GetNetWise, *available at* www.getnetwise.org; Internet Keep Safe Coalition, *available at* www.ikeepsafe.org; Stop. Think. Connect, *available at* http://safetyandsecuritymessaging.org.

Appendix 1

Microsoft Advertising

AdChoices: Learn about ads

Who delivered this ad to you?

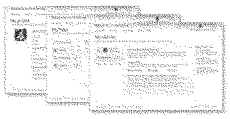
This ad was delivered to you by Microsoft Advertising.

Why are some ads personalized?

To provide you with a more relevant online experience, Microsoft Advertising customizes a portion of the online ads that you see based on your past online activity. Information about your past online activity, or the activity of other people using this computer, might be used to help predict your interests and select the ads that you see.

Where can I learn more about my online information?

View and manage your online information in the Microsoft Personal Data Dashboard **Beta**. New



Where can I learn more about how Microsoft Advertising uses the information that it collects?

For more information about Microsoft Advertising privacy practices and principles, see the Display of Advertising (Opt-out) section of the Microsoft Online Privacy Statement and Microsoft Privacy Principles for Search and Online Behavioral Targeting.

What options do I have about personalized advertising?

You can:

- Opt out of receiving personalized ads on websites that use the Microsoft Advertising Platform and manage your advertising interests with the My Interests tool.
- Opt out of receiving personalized ads from Microsoft and other advertising companies by visiting the Consumer Choice website.

How can I learn more about privacy and online advertising?

For more information about online privacy visit the Microsoft Online Services Division Online Privacy and Safety Center. New

For more information about online advertising, visit Understanding Online Advertising (North America) or Your online choices (Europe).

For more information about how online advertising affects your privacy, see

Listen to Microsoft perspectives on online **privacy**, **safety**, and **personalized advertising**.

the Learn More page on the Network Advertising Initiative (NAI) website.

For more information about how Internet Explorer 9 can help maintain your privacy choices, see the Internet Explorer 9 Features page on the Internet Explorer website.

Appendix 2

Microsoft Advertising

Sign in

Personalized Advertising from Microsoft

(Last updated February 2012)

Why are ads personalized?

Personalized ads from Microsoft help provide ads that are more relevant and useful to you. Learn more about personalized ads.

Don't want personalized ads from Microsoft?

If you don't want to see personalized ads from Microsoft, you can choose not to receive these types of ads on websites that use the Microsoft Advertising Platform by selecting the opt-out choice on this page. You can also choose to opt out of receiving personalized ads from advertising companies other than Microsoft, on the Consumer Choice Page.

How can I influence personalized ads?

At Microsoft, we do our best to provide personalized ads that you might find interesting. We don't always get it right, though. With our My Interests tool, you can help us customize your personalized ads by selecting areas that are of interest and not of interest to you.

Note
The ads you see might not always reflect your selected interests. Only a small portion of the ads that we display is personalized, and different factors influence how they're personalized.

If I opt out, what happens?

Opting out does *not* mean you will stop getting ads or see fewer ads; however, if you do opt out, the ads that you receive will no longer be personalized.
In addition, opting out does not stop information from being collected. However, neither this information nor any information collected from you in the past will be used for displaying personalized ads. Microsoft will continue to deliver content that is personalized for you, such as the news articles that are displayed on MSN and the results that appear when you search for software updates.

Your opt-out choices

On this computer or device, when you use this web browser: Save

You are opted in

On any computer or device, after you've signed in to Windows Live™:

You must sign in before you can update the setting.

My Interests

This list is generated based on interests that you have added or removed or that Microsoft has suggested.

Interests are available only after you have signed in with your Windows Live™ ID. Please sign in to manage your interests.

Does Microsoft have health based personalized ads?

Microsoft personalizes ads on many different segments including those that are health-related. 'My interests' section lists all segments or you can view the health segments.

On your computer or device, we place the following cookies associated with online advertising:

Cookie for this browser: MUID = 14CFC7EF4ACB67C937CFC4884ECB67A6
Cookie for current user:

Help build the largest human-edited directory on the web.
Submit a Site - Open Directory Project - Become an Editor
Directory listings are provided by Open Directory and enhanced by Microsoft.

Give us feedback | Help

Appendix 3

Microsoft Personal Data Dashboard Beta

Sign out

My Profile My Data My Choices More Services

My data

On this page, you can view and manage some of your online personal information.

Interests

Bing searches

More data Viewing zone

Your interests

These are topics that you said you like or that we think you might like.

You said you like these topics:

Add more interests

You haven't added any interests yet. To search for topics that might interest you, simply type the keywords in the **Add more interests** box.

You said you dislike these topics:

Add more interests

Do you want to add to your list of dislikes? To search for topics that don't interest you, simply type the keywords in the **Add more interests** box.

We think you might like these topics:

No interests are currently assigned to you.

Data tips

Managing your interests

Interests are topics that you're curious or excited about—like your favorite music, books, and Movies. You can view, confirm, or remove any of the topics in this list.

Interested in other topics?

You can add more topics by using the search box.

Privacy Legal © 2011 Microsoft Corporation Help Feedback

Microsoft Personal Data Dashboard Beta

Sign out

My Profile My Data My Choices More Services

My choices

On this page, you can make choices about how Microsoft uses your data.

Information use is allowed by the following enabled services.

Allowed Microsoft Advertising

Not Allowed Microsoft Email Communications

More services Coming soon

About Microsoft Advertising

With the Microsoft Personal Data Dashboard, you can choose not to receive personalized ads on websites that use the Microsoft Advertising Platform by not allowing Microsoft Advertising to use your information.

Information used by Microsoft Advertising

The Microsoft Advertising Platform customizes personalized ads based on different types of information, including but not limited to:

Bing searches Interests Profile

What does it mean not to allow Microsoft Advertising to use your information?

Well, first, it doesn't mean you will stop getting ads or see fewer ads; but, it *does* mean that the ads you get won't be personalized anymore by Microsoft Advertising. Microsoft will continue to collect information for other uses, such as delivering content that is personalized for you; for example, the news articles displayed on MSN and the results you get when you search for software updates.

Tips on choices

Personalized advertising from other companies

You can also opt out of getting personalized ads from advertising companies other than Microsoft, on the Consumer Choice page.

AdChoices: Learn about ads

To learn more about personalized advertising and how you can control which ads you see, see the AdChoices: Learn about ads page.

Privacy Legal © 2012 Microsoft Corporation Help Feedback

Microsoft Personal Data Dashboard Beta

Sign out

My Profile My Data My Choices More Services

More services

Here are additional Microsoft services that may store and use your personal user information. Click the link to each service to manage your personal information there.

Windows Live Services

Windows Live provides a suite of services to store and manage your profile information online, including Hotmail, Calendar, Photos, and SkyDrive. For the full list, see the Windows Live directory of services.

MSN Profile

If you created a public profile on MSN, you can edit or delete your profile in the MSN Profile Page.

Microsoft.com Profile

View and manage your microsoft.com profile at the Microsoft.com Profile Center.

Xbox

View and manage your Xbox Live or Xbox.com profile on the My Xbox page on Xbox.com

Zune

View and manage your Zune or Zune Pass profile by clicking Manage My Account on the profile page of Zune.net

To learn more about how Microsoft uses your information, please read the Microsoft Online Privacy Statement.

Privacy Legal © 2012 Microsoft Corporation Help Feedback

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, 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. Meyer follows:]

Prepared Statement of Scott Meyer

CEO and Founder

Evidon, Inc.

Before the House Committee on Energy and Commerce

Subcommittee on Commerce, Manufacturing and Trade

U.S. House of Representatives

October 13, 2011

Introduction

Chairman Bono Mack, Ranking Member Butterfield and distinguished Members of the Subcommittee, my name is Scott Meyer, and I am the CEO and Founder of Evidon. I appreciate the opportunity to appear before you today to testify about consumer expectations regarding online behavioral advertising ("OBA") and the important role that Evidon plays in meeting those expectations.

Let me begin by telling you about Evidon and our role in the online marketplace. Then, I will discuss what we are learning about consumers – specifically, what they understand and expect about advertising and data collection in the online environment.

Evidon Empowers Consumers in the Online Space

Evidon was founded specifically to promote transparency, consumer control, and accountability across the online advertising market and to facilitate the development of the self-regulatory program which empowers consumers in the online environment. That program, set out in the *Self-Regulatory Principles for Online Behavioral Advertising*[1] and released in July 2009, is designed to give consumers a better understanding of and greater control over interest-based, or "behavioral," ads. A core requirement of the Principles is the display of a distinct "Advertising Option Icon" (▷) on behavioral ads and websites where data is collected.[2]

Evidon is committed to creating technology solutions that realize these principles. While data collection and use activities across the online advertising ecosystem can be difficult

[1] AAAA, ET AL., SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf.
[2] The Advertising Option Icon is licensed by the Digital Advertising Alliance. More information is available at THE SELF-REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING, http://www.aboutads.info.

to understand, it is our belief that dedicated focus and technology is making this transparent and allowing industry to communicate with consumers in a simple and effective manner.

Evidon plays two important roles in the self-regulatory program. First, in October 2010, after an extensive 9-month evaluation, the Digital Advertising Alliance[3] chose Evidon to provide the technology powering the self-regulatory enforcement programs of the Council of Better Business Bureaus and the Direct Marketing Association.

Second, we are the leading provider of compliance services to online advertisers, advertising agencies, publishers, advertising networks, and technology providers. Our platform, called Evidon InForm, displays the Advertising Option Icon in the corner of ads and on webpages, which, when clicked, enables consumers to easily see more information about the companies involved in delivering that advertisement and to opt-out of data collection and use.[4]

Evidon has also led the market in several industry-wide initiatives, including the creation of the Open Data Partnership, which allows consumers to see what information participating companies have collected about their interests and edit that information or opt-out of collection or use. Additionally, Evidon provides a free web browser add-on called Ghostery that allows users to identify the companies tracking them on web pages they visit, and to optionally block any or all known trackers, among other features.

---

[3] The Digital Advertising Alliance (DAA) is a cross-industry coalition of five trade associations: the American Association of Advertising Agencies (AAAA), the American Advertising Federation (AAF), the Association of National Advertisers (ANA), the Direct Marketing Association (DMA), and the Interactive Advertising Bureau (IAB). The Network Advertising Initiative (NAI) and Council of Better Business Bureaus (CBBB) work closely with the DAA.

[4] Most companies honor opt-out of data use; many honor opt-out of data collection as well.

Evidon's InForm Platform, the Advertising Option Icon, and the Open Data Partnership Together Deliver to Consumers Increased Transparency and Control

Evidon's platform is an effective means for providing meaningful notice and choice to consumers, as contemplated by virtually every proposal addressing online privacy, including the Federal Trade Commission's ("FTC") Proposed Framework for Privacy and several bills that have been proposed addressing this issue. Information presented through the platform allows consumers to make informed and meaningful decisions about data collection and use. When consumers click on the Advertising Option Icon displayed by the platform (Slide 1 attached), they will see an overlay window with more information about the ad, including links to educational information about interest-based advertising, the advertiser's privacy policy, and opting-out of data collection or use (Slide 2 attached). One click takes consumers to an Evidon webpage where they can see which companies may have been involved in the collection or use of their data, and they can opt-out of data collection or use from those companies (Slide 3 attached). In addition, Evidon provides a reporting tool that tells companies how consumers are using the platform. This reporting also provides evidence of compliance with self-regulatory principles on a company-by-company basis.

The Evidon platform is thus comprised of three components:

- A *transparency component* that notifies a consumer viewing an ad that the advertisement was delivered using online behavioral data and identifies the data providers involved in its delivery.
- A *choice component* that provides consumers choice, namely, an easy method for consumers to opt-out of the collection or use of behavioral information on a company-by-company basis.

- A *reporting tool* that provides the advertising agency, advertiser, or network insight into consumers' interaction with the platform and evidence of compliance with self-regulatory principles.

Evidon's platform provides streamlined notice by presenting information on data collection to consumers through uncluttered and easy to understand in-ad notices and webpages. Importantly, this notice is provided when the consumer is viewing an individual advertisement or web page and is tailored to the consumer's particular experience at that time. Furthermore, the platform is easy to use: the icon is easily recognizable, the opt-out option is easy to find, and the process is uniform across browsers, and for all identified ad networks, data providers, and other service providers.[5] Finally, as industry adoption and consumer awareness of the Advertising Option Icon increases, consumers will be able to use it as a quick indicator that a particular advertiser is compliant with the industry's self-regulatory principles. Evidon now provides notice in nearly 20 billion online ads each month, regularly reaching more than 80 million US internet users each day.

In addition to implementing the Advertising Option Icon, Evidon has led the way in creating the Open Data Partnership ("ODP"). The ODP provides a common platform, utilized by several industry-leading data collectors,[6] that allows consumers to edit the information that ad networks have associated with their browser, rather than just opt-out of data collection or use entirely. The key feature of the ODP is an interface, called a "preference manager" that allows consumers to see, in a centralized way, what information companies have collected about their interests, and to edit that information or opt-out of collection or use (Slide 4

[5] Evidon's platform currently gives consumers the ability to opt-out of any network that may have been involved in the collection of data for the advertisement. As of October 1st, this includes 185 different ad networks, data providers, and service providers. Evidon also has a database of more than 800 companies who place third party tracking cookies on consumers' browsers, and has classified them into OBA and non-OBA providers.
[6] Participating companies include BlueKai, Lotame Solutions, eXelate, Bizo, 33Across, and Turn.

attached). The partnership is free of charge for participating companies, and the preference manager is easily accessible from the opt-out page that consumers can access via the Advertising Option Icon provided by Evidon's platform. The ODP went live earlier this year, and Evidon expects broad participation from reputable OBA providers moving forward.

Finally, in addition to providing our platform and supporting the ODP, Evidon also provides a free web browser add-on called Ghostery that gives consumers increased transparency and choice by allowing them to see which companies are tracking them on any web page they visit. Through Ghostery, consumers can see more information about those companies, and links to their privacy policy and opt-out page, if available. Additionally, Ghostery provides users with the option to block any or all known trackers. Finally, Ghostery also includes an optional, opt-in feature called GhostRank that collects completely anonymous information about the trackers its users encounter.[7] Ghostery sends this information to Evidon to help us make our privacy compliance and assurance systems more robust. Specifically, GhostRank helps Ghostery identify new trackers – for identification and blocking – and monitor industry notice and choice compliance. Ghostery has been downloaded over four million times already, is growing at a rate of 140,000 downloads per month, and has been covered by numerous media outlets.[8]

---

[7] The types of data GhostRank collects, and how those data are used, are fully disclosed in Ghostery's FAQ at http://www.ghostery.com/faq.

[8] *E.g.*, Riva Richmond, *Resisting the Online Tracking Programs*, N.Y. TIMES, Nov. 10, 2010, http://www.nytimes.com/2010/11/11/technology/personaltech/11basics.html; Wesley Fok, *Squash Web bugs with Ghostery*, GLOBE & MAIL, Aug. 10, 2009, http://www.theglobeandmail.com/news/technology/squash-web-bugs-with-ghostery/article1246594/; Erik Larkin, *With Ghostery Add-On for Firefox, Learn What Web Sites Learn About You*, WASH. POST, Mar. 9, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/03/05/AR2009030502997.html.

Consumer Testing Validates the Notion that Consumers Want Greater Choice and Control

Our testing of Evidon's platform among consumers includes both organized studies managed by third party research firms and ongoing evaluation of raw data measuring consumer interaction with our notices and control tools. Both efforts provide feedback on how we are measuring up against our goal of providing consumers with an easy and meaningful experience, and help shape the development of future products and features.

Evidon commissioned a research study by Millward Brown during Fall 2010 to learn what consumers are looking for when they engage with a privacy notice on an advertisement, and the extent to which Evidon's platform meets these expectations. In our study, 76% of consumers who clicked on the Advertising Option Icon and interacted with Evidon notices wanted to see all companies involved in targeting the ad to them. In addition, 67% felt more positive towards brands that gave them control, including the ability to opt-out.[9] Together, these metrics support the proposition that consumers want more than a simple "on-off" solution – they want substantive notice and control regarding the companies responsible for targeting ads and content to them. The Advertising Option Icon and Evidon's platform give consumers these options.

In the twelve months since the launch of the Advertising Option Icon in October 2010, we have delivered over 85 billion in-ad notices to consumers through our platform. Consumers have clicked on the Advertising Option Icon over 4.5 million times in the past year. From those clicks, more than 730,000 opt-out request have been sent through our platform.[10] These engagement metrics reflect an order of magnitude shift in the availability of information about

[9] BETTER ADVERTISING & DYNAMIC LOGIC, CONSUMER INTERACTIONS WITH IN-AD NOTICE 7 (Nov. 3, 2010), http://cdn.evidon.com/misc/consumer%20impact%20of%20ad%20notice%2011_11.pdf.
[10] Consumers frequently request an opt-out from more than one company. Each opt-out request for each company is counted separately, so there may be several opt-out requests counted for each consumer.

how data is used and the choices consumers are able to make. This is important. No longer is information solely presented in a generalized format, buried in privacy policies. Rather, it is now presented in a clear, specific, and comprehensible format, displayed to the consumer directly at the point of engagement.

At the same time, based on our consumer research, it seems clear that opt-out rates should not be the primary measurement of success for the self-regulatory program. Multiple studies have validated the notion that consumers prefer relevant content and advertising. There is no reason to assume that consumers, once afforded transparency and control, will react by opting-out of the system that powers customization and content creation. Ultimately, success should be measured by the degree to which access and control tools are produced in a credible fashion, and the extent to which these tools are offered to the consumer at the point of collection and use.

A common theme running through our consumer studies is that there can be no one-size-fits-all approach to consumer privacy. This insight is not surprising, as formal studies and lay observation clearly show that consumers take an individualized approach to how they value privacy trade-offs, particularly online. Pioneering privacy researcher Dr. Alan Westin observed that consumers fall into three general groups regarding their view on privacy: (1) those who prioritize privacy, are generally skeptical about organizations that ask for personal information, and will trade off consumer benefits for privacy protections where the two compete; (2) the majority of consumers,[11] generally pragmatic about privacy, who will weigh the intrusiveness of personal information requests against consumer benefits they will receive

[11] Humphrey Taylor, *Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits*, HARRIS INTERACTIVE (Mar. 19, 2003), http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Most-People-Are-Privacy-Pragmatists-Who-While-Conc-2003-03.pdf.

and generally want to be able to decide for themselves where privacy is concerned; and (3) those who are unconcerned about privacy, generally trustful of organizations that request personal information and are most willing to trade privacy for consumer benefits. To be successful, access and control tools should be developed with all of these groups – and in particular the majority privacy pragmatists – in mind.

Individualized privacy preferences can also be seen today in consumers' interactions with online services, in particular social media. Consumers have demonstrated that they fall along a broad line between those who want to share everything with the world, and those who want tight controls over with whom they share information. Indeed, the implementation of more granular and comprehensible privacy controls has even become an element of competition among social networks, as the growth of Google+, with its "Circles" feature, has shown. To be effective in today's online world, therefore, consumer privacy controls should also be granular, understandable, and allow consumers to express their individualized privacy interests.

One-Size-Fits-All Solutions such as "Do Not Track" Ignore Consumers' Preference for Greater Transparency, Choice, and Control

In an attempt to provide consumers with more effective privacy controls, one-size-fits-all proposals such as "Do Not Track" have gained traction, primarily due to their supposed simplicity. Indeed, during the current Congress, several Members have put forward various Do Not Track proposals as have various interest groups. I certainly understand the appeal of Do Not Track, particularly given the popularity and success of the FTC's Do Not Call list to control telemarketers. Nevertheless, based on our consumer research, we have considerable doubt that a blanket Do Not Track mandate is well-suited to address consumers' varying

privacy expectations and needs. Can it possibly do so in a way that fulfills the expectations of its name? And, as many have observed, such a mandate likely would fundamentally alter the functionality of the Internet that consumers have come to expect.

First, any universal tracking opt-out faces serious problems meeting consumer expectations while, at the same time, allowing for the continuation of basic Internet functionality. Many third parties use tracking technologies in order to provide important basic functionality on the Internet that consumers have come to expect, even if they do not necessarily understand the specifics of how the collected data is used. The types of tracking performed by these parties include important functionality such as shopping carts and techniques for thwarting hackers. Where, then, should the line be drawn between tracking that is permissible and necessary for the basic functioning of the Internet, and tracking that is forbidden? Consumers are bound to be disappointed and frustrated with a Do Not Track solution that has the appearance of being simple and universal, yet is tangled up in complex policy decisions and still, by necessity, allows a wide array of tracking.

Furthermore, how will consumers with myriad opinions and preferences on tracking and privacy be able to express their preferences with a universal tool? Will consumers be able to exclude from the prohibition companies whose tracking they do not mind or find useful? A binary tracking opt-out (that does not actually cover all tracking) is likely to be frustrating for consumers with a desire to express their individualized privacy preferences. Additionally, without informing consumers about the consequences of selecting a Do Not Track option, many may be frustrated or confused by the loss of online customization they have come to expect, and will likely have little patience to troubleshoot the cause.

In contrast to various Do Not Track proposals, the Advertising Option Icon and Evidon's platform, combined with the ODP, provide the level of transparency, control, and accountability across the online advertising market that enables consumers to express their individualized preferences in a meaningful and customizable way. Moreover, the platform's individualized notice and choice components provide the transparency needed for consumers to make informed decisions about privacy and benefit trade-offs in their online interactions. In many ways, Do Not Track is a blunt hammer for an issue in need of a scalpel, and the combination of the Advertising Option Icon, Evidon's platform, and the ODP provide that scalpel.

I am also concerned that, with a required one-size-fits-all approach such as Do Not Track, consumers, advertisers, and ad-supported publishers may not realize the benefits of innovative, and perhaps superior, privacy technologies that the marketplace is presently developing. Mandating such an approach would shift responsibility away from companies involved in the OBA market, and eliminate their incentive to innovate in this space. We suggest that policymakers carefully consider the risks inherent in this decision and allow competition to develop the best solution that (i) meets consumers' data privacy demands, (ii) is compatible with evolving online business models, and (iii) rewards companies that are making significant investments in credible self-regulatory technologies.

We are confident that competition will, indeed, foster the most effective OBA privacy solution because advertisers and ad networks have a strong incentive to provide increased transparency to consumers and drive the responsible development of OBA. As mentioned above, the Millward Brown study demonstrates that privacy-conscious consumers feel more positive towards brands that give them increased transparency and control.

In addition, consumers already have access to established technologies that meet individual privacy demands. Evidon, for example, provides Ghostery, a free web browser add-on that is described above and gives consumers increased transparency and choice by allowing them to see which companies are tracking them on any web page they visit.

Consumers also have access to a wide variety of other privacy options in addition to Ghostery, such as:

- **NoScript:**[12] NoScript is a web browser add-on that blocks all JavaScript by default unless a user specifically allows it for a site.
- **Abine:**[13] Abine is a company that offers a number of privacy related tools, including a web browser add-on formerly called Taco that provides users with a persistent set of opt-out cookies for a large number of advertising networks.
- **PrivacyChoice:**[14] PrivacyChoice is a company that also offers a variety of tools that allow consumers to understand and make choices about their online privacy. One of these tools, TrackerBlock, is a web browser add-on that blocks OBA tracking cookies.
- **Better Privacy:**[15] Better Privacy is a Firefox add-on that allows users to manage and automatically delete Flash Local Shared Objects, also known as "Flash cookies."
- **Network Advertising Initiative ("NAI") Opt-Out Tool:**[16] The NAI Opt-Out Tool allows consumers to see which NAI member companies have placed an advertising cookie file on the consumer's computer, and to opt-out of any or all member networks.

---

[12] NOSCRIPT, http://noscript.net.
[13] ABINE, http://www.abine.com.
[14] PRIVACYCHOICE, http://www.privacychoice.org.
[15] BETTERPRIVACY HOME, http://netticat.ath.cx/BetterPrivacy/BetterPrivacy.htm.
[16] NETWORK ADVERTISING INITIATIVE, OPT OUT OF BEHAVIORAL ADVERTISING, http://www.networkadvertising.org/managing/opt_out.asp.

- **AboutAds.info**:[17] The Digital Advertising Alliance ("DAA") has set up a website to inform consumers and companies about the Self-Regulatory Program for Online Behavioral Advertising. This website includes a tool that allows consumers to opt-out from receiving interest-based advertising from some or all of the DAA's participating companies, learn more about the privacy practices of each company, and see which companies have enabled OBA for the consumer's browser.

Finally, as noted above, when an individual opts-out of tracking, many attributes of their browsing experience will change. The extent to which those changes are deemed acceptable should continue to be an individual decision. With simple and clear information, we believe consumers will be able to make these subtle decisions, balancing their individual privacy and browsing preferences. We are concerned, however, that requiring the adoption of a single tool, using potentially loaded terminology, may encourage consumers to make a rapid decision without evaluating the consequences, which will only frustrate them in both the short and long term.

Conclusion

This hearing is all about consumer expectations. One thing on which we can all agree is that consumers expect free online content. Targeted advertising plays an essential role in supporting the vibrant, open, and free Internet that consumers have come to enjoy and expect.

Thank you again for inviting me to testify before you today. I hope that you will find my testimony and my answers to your questions useful as you evaluate effective solutions for meeting consumer expectations with regard to interest-based advertising.

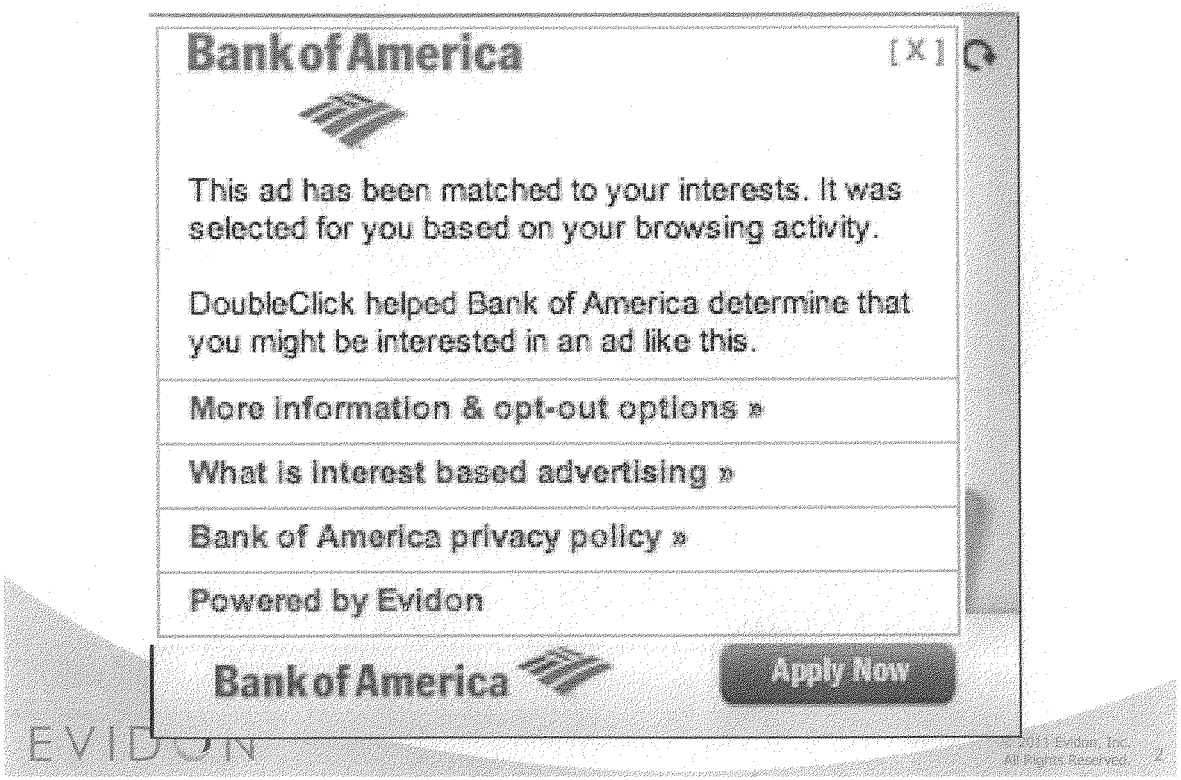
[17] THE SELF-REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING, http://www.aboutads.info.

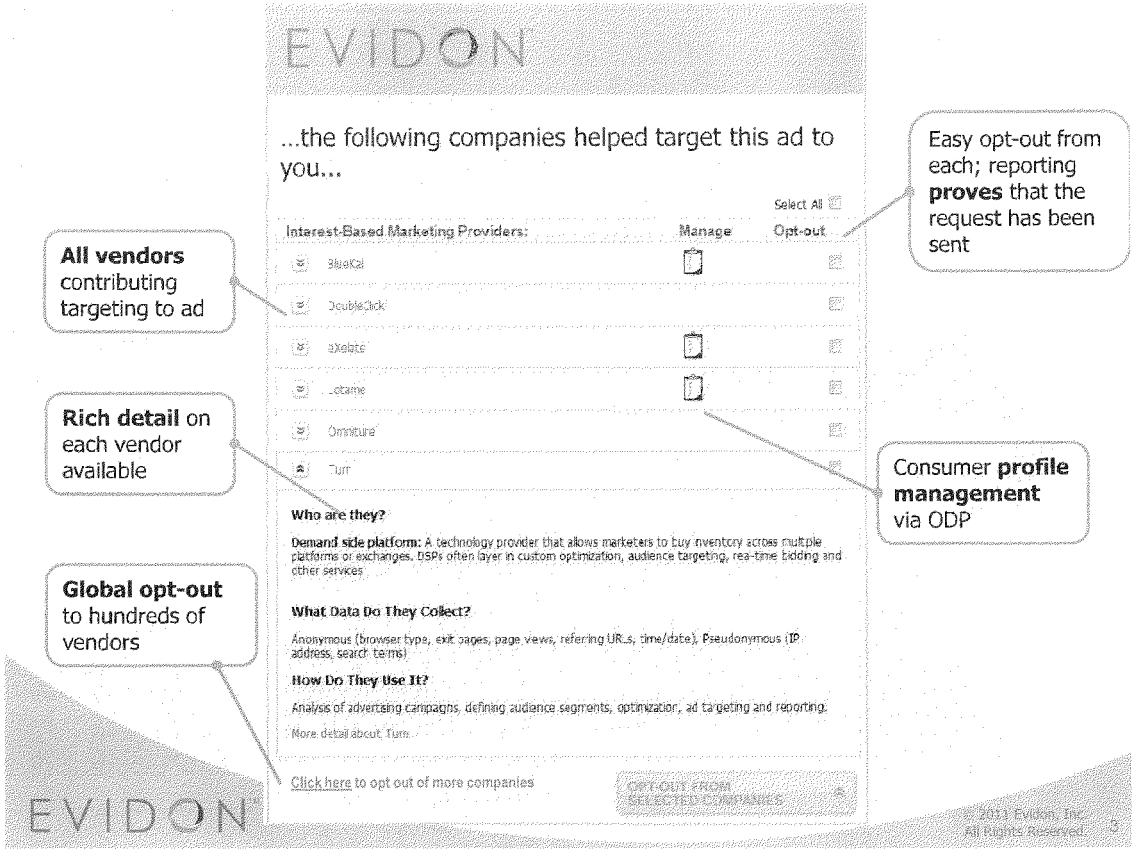
The Advertising Option Icon and Overlay – Step 1

EVIDON

2011 Evidon, Inc.
All Rights Reserved.

The Advertising Option Icon and Overlay – Step 2




EVIDON
...the following companies helped target this ad to you...
Select All
Interest-Based Marketing Providers:
Manage
Opt-out
BlueKai
DoubleClick
aXelate
Lotame
Omniture
Turn
Who are they?
Demand side platform: A technology provider that allows marketers to buy inventory across multiple platforms or exchanges. DSPs often layer in custom optimization, audience targeting, rea-time bidding and other services
What Data Do They Collect?
Anonymous (browser type, exit pages, page views, referring URLs, time/date), Pseudonymous (IP address, search terms)
How Do They Use It?
Analysis of advertising campaigns, defining audience segments, optimization, ad targeting and reporting.
More detail about Turn
Click here to opt out of more companies
OPT-OUT FROM SELECTED COMPANIES
EVIDON
© 2011 Evidon, Inc.
All Rights Reserved.
All vendors contributing targeting to ad
Rich detail on each vendor available
Global opt-out to hundreds of vendors
Easy opt-out from each; reporting proves that the request has been sent
Consumer profile management via ODP

One Place to Manage Targeting Profiles

The Open Data Partnership (ODP)

How Data Powers Your Experience

Online advertising companies tailor advertisements to you by matching summary of interests. This summary could come from several sources, browsing activity and your response to other ads. To learn more about interest-based advertising works, click here.

The following companies may have been involved with the collection or use of da interests and online activity. If you prefer that these companies not use data abo this way, you can opt-out below. If you opt out, you will still see ads online, and in may be collected about your browsing activity, but companies will not use this inf the ads you see online. For detailed information on how each company uses you their opt-out policies, click on the company name below.

Interest-Based Marketing Providers:	Manage
BlueKai	☐
DoubleClick	
eXelate	☐
Lotame	☐
Omniture	
Turn	

OPT-OUT FROM SELECTED COMPA

I am:

Gender ◉ Male ○ Female ○ N/A

Age ○ 18-24 ○ 25-34 ○ 35-44 ○ 45-54 ○ 55-64 ○ 65 ○ N/A

My interests that marketers may use to deliver relevant ads include:

- ☐ Asian Community
- ☐ Auto Buyers
- ☐ Auto Buyers - Compact
- ☒ Auto Buyers - Convertible
- ☐ Auto Buyers - Coupes
- ☐ Auto Buyers - Diesel
- ☐ Auto Buyers - Hatchback
- ☐ Auto Buyers - Hybrid
- ☐ Auto Buyers - Luxury
- ☐ Auto Buyers - Minivan
- ☐ Auto Buyers - New Cars
- ☐ Auto Buyers - Sedan
- ☐ Auto Buyers - Sports cars
- ☐ Auto Buyers - SUV
- ☐ Finance
- ☐ Finance - Small Business
- ☐ Finance - Stocks
- ☐ Guys and Gear
- ☐ Health
- ☐ HH Income $20,000-$29,999
- ☒ HH Income $30,000-$39,999
- ☐ HH Income $40,000-$49,999
- ☐ HH Income $50,000-$59,999
- ☐ HH Income $60,000-$74,999
- ☐ HH Income $75,000-$99,999
- ☐ HH Income $100,000-$124,999
- ☐ Shopping - Kitchen
- ☐ Shopping - Laptops
- ☐ Shopping - Lighting
- ☐ Shopping - Men Fashion
- ☐ Shopping - Mobile
- ☐ Shopping - Music
- ☐ Shopping - Musical Instruments
- ☐ Shopping - Outdoor
- ☐ Shopping - Personal Tech
- ☐ Shopping - Pets
- ☐ Shopping - Shoes
- ☐ Shopping - Software
- ☐ Shopping - Sports/Recreation
- ☐ Shopping - Toys
- ☐ Shopping - TVs
- ☐ Shopping - Video Games

2 of 3 eXelate Media Preference Manager

EVIDON™

© 2011 Evidon, Inc.
All Rights Reserved.

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, sen-

sitive 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 and 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:]

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE

HOUSE OF REPRESENTATIVES COMMITTEE ON ENERGY AND COMMERCE

HEARING ON

"UNDERSTANDING CONSUMER ATTITUDES ABOUT PRIVACY"

OCTOBER 13, 2011

TESTIMONY OF

LINDA WOOLLEY

MEMBER, BOARD OF DIRECTORS

DIGITAL ADVERTISING ALLIANCE

I. Introduction

Chairman Bono Mack, Ranking Member Butterfield, and Members of the Subcommittee, good morning and thank you for the opportunity to speak at this important hearing.

My name is Linda Woolley. I am the Executive Vice President of Washington Operations for the Direct Marketing Association ("DMA"), a global trade association of thousands of businesses and nonprofit organizations that use and support multi-channel direct marketing tools and techniques. Today, I am pleased to testify on behalf of the Digital Advertising Alliance ("DAA") and to report to the Subcommittee on the substantial progress of our Self-Regulatory Program.

The DAA is an organization of leading companies and trade associations formed to administer and promote the Self-Regulatory Principles for Online Behavioral Advertising. My testimony today will describe how the online advertising industry has successfully worked to give consumers transparency about online data collection practices and to create easy, uniform, and effective tools for consumers. DAA participating companies recognize that consumers may have different preferences about online advertising, and want to build consumer trust in the online experience by ensuring that consumers have meaningful choices about how data is collected and used.

II. Online Advertising Benefits Consumers and the Economy

It is impossible to overstate the economic importance of the Internet today. Even in difficult times, e-commerce has continued to grow and thrive. Simply put: the Internet economy creates jobs. A 2009 study found that more than three million Americans are employed due to the advertising-supported Internet, contributing an estimated $300

billion, or approximately 2%, to our country's GDP.[1] There is Internet employment in every single congressional district.[2] The Internet is now the focus and a symbol of the United States' famed innovation, ingenuity, inventiveness, and entrepreneurial spirit, as well as the venture funding that follows.

The Internet continues to evolve in extraordinary and exciting ways. Tools like social networking, mobile applications, and daily deals are contributing to economic growth while revolutionizing our daily lives. In 2010, the average American spent 32 hours per month online.[3] Total U.S. e-commerce spending reached $227.6 billion last year, an increase of 9% over the previous year that included travel and other retail spending.[4]

Advertising helps to fuel this Internet economic engine. According to the 2011-2012 edition of the DMA's Power of Direct Marketing Report, based on results in the first half of this year, expenditures in 2011 on online marketing in the United States, including both e-mail and Internet, are expected to total $30 billion and to generate $639 billion in U.S. sales.

Revenues from online advertising support and facilitate e-commerce and subsidize the cost of content and services that consumers value, such as online newspapers, blogs, social networking sites, mobile applications, email, and phone services. The support provided by online advertising is substantial and growing despite the difficult economic times. In the first half of 2011, Internet advertising revenues

---

[1] Hamilton Consultants, Inc. with Professors John Deighton and John Quelch, *Economic Value of the Advertising-Supported Internet Ecosystem*, at 4 (June 10, 2009), available at http://www.iab.net/media/file/Economic-Value-Report.pdf.
[2] *Id.* at 53.
[3] comScore Data Mine, "Average Time Spent Online per U.S. Visitor in 2010" (January 13, 2011) available at http://www.comscoredatamine.com/2011/01/average-time-spent-online-per-u-s-visitor-in-2010/.
[4] comScore, "The 2010 U.S. Digital Year in Review" (February 2011).

reached a new high of $14.9 billion, an impressive 23% higher than the same period last year.[5]

Because of advertising support, consumers can access a wealth of online resources for free or at a low cost. These resources have transformed our daily lives. Imagine parents who discover their child is sick at two o'clock in the morning. They can go online to look up basic medical information or find directions to the nearest doctor's office or emergency room. The Internet is now so established that we tend to take the resources that it offers for granted, but in fact, those resources are largely supported by advertising.

Interest-based advertising is an essential form of online advertising. As the Subcommittee knows, interest-based advertising, also called behavioral advertising, is delivered based on consumer preferences or interests as inferred from data about online activities. Consumers are likely to find interest-based advertisements more relevant than random messages, and advertisers are more likely to attract consumers that want their products and services. For example, browser activity can help advertisers find an audience that is likely to be interested in baby products, which is likely to be a different group from the audience advertisers are trying to reach with offers for retirement homes, world travel, or sports cars. Websites also benefit because interest-based advertising garners better responses, allowing websites to earn more revenue – and support more content and services – with fewer advertisements. These benefits help small businesses and small publishers to continue to thrive on the Internet.

---

[5] Interactive Advertising Bureau Press Release, "Internet Ad Revenues at Nearly $15 Billion in First-Half 2011, Up 23%, Second Quarter 2011 Breaks Record Again" (September 28, 2011) (reporting results of PricewaterhouseCoopers study).

Interest-based advertising is vital for new start-up companies and small businesses to reach potential customers. Smaller websites cannot afford to employ sales personnel to sell their advertising space, and may be less attractive to large brand-name advertising campaigns. Interest-based advertising helps small companies to overcome these challenges. In the online advertising ecosystem, small website publishers can increase their revenue by featuring advertising that is more relevant to their users. In turn, advertising-supported resources help other small businesses to grow. Nearly two-thirds of U.S. small businesses use online tools, such as travel booking and networking services, to help them run their companies.

Recent research highlights the importance of interest-based advertising. During the Subcommittee's September 15, 2011, hearing on "Internet Privacy: The Impact and Burden of EU Regulation," the Subcommittee heard testimony from Professor Catherine Tucker about the effect on advertising performance of the European Union's e-Privacy Directive, which limits the ability of companies to collect and use behavioral data to deliver relevant advertising. Professor Tucker's research study on this question found that the e-Privacy Directive was associated with a 65% drop in advertising performance, measured as the percent of people expressing interest in purchasing an advertised product. The NetChoice coalition has estimated that this figure would translate to a loss of $33 billion for American businesses over five years if the United States adopted similar regulation.[6] The study also found that the adverse effect of such regulation was greatest for websites with content that did not relate obviously to any commercial product, such as general news websites.

[6] NetChoice, "Estimate of U.S. Revenue Loss if Congress Mandated Opt-In for Interest-Based Ads", available at http://www.netchoice.org/library/estimate-of-us-revenue-loss-if-congress-mandated-opt-in-for-interest-based-ads/.

In general, the data used for interest-based advertising is not personally identifiable, except when consumers choose to provide personally identifiable information. Nevertheless, the advertising industry recognizes and respects that some consumers may prefer not to receive such advertising. Our industry has done a tremendous amount of work to make sure that consumers have transparency about online behavioral advertising, and that consumers can exercise control over their preferences – including opting out, if they so desire.

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

In February 2009, after an extended deliberative process, the Federal Trade Commission published a Staff Report that called upon industry to "redouble its efforts" to create self-regulation of online behavioral advertising.[7] The report set out a roadmap of several key elements that should be included in self-regulation, including transparency and consumer control. The Commission also made clear that consumer tools to exercise choice should be easy to use, effective, uniform, and ubiquitous.

Following the Commission's Staff Report, leading trade associations and companies responded quickly and effectively. This effort has been spearheaded by the DMA, the American Association of Advertising Agencies, the Association of National Advertisers, and the Interactive Advertising Bureau ("IAB"), and also includes the American Advertising Federation, the Network Advertising Initiative, and other leading industry associations that represent components of the Internet ecosystem. These associations and the companies participating in the self-regulatory effort collectively comprise the DAA.

---

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

In July 2009, just five months after the Federal Trade Commission's endorsement of self-regulation, our coalition announced a groundbreaking set of Self-Regulatory Principles for Online Behavioral Advertising.[8] The Principles apply across the entire online advertising ecosystem. They address all of the key elements called for in the Federal Trade Commission's 2009 Staff Report, namely:

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

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

These Self-Regulatory Principles are comprehensive yet flexible enough to respond to the complex and rapidly evolving online advertising ecosystem. Most importantly, they represent consensus in the online advertising community, and are supported by all of the major industry stakeholders.

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

IV. Implementing the Self-Regulatory Program

The advertising industry has put its money where its mouth is. Since releasing the Self-Regulatory Principles in July 2009, the industry has made significant investments in the infrastructure required to implement the Principles across the Internet. This tremendous effort has included designing, building, and deploying a centralized choice mechanism and launching an industry website at www.Aboutads.info. A timeline of milestones is attached (Attachment 1).

The DAA is seeing these efforts pay off. Our participating companies collectively account for the vast majority of online behavioral advertising. With companies competing for business based on privacy features, the Self-Regulatory Principles are beginning to become a part of doing business in the online advertising industry. The list of participating companies is impressive. It includes companies that serve online ads, and our program now covers all of the 15 largest online ad networks. The program also includes brand advertisers, most of which are "household names." In addition, companies that are part of the program are requiring in contracts that their business partners and suppliers participate in the Self-Regulatory Program and adhere to the Self-Regulatory Principles. I will highlight our achievements in three key areas: transparency and consumer control, consumer education, and enforcement.

A. Transparency and Consumer Control

The DAA's Advertising Option Icon is a key feature of the Self-Regulatory Program (Attachment 2). Launched in 2010, the Advertising Option Icon has already become a familiar sight across the Internet. Based on results supplied by participating companies, we estimate that tens of billions of icons are being delivered to consumers

every single day. Six hundred billion icons were served in August alone. This remarkable level of visibility makes our Program easy for consumers to find, understand, and use. Most importantly, when icons are served on ads, it is at the very moment that a consumer is likely to be interested in making a choice about his or her preference and most apt to take action.

The Federal Trade Commission made clear in its 2009 Staff Report, and we agree, that consumers should get notice of behavioral advertising practices that is uniform, ubiquitous, and timely. For uniformity, we also agreed that this notice should use a special graphic icon that would be memorable to consumers. Calling on the professional expertise of the advertising industry, we developed the Advertising Option Icon to be a simple but attention-grabbing graphic that we hope will become as universally familiar and recognizable as the recycling logo.

To make sure this notice is ubiquitous and timely as recommended by the Federal Trade Commission, we reached the innovative solution of embedding the icon where data is collected and used for online behavioral advertising. This form of enhanced notice pulls notice out of the privacy policy and makes disclosures easily detectable to consumers.

Many companies are delivering the icon on their own. For other companies, the DAA has helped to ease the compliance process by contracting with "approved providers" DoubleVerify, Evidon, and TRUSTe, which offer technical solutions for compliance. One of these providers, Evidon, is also testifying here today and will share more about the assistance offered by the approved providers to those companies that choose to work with them.

The program is designed to be as easy as possible for the consumer to use. Let me briefly summarize how the process works from a consumer's perspective. A consumer can make a choice with respect to behavioral advertising in one of two ways:

- First, an advertisement covered by the Principles is identified with the Advertising Option Icon, which appears in the advertisement right where the consumer will notice it (Attachment 3). A consumer can click the Advertising Option Icon, which links to a clear statement about online behavioral advertising, with a link to more information and opt-out choices.
- The second way that a consumer can opt out is to got directly to the program's website, which is www.aboutads.info (Attachment 4). Interested consumers can click the large "Consumer Choice Page-check mark button" in the middle of the page and see immediately the program participants that are customizing ads for that particular browser and make choices about whether to opt out (Attachment 5). The AboutAds website also provides consumer education.

No matter where consumers go online, they can see one memorable icon that leads to the same familiar, easy-to-use choice mechanism. AboutAds.info is a simple and effective "one stop" platform for consumers to opt out of having their information collected or used for interest-based advertising purposes. Consumers can opt out with respect to all participating companies, or they can pick and choose which companies may collect and use data for such purposes.

Our self-regulatory tools are providing an unprecedented level of transparency and control across the Internet. Through the DAA website and other resources made

available through the Self-Regulatory program, millions of Internet users have been educated about interest-based advertising and their choices.

B. Consumer Education

The DAA is committed to building awareness of the Self-Regulatory Program through consumer education. Consumer education is one of the seven core Self-Regulatory Principles, and the advertising industry has made significant investments in this area. Our goal is to build consumer confidence by helping consumers to understand and exercise their choices.

Coinciding with the launch of the AboutAds.info tools, our colleagues at the IAB led the "Privacy Matters" educational campaign to inform consumers about how they can manage their online experience and to explain how advertising supports the Internet. Through this effort, consumers were exposed to hundreds of millions of online public service announcements ("PSAs") linked to the "Privacy Matters" website, which features engaging educational modules on advertising practices and safe Web browsing. While the campaign was underway, 9% of all delivered impressions were "moused-over" by consumers, who spent an average of 28 seconds on a PSA once they moused over it. These are excellent results that out-perform the standard range for this type of public service campaign. The time spent viewing one of these PSAs, for example, was equivalent to about twice the exposure time of the most common television commercial exposure of 15 seconds.

Industry has also invested in publicizing the Self-Regulatory Principles and associated tools for businesses and consumers. This multifaceted campaign, which supplements the consumer notice provided by the Advertising Option Icon, has included

the launch of the AboutAds.info website, community outreach by the participating trade associations, educational webinars to assist businesses with coming into compliance with the Principles, and the delivery of additional online PSAs. We continue to develop other education initiatives to inform consumers about interest-based advertising and the choices available to them.

C. Enforcement

Finally, I want to emphasize that companies will be held accountable for complying with the Principles. Accountability is one of the seven Self-Regulatory Principles, and the DAA believes that credible and vigorous accountability is essential to successful self-regulation. The DMA and the Council of Better Business Bureaus ("CBBB") have longstanding, effective, and respected compliance programs that are being leveraged to enforce compliance with the Principles.

The DMA has incorporated the Principles into its comprehensive Guidelines for Ethical Business Practice ("Guidelines"). All DMA members must adhere to the Guidelines, which are enforced by the DMA's Corporate and Social Responsibility team and Ethics Operating Committee. The CBBB accountability program is administered with policy direction and guidance from the National Advertising Review Council ("NARC"), and is modeled after other successful CBBB/NARC accountability programs. These programs cover all companies that are subject to the Principles. The IAB also adopted a new membership code in February 2011 requiring its members to comply with the Self-Regulatory Principles as a condition of membership.

The DMA and CBBB enforcement programs are alerted to concerns through a combination of technological monitoring across the Internet and complaints that may be

filed by consumers, competitors, government agencies, and others. Based on these alerts, the programs examine complaints and evidence, and then work with companies to help them come into compliance with the Principles. Decades of self-regulation show that this is an effective and efficient way to change company behavior.

If a company fails to cooperate voluntarily, the programs can publicize the violation and refer the issue to government authorities for further investigation. Companies that claim to adhere to the Self-Regulatory Principles, but fail to do so, risk liability for deceptive acts or practices. Of course, enforcement authorities can also investigate companies on their own initiative.

V. Continued Progress

Thanks to strong investment by the business community, the DAA's Self-Regulatory Program is well underway. While our progress has been exciting, our work continues. One of the major benefits of industry self-regulation is its ability to respond quickly to changes in technology and business practices. For example, some policymakers have raised concerns that data collected for advertising purposes could be used as a basis for employment, credit, or health insurance eligibility decisions.[9] I want to emphasize that these are hypothetical concerns that do not reflect actual business practices. Nevertheless, industry is stepping forward to address these concerns and we are expanding our guidelines to clarify and ensure that such practices are prohibited and will never occur. This type of adaptability is essential to avoid stifling innovation in the

[9] Jon Leibowitz, "FTC Chairman: 'Do Not Track' Rules Would Help Web Thrive -- Online commerce and personal privacy are not incompatible," *U.S. News* (January 3, 2011), available at http://www.usnews.com/opinion/articles/2011/01/03/ftc-chairman-do-not-track-rules-would-help-web-thrive-jon-leibowitz.

complex and dynamic Internet environment. We welcome additional input from policymakers and we are committed to examining any future concerns that may arise.

The DAA, and its participating companies and associations, look forward to continuing our efforts and working cooperatively with the Congress, the Federal Trade Commission, and the Department of Commerce as we move forward on implementing the Self-Regulatory Principles and discussing these important issues. We believe that consumers are the ones who can best determine their own preferences. We also believe in the longstanding tradition and success of self-regulation in the marketing and advertising areas. Our program creates the right framework to ensure that consumers can enjoy both exciting online services and robust privacy protection.

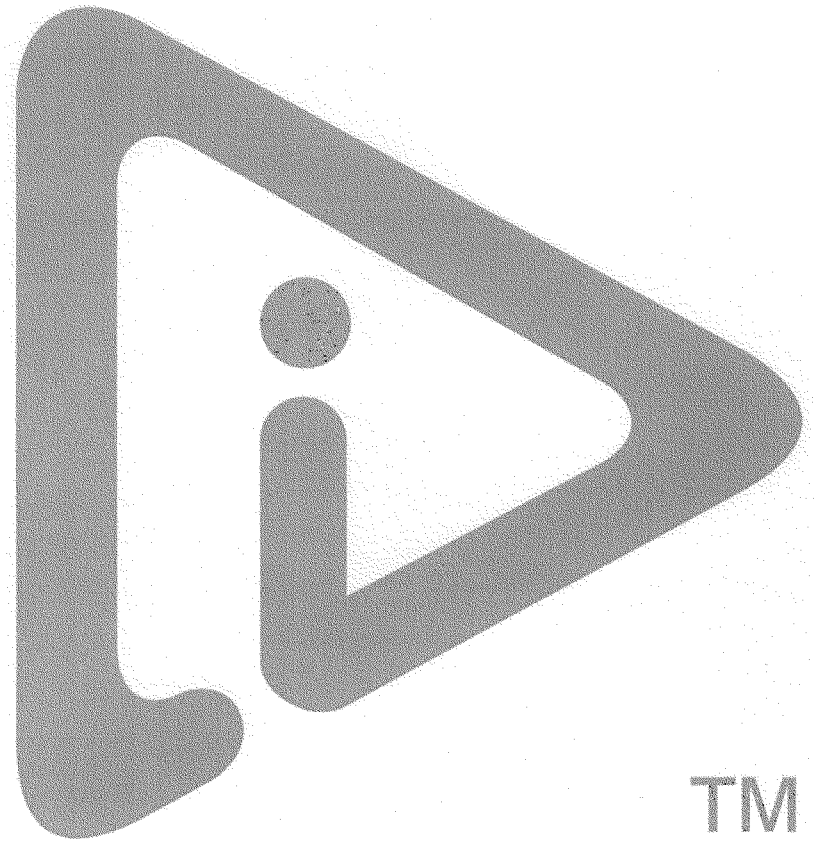
* * *

Thank you for inviting me to share the DAA's progress with the Subcommitteee. I look forward to answering any questions that the Subcommittee may have.

Attachment 1:	**Timeline of Industry Effort to Develop and Implement Self-Regulatory Principles for Online Behavioral Adverting**
December 2007	Federal Trade Commission staff releases proposed principles to guide the development of industry self-regulation in the area of online interest-based advertising.
April 2008	Industry leaders file comments on Federal Trade Commission's proposals and convene task force to examine existing self-regulatory efforts.
October 2008	Industry coalition begins drafting new self-regulatory guidelines.
February 2009	Federal Trade Commission releases final Staff Report on *Self-Regulatory Principles for Online Behavioral Advertising*
July 2009	After building support among industry stakeholders, coalition releases cross-industry *Self-Regulatory Principles for Online Behavioral Advertising* ("Principles") that correspond to the guidelines in the FTC staff report.
August 2009	Coalition turns to enforcement, operational implementation, and educational planning.
November 2009	Interactive Advertising Bureau and Network Advertising Initiative lead effort to develop technical specifications for implementing enhanced notice through a link in or around an advertisement.
December 2009	Coalition launches "Privacy Matters" education campaign, designed to educate consumers about how they can manage their online experience and to help consumers better understand how online advertising supports the Internet.
January 2010	Coalition announces intention to provide enhanced notice to consumers through a link/icon embedded in online interest-based advertisements (or, if such notice is not delivered, on the Web page where the interest-based advertisement occurs). Direct Marketing Association revises *Guidelines for Ethical Business Practice* to require members' adherence to the DAA Self-Regulatory Principles for Online Behavioral Advertising.
March 2010	Coalition commences effort to operationalize the Principles, including providing business education webinars, trademarking distinctive Advertising Option Icon, and developing an industry-wide Web site to deliver consumer education, provide information

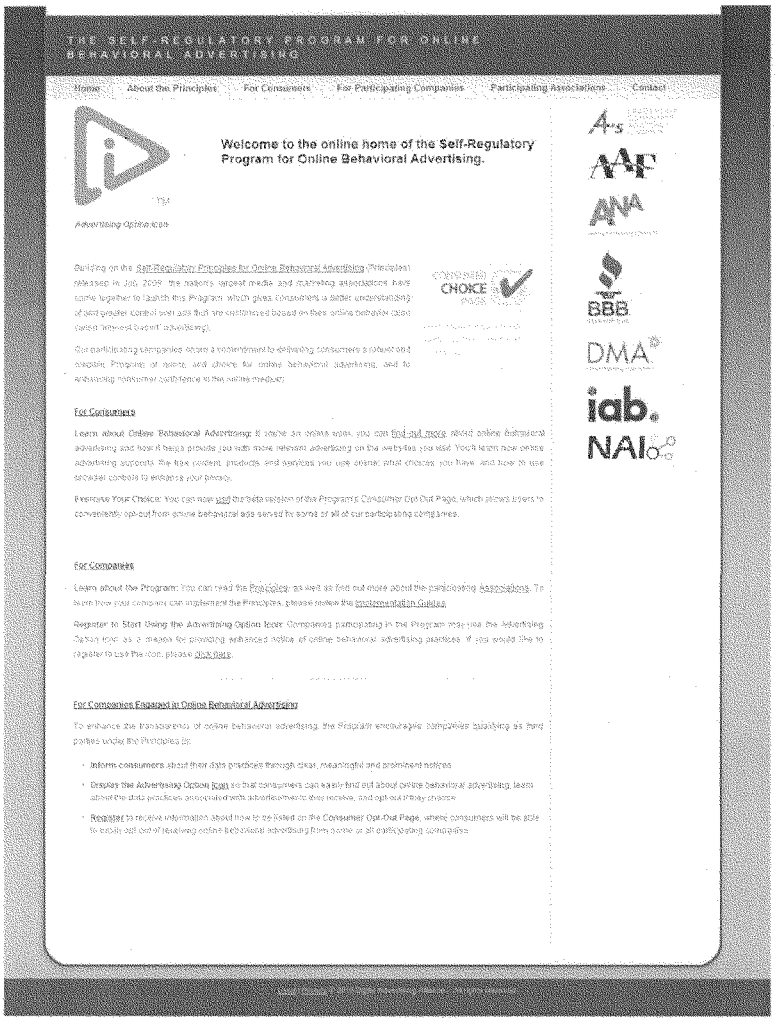
	concerning parties engaged in interest-based advertising, and offer consumer choice.
October 2010	AboutAds.info Web site launches. Companies may register to use the Advertising Option Icon and acquire specific technical guidance for the icon's implementation and use.
	Coalition selects the first "approved provider" to offer technical solutions for compliance with the Principles.
November 2010	Coalition launches consumer-facing AboutAds.info Consumer Opt-Out Page, where consumers may easily opt out of some or all of the interest-based advertisements they receive.
December 2010	Coalition selects two additional "approved provider" vendors.
January 2011	Direct Marketing Association enforcement program goes into effect.
February 2011	DAA Principles and Communications Advisory Committee convenes to consider ways to encourage international adoption of the icon and standards consistent with the Principles.
	Interactive Advertising Bureau adopts a new membership code of conduct requiring members' adherence to the DAA Self-Regulatory Principles for Online Behavioral Advertising.
March 2011	Council of Better Business Bureaus enforcement program goes into effect.
	Accountability program selects vendor to provide technical platform to monitor participating companies' compliance with the Principles.
May 2011	Council of Better Business Bureaus and the Direct Marketing Association request compliance updates from companies engaging in interest-based advertising.

Attachment 2. Advertising Option Icon



Attachment 3. Sample Advertisement with Advertising Option Icon

Attachment 4. AboutAds.info Home Page



THE SELF-REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING

Home | About the Principles | For Consumers | For Participating Companies | Participating Associations | Contact

Welcome to the online home of the Self-Regulatory Program for Online Behavioral Advertising.

Advertising Option Icon

Building on the Self-Regulatory Principles for Online Behavioral Advertising (Principles) released in July 2009, the nation's largest media and marketing associations have come together to launch this Program which gives Consumers a better understanding of and greater control over ads that are customized based on their online behavior (also called "behavioral targeted" advertising).

Our participating companies share a commitment to delivering consumers a robust and complete Program of notice and choice for online behavioral advertising, and to enhancing consumer confidence in the online medium.

For Consumers

Learn about Online Behavioral Advertising: If you're an online user, you can find out more about online behavioral advertising and how it helps provide you with more relevant advertising on the web sites you visit. You'll learn how online advertising supports the free content, products, and services you use online, what choices you have, and how to use advanced controls to enhance your privacy.

Exercise Your Choice: You can now test the beta version of the Program's Consumer Opt-Out Page, which allows users to conveniently opt-out from some behavioral ads served by some or all of our participating companies.

For Companies

Learn about the Program: You can read the Principles, as well as find out more about the participating Associations. To learn how your company can implement the Principles, please review the Implementation Guides.

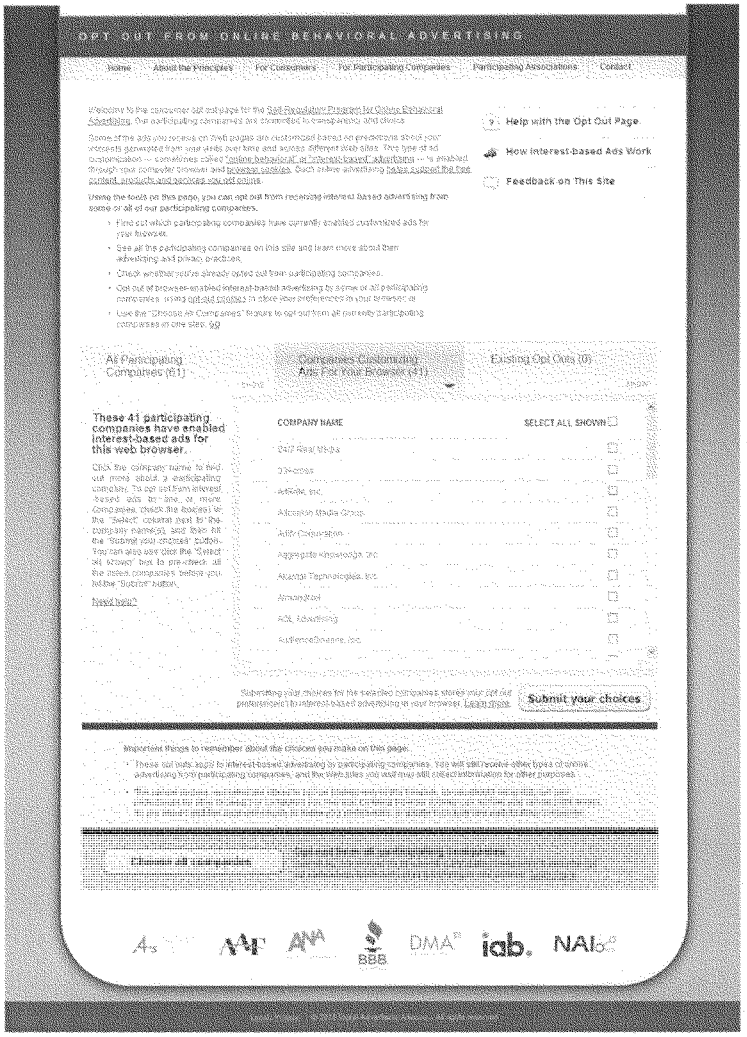
Register to Start Using the Advertising Option Icon: Companies participating in the Program may use the Advertising Option Icon as a means for providing enhanced notice of online behavioral advertising practices. If you would like to register to use the icon, please click here.

For Companies Engaged in Online Behavioral Advertising

To enhance the transparency of online behavioral advertising, the Program encourages companies including as third parties under the Principles to:

- Inform consumers about their data practices through clear, meaningful and prominent notices
- Display the Advertising Option Icon so that consumers can easily find out about online behavioral advertising, learn about the data practices associated with advertisements they receive, and opt-out if they choose
- Register to receive information about how to be listed on the Consumer Opt-Out Page, where consumers will be able to easily opt out of receiving online behavioral advertising from some or all participating companies

Attachment 5. AboutAds.info Uniform Consumer Choice Page



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 dis-

closure 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:]

TESTIMONY

Professor Alessandro Acquisti
Heinz College, Carnegie Mellon University

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

Understanding Consumer Attitudes About Privacy

October 13, 2011

Chairman Bono Mack, Ranking Member Butterfield, and Members of the Subcommittee:
I was honored to receive the invitation to appear before you today to discuss the topic of 'Understanding Consumer Attitudes About Privacy.'

My name is Alessandro Acquisti. I am an associate professor at the Heinz College, Carnegie Mellon University (CMU), and the co-director of CMU's Center for Behavioral Decision Research (CBDR).[1] I am an economist by training, and I have been studying the economics and behavioral economics of privacy for about 10 years. My research combines economics, experimental behavioral decision research, and information technology to investigate the trade-offs associated with the protection and disclosure of personal information, and how consumers calculate, and make decisions about, those trade-offs.

Some of my work focuses on quantifying the value of personal data, the costs of privacy invasions, and the benefits of information disclosure.[2] My remarks in this testimony, however, will concern research that I and others have carried out into the field of consumer privacy attitudes and behavior. I will discuss how consumers perceive, and make decisions about, the values, costs, and benefits associated with the disclosure of their personal information.

In my testimony, I will highlight three findings:

First, consumers want more than one thing when it comes to privacy and disclosure. Consumers enjoy disclosing information online to friends, and enjoy receiving personalized and free services as a result of the information they disclose. However, they also want the information they reveal to others to be protected, and they are concerned about misuses of their personal data.

Second, consumers face major hurdles in properly trading-off privacy and disclosure in the marketplace. Problems of asymmetric information, bounded rationality, and cognitive and behavior biases make it difficult for consumers to choose optimally between protecting privacy and sharing data.

Third, industry and academic research on privacy enhancing technologies suggests that consumers and firms can simultaneously achieve information sharing and privacy protection. In fact, research in this area shows that it is possible for companies to make innovative uses of personal data, and tap information as an economic resource, in ways that do not sacrifice consumer privacy. Therefore, a critical question for Congress is how to create incentives that will foster the deployment of these innovative technologies.

1. Consumers Attitudes: Consumers Want Privacy, Like Sharing

Over the years, surveys have found repeated evidence of significant privacy concerns among US consumers.[3] Most Americans believe that their right to privacy is "under serious threat" and express concerns over the way businesses collect their personal data.[4] According to some studies, a majority of individuals believe that privacy is a right, and that being asked to pay for it is "extortion."[5] Many individuals favor governmental intervention and legislation over self-regulation as a means for privacy protection.[6] Other surveys report that privacy concerns negatively affect consumers' willingness to purchase online or register on websites.[7]

Consumers seem especially troubled by tracking technologies. In a survey of 587 US adults about attitudes towards location-tracking techniques, Tsai et al. found widespread and elevated concerns about the control over data about individuals' location; generally, "respondents [felt that] the risks of using location-sharing technologies outweigh[ed] the benefits."[8] In a nationally representative survey about online behavioral targeting by marketers, Turow et al. found that 66% of US consumers did not want marketers to tailor advertisements to their interests, and that the majority "mistakenly believe[d] that current government laws restrict companies from selling wide-ranging data about them."[9] Very similar findings were reported in a different study by CMU researchers about targeted advertising.[10]

Recently, empirical experimental research has provided behavioral support for the view that consumers care for privacy: when decision-making hurdles are mitigated, consumers make deliberate decisions to protect their data, at the cost of foregoing monetary advantages.[11]

However, other market-based evidence, surveys,[12] and experiments[13] have highlighted apparent discrepancies between privacy attitudes (what consumers claim in surveys) and actual behavior. Individuals seem willing to trade privacy for convenience and bargain the release of personal information in exchange for relatively small rewards. The success of many social media services indicates that consumers like sharing information online with their friends, and enjoy the free services or personalized experiences that are made possible by sharing personal information with online providers.

2. Privacy Behavior: Hurdles In Decision Making

Consumers' willingness to share personal information is not in contradiction with their desire for privacy.[14] In economic terms, both the protection and the disclosure of personal information carry tangible and intangible trade-offs for data subjects and data holders alike. In an information economy, personal information is a currency that both consumers and firms can try to use strategically, to optimize those trade-offs.

Research, however, suggests that consumers face significant challenges in navigating those complex trade-offs in ways that reflect their self-interests. Due to those challenges, actual privacy behavior may differ from stated attitudes and, more importantly, consumers' decisions to reveal or protect personal information may be suboptimal. Roughly speaking, research has uncovered three types of hurdles that can impair privacy decision making:

a) *Asymmetric information.* Research has suggested that US consumers are often ill-informed about the collection and usage of their personal information, and the consequences of those usages. This puts them in a position of asymmetric information, and sometimes disadvantage, relative to the data holders that collect and use that information. For instance, studies have shown that websites have used tracking technologies such as "flash cookies" without disclosing their presence to consumers, and sometimes even in ways that stand directly in contrast to consumers' revealed preferences.[15] Other studies have shown that a majority of consumers mistakenly interpret the presence of a privacy policy on a website as implying privacy

protection,[16] and that members of social network sites hold erroneous beliefs about the actual visibility of their online profiles and the way social media companies handle their data.[17]

b) *Bounded rationality.* As consumers, we are limited in our ability to process information available to us and formulate rational plans for solving complex problems.[18] In the field of privacy, research has shown that 54% of privacy policies are written in ways that render them beyond the grasp of 57% of the Internet population (requiring the equivalent of more than fourteen years of education).[19] Furthermore, if US consumers were to read online privacy policies word–for–word, the opportunity costs to the economy of the time lost reading would be about $652 billion annually.[20] The problem of bounded rationality is exacerbated by the fact that the proliferation of consumer data tracking and progresses in data mining have made it possible to re-identify seemingly anonymous data and infer sensitive information from non-sensitive data. In experiments at Carnegie Mellon University, my co-authors and I were able to predict individuals' SSNs using simple demographic data made available by the individuals themselves through their social media profiles.[21] We were also able to identify (and infer personal information about) individuals in public spaces using face recognition technologies and photos made publicly available by the targets on social networking sites.[22] Consumers are unlikely to predict how the non-sensitive information they reveal today will be aggregated and analyzed tomorrow to produce such sensitive inferences.

c) *Cognitive and behavioral biases.* Even if consumers had access to complete and perfect information about all usages of their personal information, and all trade-offs associated with those usages, a host of cognitive and behavioral biases (that is, systematic deviations from theoretically rational decision making) may impact their marketplace behavior, leading to suboptimal disclosure decisions. Such biases have been analyzed by behavioral economists and decision researchers for several years. Some examples applicable to the field of privacy include:

- *Instant gratification bias.* Human beings tend to value the present more than the future, which may lead consumers to underappreciate future negative

consequences of current actions.[23] In previous research, I have shown that while the benefits of information disclosure are often immediate, the costs associated with those disclosures are not just uncertain, but appear as distant in the future. As a consequence, even when the benefits of disclosure may be small compared to its possible risks (for instance, identity theft), consumers may give in to immediate gratification, disclosing information that may put them at risk in the future.[24]

- *The paradox of control in privacy decision making.* In a series of experiments at Carnegie Mellon University, we have found that increasing the feeling of control over the release of private information can decrease individuals' concern about privacy, and paradoxically increase their propensity to disclose sensitive information - even when the objective risks associated with such disclosures do not change or, in fact, *worsen*. Our findings highlight how technologies that make individuals feel more in control over the release of personal information may have the consequence of eliciting greater disclosure of sensitive information and more elevated privacy risks.[25]
- Numerous additional experiments we ran at Carnegie Mellon University (online, in the lab, or in natural conditions) suggest that the disclosure of personal and even sensitive information by individuals can be manipulated merely by subtly altering the interface of Internet services – for instance, by showing that other individuals have made sensitive disclosures,[26] by asking questions covertly so that the act of disclosing is not salient,[27] or by altering the order in which questions of varying sensitivity are asked.[28]

The results in this area suggest that consumers often lack the information, resources, foresight or self-insight to make optimal decisions about privacy protection and information disclosure. In fact, the decision-making challenges that consumers face in the marketplace can be, and sometimes have been, exploited by firms to nudge consumers towards more disclosures.[29]

On the other hand, research suggests that, *if and when* both informational and behavioral gaps are addressed, consumers make conscious decisions to protect their privacy.

In an experiment with actual cash incentives and real privacy/monetary trade-offs, my co-authors and I investigated whether more prominent, salient, and straightforward information comparing the data handling strategies of different merchants will cause consumers to incorporate privacy considerations into their online purchasing decisions. We designed an experiment in which a shopping search engine interface clearly and compactly compared privacy policy information for different merchants. When such information was made available, consumers tended to purchase from online retailers who better protected their privacy. In fact, our experiment indicated that when comparative privacy information was made more salient and accessible, consumers were willing to pay a *premium* to purchase from more privacy protective websites.[30]

In another series of experiments, we examined the power of framing on consumers' valuations of their personal data. In one of those experiments, subjects were asked to choose between a $10 gift card with privacy protection and a $12 gift card with no such protection. In a first condition, subjects were first endowed with the card with more protection, and then asked whether they were wanted to swap that card for the more valuable, but less protected, card. In a second condition, subjects were presented with exactly the same two alternatives – but the order in which they received the cards was inverted. Our subjects were five times more likely to choose privacy protection (and reject the additional cash provided by the $12 card) in the first condition, in which they had been primed to think that their privacy would be, by default, protected. The results suggest that consumers who start from positions of greater privacy protection are much more likely to forego monetary offers and preserve that protection than consumers who feel that their data is not protected. As a consequence, repeated claims that consumers do not have privacy protection may be self-fulfilling: if consumers are told not to expect privacy, then their expectations may be altered, and they may end up valuing privacy less.[31]

3. Privacy Enhancing Technologies: Sharing Data While Protecting Privacy

While self-regulatory solutions based on notice and choice do offer consumers some degree of transparency and control, they are unlikely to solve consumers' hurdles in privacy decision

making, and sometimes fail to create sufficient incentives for firms to comply. For instance, recent Carnegie Mellon research on behavioral targeting and opt-out technologies reported numerous instances of non-compliance with the Network Advertising Initiative (NAI) and Digital Advertising Alliance (DAA) behavioral ads opt-out mechanisms among 100 leading websites.[32] Related research also indicated that consumers do not understand what they are opting out of, have difficulty opting out, and are not able to distinguish among the hundreds of tracking companies to make informed opt-out decisions.[33]

However, industry and academic labs across the United States have also developed other technologies that may address the problem of consumers' decision making hurdles, without sacrificing firms' ability to access data and innovate. "Privacy Enhancing Technologies" (or PETs) can be used to protect, aggregate, and anonymize those data in ways that are both effective (in the sense that re-identifying individual information becomes so costly to discourage the attempt) and efficient (in the sense that the desired transaction can be completed with no or minor additional costs for the parties involved). In other words, privacy-enhancing principles can be utilized without limiting the main purpose of an application or a transaction.

A vast body of research in privacy enhancing technologies suggests, in fact, that cryptographic protocols can be leveraged to satisfy both needs for data sharing and needs for data privacy. Not only is it already possible to complete verifiable and yet privacy enhanced transactions in areas as diverse as electronic payments,[34] online communications,[35] Internet browsing,[36] or electronic voting;[37] but it is also possible to have credential systems that provide authentication without identification,[38] share personal preferences while protecting privacy,[39] leverage the power of recommender systems and collaborative filtering without exposing individual identities,[40] or even execute calculations while keeping data encrypted and confidential,[41] opening the doors for novel scenarios of privacy preserving data gathering and analysis, and even privacy-preserving behavioural targeting.[42]

In other words, privacy enhancing technologies may make it possible to reach equilibria where data holders can still analyse and act upon vast amounts of micro-data, while individual information stays protected. Hence, results in this area suggest that there are ways to protect privacy without causing inefficiencies in the marketplace. Arguably, the transition to these new

equilibria would not be costless; but it could be welfare-enhancing for consumers and society as a whole.[43] Such transition could also provide the right conditions for new business models, and – as consumers develop greater trust in the way their information is protected - for more truthful sharing of consumers' data.

4. Conclusion

Consumers' attitudes towards privacy and disclosure are nuanced. Consumers enjoy exchanging information online with friends and receiving personalized services through the information they disclose. But they also want the information they reveal to be protected, and remain concerned about abuses of their personal information. Consumers thus face significant decision making hurdles when navigating the complex privacy trade-offs that emerge in the marketplace. Research suggests that self-regulatory solutions do not address those hurdles. Giving consumers knowledge of and control over the usage of their data may be *necessary* conditions for privacy protection; but empirical evidence supported by behavioral economics and decision research suggests that they are not *sufficient* conditions. As Loewenstein and Haisley write, "[i]nformational interventions are only effective against one of the two broad categories of mistakes that people make – those that result from incorrect information – and not against the other: self-control problems."[44]

However, both industry and academic labs in the United States have developed tools that can help both consumers and companies find a more desirable balance between information disclosure and information protection, and achieve better trade-offs. Research in the area of privacy enhancing technologies shows that it is possible for companies to make innovative uses of personal data, and tap information as an economic resource, in ways that do not sacrifice privacy. Policy makers should consider how to create mechanisms that will incentivize the deployment of these innovative technologies.

Thank you for inviting me to testify today. I look forward to answering your questions.

---

[1] Http://www.heinz.cmu.edu/~acquisti/

[2] A. Acquisti, 2010. "The Economics Of Personal Data and The Economics Of Privacy." Commissioned By The OECD, For The OECD Roundtable On The Economics Of Privacy and Personal Data, Paris, December 2010. http://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-OECD-22-11-10.pdf.

[3] Early Works In This Area Include: A.F. Westin, 1991. "Harris-Equifax Consumer Privacy Survey."; M. Ackerman, L. Cranor, and J. Reagle, 1999. "Privacy In Ecommerce: Examining User Scenarios and Privacy Preferences." ACM Electronic Commerce Conference (EC), 1-8. More Recent Studies Include: Harris Interactive, 2001. "Privacy On and Off The Internet: What Consumers Want."; CBS News, 2005. "Poll: Privacy Rights Under Attack." http://www.cbsnews.com/stories/2005/09/30/opinion/polls/main89473.shtml; J. Turow, L. Feldman, K. Meltzer, 2005. "Open To Exploitation: American Shoppers Online and Offline." A Report From The Annenberg Public Policy Center Of The University Of Pennsylvania; Burst Media, 2009. "Online Privacy Still A Consumer Concern." http://www.burstmedia.com/assets/newsletter/items/2009_02_01.pdf.

[4] CBS News, 2005. "Poll: Privacy Rights Under Attack." http://www.cbsnews.com/stories/2005/09/30/opinion/polls/main89473.shtml.

[5] A.M. McDonald, and L.F. Cranor, 2010. "Americans' Attitudes About Internet Behavioral Advertising Practices." Workshop On Privacy In The Electronic Society (WPES).

[6] A. Acquisti, and J. Grossklags, 2005. "Privacy and Rationality In Decision Making." IEEE Security and Privacy 3(1) 26–33. http://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf.

[7] Privacy & American Business (P&Ab). 2005. "New Survey Reports An Increase In Id Theft and Decrease In Consumer Confidence." Conducted By Harris Interactive. http://www.pandab.org/deloitteidsurveypr.html.

[8] J. Tsai, P. Kelley, L. Cranor, and N. Sadeh, 2009. "Location-Sharing Technologies: Privacy Risks and Controls." Telecommunications Policy Research Conference (TPRC).

[9] J. Turow, J. King, C. Hoofnagle, A. Bleakley, and M. Hennessy, 2009. "Americans Reject Tailored Advertising and Three Activities That Enable It." Available At SSRN: http://ssrn.com/abstract=1478214.

[10] A.M. McDonald, and L.F. Cranor, 2010. "Americans' Attitudes About Internet Behavioral Advertising Practices." Workshop On Privacy In The Electronic Society (WPES).

[11] J. Tsai, S. Egelman, L. Cranor, and A. Acquisti, 2011. "The Effect Of Online Privacy Information On Purchasing Behavior: An Experimental Study." Information Systems Research, 22, 254-268. http://www.heinz.cmu.edu/~acquisti/papers/acquisti-onlinepurchasing-privacy.pdf. A. Acquisti, L. John, and G. Loewenstein, 2010. "What Is Privacy Worth?" In Workshop On The Economics of Information Security (WISE). (Leading Paper, 2010 Future Of Privacy Forum's Best "Privacy Papers For Policy Makers" Competition.) http://www.heinz.cmu.edu/~acquisti/papers/acquisti-ISR-worth.pdf.

[12] Harris Interactive, 2003. "Most People Are 'Privacy Pragmatists' Who, While Concerned About Privacy, Will Sometimes Trade It Off For Other Benefits." www.harrisinteractive.com/harris_poll/index.asp?pid=365.

[13] S. Spiekermann, J. Grossklags, and B. Berendt, 2001. "E-Privacy In Second Generation E-Commerce: Privacy Preferences Versus Actual Behavior," ACM Electronic Commerce Conference (EC), 38–47.

[14] Attitudes framed in broad scenarios are not accurate predictors of context-specific behavior. See M. Fishbein and I. Ajzen, 1975. *Belief, Attitude, Intention and Behavior: An Introduction To Theory and Research*, Addison-Wesley.

[15] Websites Have Used Flash Cookies To Surreptitiously Re-Instantiate cookies deleted by users. See A. Soltani, S. Canty, Q. Mayo, L. Thomas, and C. Hoofnagle, 2009. "Flash Cookies and Privacy." Available At SSRN: http://ssrn.com/abstract=1446862.

[16] J. Turow, C. Hoofnagle, D. Mulligan, N. Good, and J. Grossklags, 2006. "Consumers & Privacy In The Coming Decade." Session On Communicating With Consumers In The Next Tech-Ade - The Impact Of Demographics and Shifting Consumer Attitudes, Public Hearings On Protecting Consumers In The Next Tech-Age, Federal Trade Commission (FTC), Washington D.C., November 6 - 8, 2006.

[17] Acquisti, A. and J. Grossklags, 2005. "Privacy and Rationality In Individual Decision Making." IEEE Security and Privacy 3 (1), 24-30. The study was contacted in 2005. As consumers get more informed about the privacy trade-offs associated with an existing technology (for instance, online social networks), new tracking technologies often arise that leave the consumer uninformed (for instance, flash cookies and behavioral tracking).

[18] H. Simon, 1957. "A Behavioral Model Of Rational Choice." In *Models Of Man, Social and Rational: Mathematical Essays On Rational Human Behavior In A Social Setting*. New York: Wiley. H. Simon, Herbert, 1991. "Bounded Rationality and Organizational Learning." Organization Science, 2 (1): 125-134.

[19] C. Jensen and C. Potts, 2003. "Privacy Policies Examined: Fair Warning Or Fair Game?" GVU Technical Report 03-04, ftp://ftp.cc.gatech.edu/pub/gvu/tr/2003/03-04.pdf.

[20] A. McDonald, and L. Cranor, 2008. "The Cost Of Reading Privacy Policies." I/S: A Journal Of Law and Policy For The Information Society.

[21] A. Acquisti and R. Gross, 2009. "Predicting Social Security Numbers From Public Data." Proceedings Of The National Academy Of Science, 106(27), 10975-10980. http://www.pnas.org/content/106/27/10975.full.pdf+html.

[22] A. Acquisti, R. Gross, and F. Stutzman, 2011. "Faces Of Facebook: Privacy In The Age Of Augmented Reality." Blackhat USA. http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/.

[23] T. O'Donoghue and M. Rabin, 2000. "The Economics Of Immediate Gratification," Journal Behavioral Decision Making, 13, 233–250.

[24] A. Acquisti, 2004. "Privacy In Electronic Commerce and The Economics Of Immediate Gratification." ACM Electronic Commerce Conference (EC), 21-29. http://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf. Also see: A. Acquisti, and J. Grossklags, 2005. "Privacy and Rationality In Decision Making." IEEE Security and Privacy 3(1) 26–33.

[25] L. Brandimarte, A. Acquisti, and G. Loewenstein, 2010. "Misplaced Confidences: Privacy and The Control Paradox." CIST. (Winner, Best Doctoral Student Paper Award, Cist 2010; Runner-Up, Best Paper Award, Cist 2010; Leading Paper, 2010 Future Of Privacy Forum's Best "Privacy Papers For Policy Makers" Competition.) http://www.heinz.cmu.edu/~acquisti/papers/acquisti-SPPS.pdf.

[26] A. Acquisti, L. John, and G. Loewenstein, 2011. "The Impact Of Relative Judgments On Concern About Privacy." Journal Of Marketing Research, Forthcoming 2011. http://www.heinz.cmu.edu/~acquisti/papers/acquisti-JMR.pdf.

[27] L. John, A. Acquisti, and G. Loewenstein, 2011. "Strangers On A Plane: Context-Dependent Willingness To Divulge Personal Information." Journal Of Consumer Research, 37(5), 858-873. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1430482.

[28] A. Acquisti, L. John, and G. Loewenstein, 2011. "The Impact Of Relative Judgments On Concern About Privacy." Journal Of Marketing Research, Forthcoming 2011. http://www.heinz.cmu.edu/~acquisti/papers/acquisti-JMR.pdf.

[29] R. Balebako, P. G. Leon, H. Almuhimed, P.G. Kelley, J. Mugan, A. Acquisti, L. Cranor and N. Sadeh, 2011. "Nudging Users Towards Privacy On Mobile Devices," Proceedings Of The Workshop On Persuasion, Nudge, Influence and Coercion, Computer-Human Interaction Conference (CHI).

[30] J. Tsai, S. Egelman, L. Cranor, and A. Acquisti, 2011. "The Effect Of Online Privacy Information On Purchasing Behavior: An Experimental Study." Information Systems Research, 22, 254-268.

[31] A. Acquisti, L. John, and G. Loewenstein, 2010. "What Is Privacy Worth?" In Workshop On The Economics of Information Security (WISE). (Leading Paper, 2010 Future Of Privacy Forum's Best "Privacy Papers For Policy Makers" Competition.) http://www.heinz.cmu.edu/~acquisti/papers/acquisti-ISR-worth.pdf.

[32] S. Komanduri, R. Shay, G. Norcie, B. Ur, L. Cranor, 2011. "Adchoices? Compliance With Online Behavioral Advertising Notice and Choice Requirements." Carnegie Mellon CyLab Technical Report CMU-Cylab-11-005. http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11005.html.

[33] P. Leon, B. Ur, R. Balebako, L. Cranor, R. Shay, and Y. Wang, 2011. "Why Johnny Can't Opt Out: A Usability Evaluation Of Tools To Limit Online Behavioral Advertising." Under Review. [Draft Available From The Authors].

[34] D. Chaum, 1983. "Blind Signatures For Untraceable Payments." Advances In Cryptology, 199-203. Plenum Press.

[35] D. Chaum 1985. "Security Without Identification: Transaction Systems To Make Big Brother Obsolete." Communications Of The ACM 28 (10), 1030-1044.

[36] R. Dingledine, N. Mathewson, and P. Syverson, 2004. "Tor: The Second-Generation Onion Router." Usenix Security Symposium, 13, 21.

[37] J.C. Benaloh, 1987. *Verifiable Secret-Ballot Elections*. Ph. D. Thesis, Yale University.

[38] J. Camenisch, J. and A. Lysyanskaya, 2001. "An Efficient System For Non-Transferable Anonymous Credentials With Optional Anonymity Revocation." Advances In Cryptology - Eurocrypt, 93-118. Springer-Verlag, Lncs 2045.

[39] E. Adar and B. Huberamn, 2001. "A Market For Secrets." First Monday 6, 200-209.

[40] J. Canny, 2002. "Collaborative Filtering With Privacy." IEEE Symposium On Security and Privacy, 45-57.

[41] C. Gentry, 2009. "Fully Homomorphic Encryption Using Ideal Lattices. ACM Symposium On Theory Of Computing, 169-178.

[42] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, S. Barocas, 2010. "Adnostic: Privacy Preserving Targeted Advertising." NDSS 2010.

[43] A. Acquisti, 2008. Identity Management, Privacy, and Price Discrimination. IEEE Security & Privacy, 46-50.

[44] G. Loewenstein and E. Haisley, 2008. "The Economist As Therapist: Methodological Ramifications Of 'Light' Paternalism." *Perspectives On The Future Of Economics: Positive and Normative Foundations*, A. Schotter & A. Caplin (Eds.).

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:]

Testimony of Pam Dixon Executive Director, World Privacy Forum

Before the Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce

What's a Consumer to Do? Consumer Perceptions and Expectations of Privacy Online

October 13, 2011

Chairman Mack, and Members of the Committee, thank you for the opportunity to testify today about consumers' expectations and perceptions of privacy online. My name is Pam Dixon, and I am the Executive Director of the World Privacy Forum. The World Privacy Forum is a 501(c)(3) non-partisan public interest research group based in California. Our funding is from foundation grants, cy pres awards, and individual donations. We focus on conducting in-depth research on emerging and contemporary privacy issues as well as on consumer education.

I have been conducting privacy-related research for more than ten years, first as a Research Fellow at the Denver University School of Law's Privacy Foundation where I researched privacy in the workplace and employment environment, as well as technology-related privacy issues such as online privacy. While a Fellow, I wrote the first longitudinal research study benchmarking data flows in employment online and offline, and how those flows impacted consumers.

After founding the World Privacy Forum, I wrote numerous privacy studies and commented on regulatory proposals impacting privacy as well as creating useful, practical education materials for consumers on a variety of privacy topics. In 2005 I discovered previously undocumented consumer harms related to identity theft in the medical sector. I coined a termed for this activity: medical identity theft. In 2006 I published a groundbreaking report introducing and documenting the topic of medical identity theft, and the report remains the definitive work in the area. In 2007 I coined and introduced the original Do Not Track idea. In 2010 I published the first report on privacy and digital signage networks.

Beyond my research work, I have published widely, including a 2011 reference book on online privacy (*Online Privacy*, ABC-CLIO) and seven books on technology issues with Random House, Peterson's and other large publishers, as well as more than one hundred

articles in newspapers, journals, and magazines.[1]

Today I will discuss consumer expectations of privacy online and the tremendous misperceptions and concomitant risks that exist for consumers. I will also discuss the features of past and current approaches that have allowed these problems to proliferate, with suggestions for remedies.

Online privacy is not just a theoretical exercise of academics and experts talking about potential risks that may someday occur. Privacy difficulties in the online world now readily leak over into the offline world with real consequences such as price discrimination, difficulty finding employment, problems with insurability, and sometimes just plain old embarrassment or social difficulties such as the loss of a friend. In some situations, misperceptions about what online privacy does and doesn't mean can lead to issues with personal finances, safety, and other aspects of well-being. As we documented in our 2010 report on digital signage, consumers' online activities now intersect with everyday activities in profound ways, including issues relating to facial recognition and identifiability.

I have observed that the regulatory conversation about what to do about online privacy often focuses on advertising, in particular behavioral advertising. This focus began in earnest in 1997 with the inception of the self-regulatory Network Advertising Initiative. The conversation continues today with a similar focus. There is an emphasis on self-regulatory efforts, and an emphasis on a narrow slice of privacy-related problems online.

We need to expand our privacy vocabulary and our thinking at this point. Online privacy includes advertising *and* it includes many other things now, including many other kinds of privacy risks from third parties. Online privacy risks include information leakage in many forms and varieties, and online privacy risks may be tied to offline behavior. Consumers simply do not know about these risks for the most part, and given the complexity of the online environment and the number and variety of privacy risks, I am not persuaded that consumer education can do enough quickly enough to be a viable stand-alone solution. I am also concerned that history indicates strongly that the current self-regulatory regimes will fail to adequately protect consumers from the privacy realities online.

In 2007 the World Privacy Forum held a meeting in Berkeley, California about online privacy. Our purpose was to find a collaborative way to have a broader, more accurate discussion about online privacy and to foster ideas about solutions to the existing problems that consumers face. We invited all of the leading privacy and consumer groups to the meeting. Most came. At that meeting, I proposed the Do Not Track idea, and I later wrote the original Do Not Track proposal collaboratively with the groups at the meeting

---

[1] Much of my privacy-related research work and writings are available at the World Privacy Forum web site, <http://www.worldprivacyforum.org>.

and submitted it to the FTC with signatories.[2] My idea behind Do Not Track was to provide consumers a way to opt out of the various forms of online and potentially offline tracking in one place. The idea was born from the knowledge of how deep the consumer misperceptions of online privacy protections are, and from the knowledge of just how challenging it is for consumers to truly manage their information online knowledgeably.

The World Privacy Forum believes that an approach that repeats the mistakes of past unsuccessful privacy protection efforts will replicate the same results. There needs to be a different approach. Later in this testimony, I will discuss potential ways forward in providing consumers with solutions to online privacy challenges. First, I would like to discuss the deep consumer misperceptions about online privacy that exist.

I. Consumer Expectations of Privacy: Deep Misperceptions About What is Happening Online and what is Protected ... or Not

Consumers' expectations of privacy online rarely match the reality of what is happening to their information. Consumers don't have the ability to see or understand the information that is being collected about them,[3] and they don't have the tools to see how that information is impacting the opportunities that are being offered – or denied – to them. Consumers also believe incorrectly that privacy icons and privacy policies offer more protection for them than they actually do.[4] This disconnect is due to an abundance of consumer misperceptions of what privacy really means as defined by actual industry practices today. It is also due to the reality that it is extremely challenging for individual consumers to have the skills and knowledge to fully understand the information privacy risks they can encounter online, much less navigate the risks.

We see this first hand. The World Privacy Forum receives consumer queries about online privacy issues, and we have for years. The consumer complaints we have received run the gamut. We have received calls from surprised, worried, and frustrated consumers who discovered their private medical information online, consumers who wanted to figure out how to stop Google Street View from displaying images of their backyard, people who were not able to exercise opt outs at data broker web sites, consumers who were upset and privacy changes on Facebook, and many more. What the complaints have in common

---

[2] Do Not Track, *Consumer Rights and Protections In the Behavioral Advertising Sector*, October 30, 2007, *available at*: http://www.worldprivacyforum.org/pdf/ConsumerProtections_FTC_ConsensusDoc_Final_s.pdf.

[3] See, for example, a new Carnegie-Mellon study on one aspect of consumer data collection, behaviorally targeted online ads. This study found that "many participants have a poor understanding of how Internet advertising works, do not understand the use of first-party cookies, let alone third-party cookies, did not realize that behavioral advertising already takes place, believe that their actions online are completely anonymous unless they are logged into a website, and believe that there are legal protections that prohibit companies from sharing information they collect online." Aleecia M. McDonald and Lorrie Faith Cranor, Carnegie Mellon University, *An Empirical Study of How People Perceive Online Behavioral Advertising*, Nov. 10, 2009.

[4] Chris Jay Hoofnagle and Jennifer King, Samuelson Law, Technology and Public Policy Clinic, University of California-Berkeley School of Law, *What Californians Understand About Privacy Offline*, May 15, 2008.

was the question at the end of the conversation, which in many variations simply stated: what can I do?

I wish we had better answers for them. We often don't, because of the lack of consumer protections or rights in this core area of life for so many digital citizens. The consumers who contact us are those who *know* they have a privacy problem. They are the fortunate ones. Far more consumers are simply not aware of the risks they face.

Most consumers are not aware that based on their activities, online data handlers can build extensive profiles about consumers' backgrounds and interests. Third-party cookies from one company alone—Google—can track users' browsing activity across much of the web and collect data such as clickstream, ad impression history and ad click history.[5] A single click on a website can reveal plentiful information about a consumer – current location[6], parenthood, education, income range, shopping habits, and more.[7] Using this information obtained by tracking consumers, data handlers can construct detailed profiles[8] about the consumers.[9] These profiles are sometimes linked to individuals' identities.[10]

I want to emphasize that consumer tracking and targeting goes beyond web browsers. This will be an important area of inquiry going forward as online information access moves beyond traditional Internet connectors such as laptop computers. Data handlers track consumers when they connect to the Internet through a variety of devices such as mobile phones, televisions and video game consoles. When the device is a mobile phone, the tethering of consumers' habits to their device can be quite personal because consumers carry it all the time, and because advertisers have employed identifiers for tracking that are hard coded into the telephone. Unlike standard web cookies, these tracking tools lack controls and cannot be deleted. Applications and services on the

---

[5] A clickstream is a list of URLs visited by the user; an ad impression history is a list of ads that have been displayed to the user; an ad click history is a list of all ads that the user has clicked on. *See* Vincent Toubiana et al., *Adnostic: Privacy Preserving Targeted Advertising*, at 4; *see also* UC Berkeley, School of Information, *KnowPrivacy,* June 1st, 2009, http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf "Google in particular had extensive coverage. It had a web bug on 92 of the top 100 sites, and on 88% of the total domains reported in the data set of almost 400,000 unique domains."

[6] *Beyond Voice Mapping the Mobile Marketplace*, at 15-16, Federal Trade Commission Staff Report, (April 2009), *available at:* http://www.ftc.gov/reports/mobilemarketplace/mobilemktgfinal.pdf. For example, when a consumer uses a location-based service — one of the widely used location-based applications is the mobile family and finder application that enables users to determine their family members' and friends' locations.

[7] Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J., Aug. 4, 2010, *available at:* http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html ("From a single click on a web site, [x+1] correctly identified Carrie Isaac as a young Colorado Springs parent who lives on about $50,000 a year, shop at Wal-Mart and rents kids' videos. The company deduced that Paul Boulifard, a Nashville architect, is childless, likes to travel and buys used cars. And [x+1] determined that Thomas Burney, a Colorado building contractor, is a skier with a college degree and looks like he has good credit.").

[8] A profile is a description of the user's interests inferred from the clickstream created by data handlers. *See* Vincent Toubiana et al., *Adnostic: Privacy Preserving Targeted Advertising*, at 4.

[9] Elli Androulaki & Steven Bellovin, *A Secure and Privacy-Preserving Targeted Ad-System*, at 1.

[10] Emily Steel, *A Web Pioneer Profiles Users by Name*, WALL ST. J., October 25, 2010.

mobile phone allow data handlers to access consumers' current physical location using GPS technology.[11] For example, Apple's iPhone kept a record of real-time location information even when location services were turned off.[12] Although the location data is "anonymous," the data reveals a lot of information about the user such as home address, work location and daily routines. Because the information is so specific and personal, anyone who has access to it can potentially work out the identity of the user.[13] Therefore, the location information is not truly "anonymous" and poses significant privacy risk.

The information that has been collected online can be used to make snap judgments about consumers. This practice often shapes the consumer's online experience. Some financial companies show entirely different pages to visitors based on assumptions made about consumers' income and education level.[14] For example, credit card companies may present a set of high interest rate but easy-to-qualify credit card offers to a visitor based on the web-history-based assumptions that the visitor has a bad credit history. The visitor may in fact have a good credit score and may simply be interested in high-reward credit cards. To date, no court has applied fair-lending laws to the practice of using web-browsing history to make lending decisions. A bank could choose not to send a lending offer, or to send a different offer, based upon an applicant's browsing history, such as visits to a gambling site.[15]

There are further areas of consumer misperceptions about online privacy. We have highlighted just a few examples:

- Consumers who think they are visiting a single web page may be surprised to learn that if they registered at a site, some parts of their information, including in some cases email addresses and usernames, may be flowing to an invisible (to them) array of third parties, including advertisers. A Stanford study revealed that websites studied were leaking usernames and user IDs to third parties such as Facebook,ComScore, Google Advertising (Doubleclick), and Quantcast, among other parties. The study found that viewing a local ad on the Home Depot web site sent the user's first name and email address to 13 companies, among other data leakage examples.[16]

---

[11] Ashkan Soltani, *Testimony of Ashkan Soltani Before the Senate Committee on Commerce, Science, and Transportation Hearing on The State of Online Consumer Privacy*, March 16, 2011, at 4-5.

[12] Jennifer Valentino-Devries, *IPhone Stored Location in Test Even if Disabled*, WALL ST. J, April 25, 2011, *available at:* http://online.wsj.com/article/SB10001424052748704123204576283580249161342.html.

[13] Eric Chabrow, *Apple, Google Under Fire at Hearing*, Government Information Security, (May 10, 2011), *available at:* http://www.govinfosecurity.com/articles.php?art_id=3623

[14] Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., (July 30, 2010), *available at:* http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

[15] Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J., (Aug. 4, 2010), *available at:* http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html.

[16] Jonathan Mayer, *Tracking the Trackers: Where Everybody Knows Your Username*, Stanford Law School Center for Internet and Society, October 11, 2011, *available at:* http://cyberlaw.stanford.edu/.

Advertising companies incentivize consumers to identify themselves online by giving them free offers or requests for registration. Once the consumers identify themselves on a website, the historically tracked non-personally identifiable information can be merged with the personally identifiable information.[17] Unfortunately, this choice of "re-identification" is not always voluntary, as identifiable information can be leaked to third-party data handlers. For example, when a consumer makes purchase online, the merchant can share the consumer's email address, collected through the billing process, with a third party that was present on the purchase page.[18]

- A Wall Street Journal article revealed an online tracking company called RapLeaf collected information from social networking profiles and matched it with email addresses in order to link consumers' real world identities. In fact, RapLeaf admits that in addition to tracking consumers online, it also collected names and used the Facebook ID in compiling its database of consumer profiles. RapLeaf gathered and sold very specific information about individuals. The Journal uncovered that RapLeaf segmented people into more than 400 categories, such as income range, political leaning, religion, and interest in adult entertainment.[19]

- People who typed search queries to the AOL search bar had no idea that their search queries would be made public. In 2006, AOL released a compressed text file containing search keywords from users. Although AOL did not identify specific users in its report, individuals could still be identified and matched to their search history by the bits of disconnected personally identifiable information in the aggregated search queries. The New York Times was able to locate and interview an individual from the search records by cross-referencing the search data with publicly available phonebook listings.[20] If an individual can be identified using AOL search queries alone, companies or data handlers can similarly identify an individual by name using similar kinds of online behavioral information.

- Consumers may not realize that data handlers can gather information such as medical conditions, finances or sexual orientation indiscriminately. One Wall Street Journal article describes a high school graduate who often does online

---

[17] *Online Profiling: A Report to Congress*, at 4, Federal Trade Commission, (June 2000), *available at:* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf ("For example, a network advertising company could operate its own Web site at which consumers are asked to provide personal information. When consumers do so, their personal information could be linked to the identification number of the cookie placed on their computer by that company, thereby making all of the data collected through that cookie personally identifiable.").

[18] Ashkan Soltani, *Testimony of Ashkan Soltani Before the Senate Committee on Commerce, Science, and Transportation Hearing on The State of Online Consumer Privacy*, at 3-4, (March 16, 2011).

[19] Emily Steel, *A Web Pioneer Profiles Users by Name*, WALL ST. J., (October 25, 2010).

[20] Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N. Y. TIMES, (August 9, 2006), *available at:* http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482.

research about weight loss.[21] The high school graduate sees weight-loss ads every time she goes on the Internet. "I'm self-conscious about my weight," she said. "I try not to think about it . . . Then the ads make me start thinking about it." There are technical steps this young woman could take to get rid of the ads, such as using the Mozilla web browser with an adblocking plug in. How many consumers know about such technologies? Did she?

II. Consumer Want Privacy Protection – But Misperceive Actual Protections

Consumers do want privacy protection. Surveys have indicated that people value privacy even when it is contrasted with other social or personal interests.[22] Most Americans do not want marketers to tailor advertisements to their interests.[23] Americans' rejection of even anonymous behavioral targeting indicates that they do not believe that the collected data will remain disconnected from their PII.[24] Research has unambiguously shown that consumers want to control and shape their online experience, and that they are worried about other uses of their data in ways they do not know or understand, and might not like.[25]

Consumers feel uneasy about online tracking. In 2000, a study found that 67% of individuals were "not at all comfortable" if a Website shared their information so they could be tracked on multiple Websites. The same study reveals that 63% of individuals were "not very comfortable" or "not at all comfortable" when a website tracked their movements when they browsed the site, even if those data are not tied to their names or real-world identities.

Another study in 2000 found that consumers would spend a total of $6 billion more per year online if they did not feel that their privacy was at stake every time they made a transaction online. A 2007 study found that consumers are willing to pay approximately 60 cents more per fifteen-dollar spent to protect their privacy online.

These consumer expectations are clear: consumers want online privacy. But the problem is that consumer expectations are not aligned correctly with what protections are available and what privacy indicators mean.

---

[21] Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., (July 30, 2010), *available at:* http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

[22] Priscilla Regan, *Legislating privacy: Technology, social values, and public policy*, at 177, Chapel Hill, U.S., The University of North Carolina Press.

[23] Joseph Turow et al., *Americans Reject Tailored Advertising*, at 3, (September 2009), *available at:* http://ssrn.com/abstract=1478214. 66% of adult Americans do not want marketers to tailor advertisements to their interests. When Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages, between 73% and 86%, say they would not want such advertising.

[24] Joseph Turow et al., *Americans Reject Tailored Advertising*, at 4, (September 2009), *available at:* http://ssrn.com/abstract=1478214.

[25] Joseph Turow et al., *Americans Reject Tailored Advertising*, at 4-5, (September 2009), *available at:* http://ssrn.com/abstract=1478214.

A groundbreaking 2008 study on what consumers understood about privacy online revealed that a majority of California consumers who see privacy policies on a web site overvalue the protections the privacy policy offers in multiple ways. For example, respondents believed that privacy policies create a right for deletion of data upon request. Online shoppers believed that online privacy policies prohibited third-party information sharing.[26] Additional studies have backed up these findings of consumers over-estimating privacy protections.[27]

Given the disparity between what is actually happening online and what consumers believe is protected, it is no surprise that consumers do not take affirmative action to protect themselves. Every person who uses the Internet is not necessarily technologically skilled or a privacy expert. Even with such expertise, the reality is that the solutions that are available to most consumers are limited.

III. Lessons from History: Correcting the Course of Consumer Protection

The World Privacy Forum supports consumer-protective legislation in the area of online privacy. We note that if self-regulation is going to be the course of action, it is absolutely critical to construct self-regulation differently than it has been done in the past. In 2007, the World Privacy Forum (WPF) issued a report on the National Advertising Initiative's early efforts at business-operated self-regulation for privacy. The report was *The NAI: Failing at Consumer Protection and at Self-Regulation.*[28] In 2010, the World Privacy Forum issued a report on privacy activities of the Department of Commerce, *The US Department of Commerce and International Privacy Activities: Indifference and Neglect.*[29] Tomorrow we will be publishing a new report on the history of privacy self-regulation, which we include in this testimony today. Next week, we are publishing a detailed analysis of the Digital Advertising Alliances' self-regulatory program, a report that we prepared in collaboration with the Samuelson Law, Technology & Public Policy Clinic at the University of California, Berkeley School of Law.

We can summarize what we have learned from our work. Privacy self-regulation in the past has been a Potemkin Village of privacy protection. The self-regulatory privacy programs appear when there is a threat of legislation, then they disappear when the eye of the regulatory storm passes by. The programs look good from a distance, but upon closer inspection they offer no substantive consumer privacy protections.

---

[26] Chris Jay Hoofnagle, Jennifer King, *What Californians Understand About Privacy Online*, September 3, 2008.

[27] *See* 2. *See also* Joseph Turow, *Americans and Online Privacy, The System is Broken*, Annenberg Public Policy Center (June 2003), *available at*: http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf.

[28] http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf (last visited 10/12/11).

[29] http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf (last visited 10/12/11).

If privacy self-regulation is undertaken in the same way it has been in the past, history indicates those efforts will fail. Self-regulation created by industry, for industry, and then policed by industry has a very poor track record.

Consider these past industry self-regulatory privacy programs, of which only one is in existence today:

- The **Individual Reference Services Group** was announced in 1997 as a self-regulatory organization for companies providing information that identifies or locates individuals. The group terminated in 2001, deceptively citing a recently-passed regulatory law as making the group's self-regulation unnecessary. However, that law did not cover IRSG companies.

- The **Privacy Leadership Initiative** began in 2000 to promote self-regulation and to support privacy educational activities for business and for consumers. The organization lasted about two years.

- The **Online Privacy Alliance** began in 1998 with an interest in promoting industry self-regulation for privacy. OPA's last reported substantive activity appears to have taken place in 2001, although its website continues to exist and shows signs of an update in 2011, when FTC and congressional interest recurred. The group does not accept new members.[30]

- The **Network Advertising Initiative** had its origins in 1999, when the Federal Trade Commission showed interest in the privacy effects of online behavioral targeting. By 2003, when FTC interest in privacy regulation had diminished, the NAI had only two members. Enforcement and audit activity lapsed as well. NAI did not fulfill its promises or keep its standards up to date with current technology until 2008, when FTC interest increased.

- The **BBBOnline Privacy Program** began in 1998, with a substantive operation that included verification, monitoring and review, consumer dispute resolution, a compliance seal, enforcement mechanisms and an educational component. Several hundred companies participated in the early years, but interest did not continue and BBBOnline stopped accepting applications in 2007. The program has now disappeared.

The self-regulatory programs advanced by the industry can be thought of as quasi-contracts with consumers. Lawmakers permit the industry to continue its profitable enterprise of Online Consumer Tracking and Profiling without strict legal oversight and consumers are supposed to get a level of privacy in return. In today's terms, the sets of self-regulatory principles advanced for example by the Network Advertising Initiative

[30] http://www.privacyalliance.org/join/. (Last visited October 12, 2011.)

and the Digital Advertising Alliance are the terms. The analysis the World Privacy Forum has conducted indicates that the terms are lacking and consumers are not getting a fair bargain.

IV. Going Forward

In our report on the history of self-regulation, we discuss ideas for doing things differently, in a way that will work to correct the mistakes of the past. These ideas include:

- **Tension in the Process:** Successful privacy self-regulation requires standards responsive to the actual problems, robust policies, meaningful enforcement, and effective remedies. Privacy self-regulation of industry, by industry, and for industry will not succeed. Tension in self-regulation can be provided by a defined and permanent role for consumers who are the intended beneficiaries of privacy protection. Government may also be able to play a role, but government cannot be relied upon as the sole overseer of the process. The past has shown that the interest of the FTC waxed and waned with the political cycle, and the Department of Commerce did not provide sufficient oversight.

- **Scope:** The scope of a self-regulatory regime must be clearly defined at the start. It must apply to a reasonable segment of industry, and it must attract a reasonable percentage of the industry as participants. There must be a method to assess the penetration of the self-regulatory regime in the defined industry.

- **Fair Information Practices:** Any self-regulatory regime should be based on Fair Information Practices (FIPs). Implementation of FIPs will vary with the industry and circumstances, but all elements of FIPs should be addressed in some reasonable fashion.

- **Open Public Process:** The development of basic policies and enforcement methods should take place to a reasonable degree in a public process open to every relevant perspective. The process for development of privacy self-regulatory standards should have a reasonable degree of openness, and there should be a full opportunity for public comment before any material decisions become permanent. Consumers must be able to select their own representatives. Neither government nor those who are to be regulated should select consumer participants – the selection should be up to the consumers.

- **Independence:** The organization that operates a privacy self-regulatory system needs to have some independence from those who are subject to the self-regulation. Those who commit to comply with privacy self-regulation must make a public commitment to comply for a term of years and a financial commitment for that entire period.

- **Benchmarks:** Past self-regulatory efforts and codes of conduct lack benchmarks for success. What constitutes success? Is it membership? Market share? Is it actual enforcement of the program? Without specific benchmarks for a privacy program, it is much more difficult to gauge success in real-time. Without the ability to accurately assess activities within a current program, both success and failure are more difficult to ascertain and may only be gleaned in hindsight.

Another evaluative tool exists. The United Kingdom-based National Consumer Council ("NCC") published a checklist for self-regulatory schemes in 2000 that provides a starting point to discuss what the industry principles should contain.[31] The checklist provides the following requirement for a "credible" self-regulatory scheme:

1. The scheme must be able to command **public confidence**.

2. There must be strong **external consultation and involvement** with all relevant stakeholders in the design and operation of the scheme.

3. As far as practicable, the operation and control of the scheme should be **separate** from the institutions of the industry.

4. Consumer, public interest and other **independent representatives must be fully represented** (if possible, up to 75 per cent or more) on the governing bodies of self-regulatory schemes.

5. The scheme must be based on **clear and intelligible statements of principle** and **measurable standards** – usually in a Code – which address **real consumer concerns**. The objectives must be rooted in the reasons for intervention [].

6. The rules should **identify the intended outcomes**.

7. There must be clear, accessible and **well-publicised - complaints procedures** where breach of the code is alleged.

8. There must be adequate, meaningful and commercially significant **sanctions** for non-observance.

9. **Compliance must be monitored** (for example through complaints, research and compliance letters from chief executives).

10. **Performance indicators** must be developed, implemented and published to measure the scheme's effectiveness.

---

[31] *See* National Consumer Council, *Models of self-regulation: An overview of models in business and the professions* 51-52 (November 2000), *available at:* http://www.talkingcure.co.uk/articles/ncc_models_self_regulation.pdf.

11. There must be a degree of **public accountability**, such as an Annual Report.

12. The scheme must be **well publicised**, with maximum education and information directed at consumers and traders.

13. The scheme must have **adequate resources** and be funded in such a way that the objectives are not compromised.

14. **Independence** is vital in any redress scheme which includes the resolution of disputes between traders and consumers.

15. The scheme must be regularly reviewed and **updated** in light of changing circumstances and expectations.[32]

V. Conclusion

Consumers no longer have the option of simply living in an opt-out village[33] and avoiding going online to conduct the business of their daily lives. That is not a realistic choice anymore. Given the deep lack of understanding about the complexity and pervasiveness and impact of online privacy web leakage and tracking, consumers need practical options about how to handle their information privacy online and off. Consumer misperception about what and when privacy protective mechanisms are in force complicates matters further. If consumers knew the risks, they would have more opportunity to change behaviors. If consumers understood actual privacy protections, they may make different choices about information sharing.

Currently, no substantial protections are available for consumers. Most privacy self-regulatory schemes that have been produced thus far have many defects. The current online self-regulatory programs have many of the characteristics of past self-regulatory programs that eventually disappeared altogether. If Congress is to avoid a Potemkin Village of consumer protection, the path forward will need to include a very new and fresh approach to the issue of consumer protection.

We support legislation, but if faced with a situation where there is no legislation, then we urge Congress to look deeply at the flaws of past self-regulatory efforts and do things differently this time. We urge Congress to look at the deeper question facing online privacy today: what can we do differently that will give consumers a better result?

---

[32] National Consumer Council, *Models of self-regulation: An overview of models in business and the professions* 51-52 (November 2000), *available at* http://www.talkingcure.co.uk/articles/ncc_models_self_regulation.pdf (emphasis in original).

[33] The idea of the "Opt Out Village" arises from a video spoof on privacy published by the Onion. Google Opt Out Feature Lets Users Protect Privacy by Moving to Remote Village, The Onion, < http://www.theonion.com/video/google-opt-out-feature-lets-users-protect-privacy,14358/ >.

Thank you for your invitation to testify and your attention today.

Respectfully submitted,

Pam Dixon

Attachment:

Many Failures: A Brief History of Privacy Self-Regulation in the United States, Robert Gellman & Pam Dixon, World Privacy Forum, October 14, 2011.

World Privacy Forum

Many Failures: A Brief History of Privacy Self-Regulation in the United States

Robert Gellman & Pam Dixon

October 14, 2011

Brief Summary of Report

Efforts to create self-regulatory, or voluntary, guidelines in the area of privacy began in 1997. Privacy self-regulation was promoted at the time as a solution to consumer privacy challenges. This report reviews the leading efforts of the first self-regulatory wave from 1997 to 2007, and includes a review of the life span, policies, and activities of the Individual Reference Services Group, Privacy Leadership Initiative, Online Privacy Alliance, Network Advertising Initiative, BBBOnline Privacy Program, US-EU Safe Harbor Framework, Children's Online Privacy Protection Act, and the Platform for Privacy Preferences. A key finding of this report is that the majority of the industry self-regulatory programs that were initiated failed in one or more substantive ways, for example, many have disappeared. The report concludes with a discussion of possible reforms for the process for example, a defined and permanent role for consumers, independence, setting benchmarks, and other safeguards.

About the Authors

Robert Gellman is a privacy and information policy consultant in Washington DC. (www.bobgellman.com.) Pam Dixon is the Executive Director of the World Privacy Forum. Gellman and Dixon are the authors of *Online Privacy A Reference Handbook* (ABC CLIO, 2011.)

About the World Privacy Forum

The World Privacy Forum is a non-profit consumer education and public interest research group. It focuses on a range of privacy matters, including financial, medical, employment and online privacy. The World Privacy Forum was founded in 2003. www.worldprivacyforum.org.

I. Introduction and Summary

Current online privacy debates focus on respecting the privacy interests of Internet users while accommodating business needs. Formal and informal proposals for improving consumer privacy offer different ideas for privacy *regulation* and privacy *self-regulation,* sometimes called *codes of conduct.*[34] Some in the Internet industry continue to advance or support ideas for privacy self-regulation. Many of these same players proposed and implemented privacy self-regulatory schemes that started in the late 1990s.

Missing from current debates on self-regulation in the online privacy arena is a basic awareness of what happened with the first round of industry self-regulation for privacy. Also missing are the lessons that that should have been learned from the failures of past privacy self-regulatory efforts.

This report reviews the history of the leading efforts that comprised that early wave of privacy self-regulation, which occurred from 1997 to about 2007. One purpose of this report is to document the facts about that first wave of self-regulation. The other purpose of this report is to inform current discussions about the recent past. A key finding of this report is that the majority of the industry self-regulatory organizations that were initiated have now disappeared. The disappearance of a self-regulatory organization constitutes a failure of the self-regulatory scheme.

This is not the first World Privacy Forum report on privacy self-regulation. In 2007, the World Privacy Forum (WPF) issued a report on the National Advertising Initiative's early efforts at business-operated self-regulation for privacy. The report was *The NAI: Failing at Consumer Protection and at Self-Regulation.*[35] In 2010, the WPF issued a report on privacy activities of the Department of Commerce, *The US Department of Commerce and International Privacy Activities: Indifference and Neglect.*[36] The Commerce report reviewed in some detail the government supervised self-regulatory Safe Harbor Framework for personal data exported from Europe to the US. Unlike most other privacy self-regulatory efforts, the Safe Harbor Framework continues to exist, largely because of the government role. But the Safe Harbor Framework is deficient in enforcement and some other areas, and it cannot be counted as successful.

The privacy self-regulation programs reviewed in this report were effectively a Potemkin Village of privacy protection. Erected quickly, the schemes were designed to look good from a distance. Upon closer inspection, however, the protections

---

[34] This report uses *self-regulation* instead of the term *codes of conduct.*
[35] http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf (last visited 9/20/11).
[36] http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf (last visited 9/20/11).

offered were just a veneer. The privacy Potemkin Village fell down soon after the gaze of potential regulators drifted elsewhere. Efforts such as the Individual Reference Service Group (IRSG) and the National Advertising Initiative (NAI) are examples of classic, failed privacy self-regulatory efforts. These and other poorly designed privacy self-regulation schemes had limited market penetration and insufficient enforcement. Still, that was enough to fend off regulators until political winds blew in other directions.

Many participants to the debate are new to the issue and are unaware of recent history. Even the Federal Trade Commission has a short memory. The FTC appeared to acknowledge the limits of self-regulation when, it concluded in 2000 that self-regulatory programs fell "well short of the meaningful broad-based privacy protections the Commission was seeking and that consumers want."[37] But in 2010, a staff report from the FTC continued to show support for self-regulation as an alternative to legislation, seemingly ignoring the Commission's own experience from ten years earlier.[38] The pressure to believe that "this time, things will be different" remains significant. This belief is fueled by industry pressure, industry desire for no formal regulation, a continually shifting political environment, and the absence of meaningful rulemaking authority at the Federal Trade Commission.

This report offers a simple and clear history lesson. Industry self-regulation for privacy as it has been done in the past has failed. Past industry self-regulatory programs for privacy have lacked credibility, sincerity, and staying power. This report does not propose a new model for self-regulation, but it does conclude with some suggestions for a different approach that is based on a a defined role for consumers, more transparency, better definitions, and firmer commitments by those subject to self-regulation.[39]

---

[37] See Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report To Congress* 35 (2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited 9/20/11).

[38] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers* (Preliminary Staff Report 2010) at 66, http://ftc.gov/os/2010/12/101201privacyreport.pdf, (last visited 9/20/11) ("Such a universal [Do Not Track] mechanism could be accomplished by legislation or potentially through robust, enforceable self-regulation.")

[39] The National Consumer Council (UK) published a checklist for self-regulatory schemes in 2000 that remains worthy of attention. *Models of self-regulation: An overview of models in business and the professions* 51-52 (November 2000), *available at:* http://www.talkingcure.co.uk/articles/ncc_models_self_regulation.pdf (last visited 9/21/2011). The checklist offers the following requirements for a "credible" self-regulatory scheme: 1. The scheme must be able to command **public** confidence. 2. There must be strong external consultation and involvement with all relevant stakeholders in the design and operation of the scheme. 3. As far as practicable, the operation and control of the scheme should be separate from the institutions of the industry. 4. Consumer, public interest and other independent representatives must be fully represented (if possible, up to 75 per cent or more) on the governing bodies of self-regulatory

It is beyond the scope of this report to consider whether the public's demands for greater privacy protections should be met with legislation, self-help mechanisms, some yet untested form of activity (regulatory, co-regulatory, or otherwise), or nothing at all.[40] This report is offered as a resource to help those who are debating these questions today.

Characteristics Common to Privacy Self-Regulation

This report reviews early industry self-regulatory activities for privacy during the years just before and after 2000. This period was the high watermark for privacy self-regulation. This report distinguishes between industry efforts at self-regulation, and government efforts. For most industry-supported self-regulatory efforts for privacy, a clear pattern developed in the years covered by this review. Feeling pressure from Federal Trade Commission scrutiny and from legislative interest, industry self-regulatory efforts for privacy developed quickly in an attempt to avoid any formal regulation. It can be observed that the self-regulatory activities typically were characterized by some or most of the following qualities:

- Self-regulatory organizations were most often based in Washington, D.C, where potential regulators are.
- Self-regulatory organizations formulated their rules in secret, typically with no input from non-industry stakeholders.
- The governing boards of privacy self-regulatory organizations typically had no non-industry board members of these groups. There were typically few or no consumer representatives.

---

schemes. 5. The scheme must be based on clear and intelligible statements of principle and measurable standards – usually in a Code – which address real consumer concerns. The objectives must be rooted in the reasons for intervention . 6. The rules should identify the intended outcomes. 7. There must be clear, accessible and well-publicised - complaints procedures where breach of the code is alleged. 8. There must be adequate, meaningful and commercially significant sanctions for non-observance. 9. Compliance must be monitored (for example through complaints, research and compliance letters from chief executives). 10. Performance indicators must be developed, implemented and published to measure the scheme's effectiveness. 11. There must be a degree of public accountability, such as an Annual Report. 12. The scheme must be well publicised, with maximum education and information directed at consumers and traders. 13. The scheme must have adequate resources and be funded in such a way that the objectives are not compromised. 14. Independence is vital in any redress scheme which includes the resolution of disputes between traders and consumers. 15. The scheme must be regularly reviewed and updated in light of changing circumstances and expectations.

[40] For a thoughtful discussion of self-regulation and analysis of alternatives, see Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S A Journal of Law and Policy for the Information Society 356 (2011), available at http://www.is-journal.org/hotworks/rubinstein.php (last visited 9/20/11).

- Privacy self-regulatory rules covered only a fraction of an industry or covered an industry subgroup, leaving many relevant business practices and many players untouched.

- Privacy self-regulation organizations were short-lived, typically surviving for a few years, and then diminishing or disappearing entirely when pressure faded.

- Privacy self-regulation organizations were loudly promoted despite their limited scope and substance.

- Privacy self-regulation organizations were structurally weak, lacking meaningful ability to enforce their own rules or maintain memberships. Those who subscribed to self-regulation were usually free to drop out at any time.

- Privacy self-regulation organizations were typically underfunded, and industry financial support in some cases appeared to dry up quickly. There was no long-term plan for survival or transition.

Not all of these characteristics were present in government supervised self-regulatory efforts, although those efforts were not necessarily any more successful.

Summary of Privacy Self-Regulatory History

Self-regulatory efforts do not fall neatly into narrow categories. However, some generalizations may be made that efforts fell into two broad categories, industry-supported and government-supported. One exception exists that is a mix of government, civil society, industry, and academia.

Industry-Supported Self-Regulatory Programs

The early **industry-supported** privacy self-regulatory efforts included:

• The **Individual Reference Services Group** was announced in 1997 as a self-regulatory organization for companies providing information that identifies or locates individuals. The group terminated in 2001, deceptively citing a recently-passed regulatory law as making the group's self-regulation unnecessary. However, that law did not cover IRSG companies.

• The **Privacy Leadership Initiative** began in 2000 to promote self-regulation and to support privacy educational activities for business and for consumers. The organization lasted about two years.

• The **Online Privacy Alliance** began in 1998 with an interest in promoting industry self-regulation for privacy. OPA's last reported substantive activity appears to have taken place in 2001, although its website continues to exist and shows signs of an update in 2011, when FTC and congressional interest recurred. The group does not accept new members.[41]

• The **Network Advertising Initiative** had its origins in 1999, when the Federal Trade Commission showed interest in the privacy effects of online behavioral targeting. By 2003, when FTC interest in privacy regulation had diminished, the NAI had only two members. Enforcement and audit activity lapsed as well. NAI did not fulfill its promises or keep its standards up to date with current technology until 2008, when FTC interest increased.[42]

• The **BBBOnline Privacy Program** began in 1998, with a substantive operation that included verification, monitoring and review, consumer dispute resolution, a compliance seal, enforcement mechanisms and an educational component. Several hundred companies participated in the early years, but interest did not continue and BBBOnline stopped accepting applications in 2007. The program has now disappeared.

Government-Supported Self-Regulatory Efforts

Not all privacy self-regulatory efforts were solely industry supported. Some were government sponsored in some manner, and there is one effort that involved consumers, academics, public interest groups as well as industry. These efforts included:

• The **US-EU Safe Harbor Framework** began in 2000 to ease the export of data from Europe to US companies that self-certified compliance with specified Safe Harbor standards. Three studies have documented that compliance was spotty, with many and perhaps most companies claiming to be in the Safe Harbor not meeting the requirements. The Department of Commerce continues to run the program but has undertaken negligible oversight or enforcement. Thus, the Safe Harbor Framework is a form of government-supervised self-regulation but with little evidence of active supervision. Some EU data protection authorities recently rejected reliance on the Safe Harbor framework because of its lack of reliability.

• The **Children's Online Privacy Protection Act** (COPPA), which passed in 1998, involves both legislation and self-regulation. It is

---

[41] http://www.privacyalliance.org/join/. (Last visited October 12, 2011.)
[42] This report evaluates the original NAI self-regulatory program that existed until 2007/2008.

technically a form of government-supervised self-regulation. The COPPA law provides for a safe harbor provision[43] that is sometimes cited as a self-regulatory program. Industry participation in the COPPA safe harbor program is not widespread. Under COPPA, the same statutory standards apply whether a business is in the COPPA safe harbor program or not.

Combination Self-Regulatory Efforts

• The **Platform for Privacy Preferences Project** (P3P) is a standard for communicating the privacy policies of a website to those who use the website. A user can retrieve a standardized machine-readable privacy policy from a website and use the information to make a decision about how to interact with the website. Sponsors presented a prototype at an FTC Workshop in 1997, and the first formal technical specification came in 2000. Major web browsers still support P3P in part, and there is some usage by websites. A 2010 study found that there are widespread errors in implementation of P3P requirements and that large numbers of websites that use P3P compact policies are misrepresenting their privacy practices, misleading users and making the privacy protection tools ineffective.

This report does not aim to be comprehensive. We have limited the scope to the early, leading efforts. Some privacy self-regulatory efforts developed or revived more recently.[44] The Network Advertising Initiative began in 1999 and nearly disappeared a few years later. NAI revived around 2008, when FTC interest in online privacy reawakened, and industry felt threatened once again by regulation and legislation. This report discusses the early iteration of the NAI. The NAI issued a new set of self-regulatory principles in 2008, and membership increased. The revival of NAI follows the earlier pattern so far. Because the new NAI effort is still underway, this report does not attempt to evaluate the NAI's post-1998 efforts. The new NAI looks a lot like the old NAI, however. Also not reviewed in this report is TRUSTe.[45]

---

[43] 15 U.S.C. §§ 6501-6506.

[44] The Digital Advertising Alliance self-regulatory program is not analyzed in this report, as it was launched in July 2009 and falls out of range of this study. *See* http://www.aboutads.info (last visited 9/21/11).

[45] TRUSTe, a privacy seal that continues to exist, became a for-profit company in 2008. Saul Hansell, *Will the Profit Motive Undermine Trust in Truste?*, New York Times (July 15, 2008), http://bits.blogs.nytimes.com/2008/07/15/will-profit-motive-undermine-trust-in-truste (last visited 2/14/11). TRUSTe has morphed significantly in its scope, purpose, and composition during its lifetime, and as such requires a separate discussion. TRUSTe is discussed in this report in the context of the first iteration of the NAI program and in the context of P3P. For more on TRUSTe see also Ben Edelman, *Certifications and Site Trustworthiness* (Sept. 25, 2006), http://www.benedelman.org/news/092506-1.html (last visited 2/14/11) ("Of the

II. Discussion: Industry-Supported Self-Regulatory Programs for Privacy

This section offers a historical review of privacy self-regulation that occurred in the years just before and just after 2000. For a variety of reasons, it is not necessarily fully comprehensive. Some self-regulatory efforts may have disappeared without a trace. Activities within existing trade associations are difficult or impossible to assess from evidence available to those outside the associations. However, this discussion captures the leading organizations of the time. [46]

This review does not generally attempt to complete a comprehensive analysis of the quality of each self-regulatory effort. The standards promulgated by the self-regulatory programs were often general and quickly became outdated because of technology and other changes. It appears that audits or reviews of compliance with self-regulatory standards were often not attempted, not completed, not credible, or not transparent. Finding original documents is often difficult or impossible now. However, there is enough available information to describe the programs, their rise, their activities, and in some cases, their demise.

Individual Reference Services Group

The creation of the Individual Reference Services Group (IRSG) was announced in June 1997 at a workshop held by the Federal Trade Commission.[47] According to a document filed with the FTC, the group consisted of companies that offered individual reference services that provided information that identifies or locates

---

sites certified by TRUSTe, 5.4% are untrustworthy according to SiteAdvisor's data, compared with just 2.5% untrustworthy sites in the rest of the ISP's list. So TRUSTe-certified sites are more than twice as likely to be untrustworthy."]. See also the discussion of the Platform for Privacy Preferences (P3P) later in this document for a reference to numerous TRUSTe certified websites that had errors in implementation of P3P requirements.

[46] Also, privacy seal programs arose during the period of this review, but some disappeared entirely. None beyond BBBOnline and TRUSTe developed sufficient credibility, reliability, or public recognition to warrant investigation in this report.

[47] Federal Trade Commission, *Individual Reference Services, A Report to Congress* (1997), http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm (last visited 9/20/11).

individuals.[48] The IRSG reported fourteen "leading information industry companies" as members, including US Search.com, Acxiom, Equifax, Experian, Trans Union, and Lexis-Nexis.[49]

The IRSG described its self-regulatory activities in this manner:

> The core of the IRSG's self-regulatory effort is the self-imposed restriction on use and dissemination of non-public information about individuals in their personal (not business) capacity. In addition, IRSG members who supply non-public information to other individual reference services will provide such information only to companies that adopt or comply with the principles. The principles define the measures that IRSG members will take to protect against the misuse of this type of information. The restrictions on the use of non-public information are based on three possible types of distribution that the services provide.[50]

A principal purpose of the IRSG plan appeared to be to avoid any real regulation. It was successful in achieving that goal. In its 1999 report to Congress, the FTC recommended that the industry be left to regulate itself despite some *significant shortcomings*:

> A. Recommendations Regarding the IRSG Principles
>
> The Commission recommends that the IRSG Group be given the opportunity to demonstrate the viability of the IRSG Principles.
>
> The present challenge is to protect consumers from threats to their psychological, financial, and physical well-being while preserving the free flow of truthful information and other important benefits of individual reference services. The Commission commends the initiative and concern on the part of the industry members who drafted and agreed to the IRSG Principles, an innovative and far-reaching self-regulatory program. The Principles address most concerns associated with the increased availability of non-public information through individual reference services. With the promising compliance assurance program, the Principles should substantially lessen the risk that information made available through the services is misused, and should address consumers' concerns about the privacy of non-public information in the services' databases. Therefore, the Commission recommends that the IRSG Group be given the opportunity to demonstrate the viability of the IRSG Principles. ***

---

[48] Individual Reference Services Group, Industry Principles — Commentary (Dec. 15, 1997), http://www.ftc.gov/os/1997/12/irsappe.pdf (last visited 9/20/11).
[49] http://web.archive.org/web/19990125100333/http://www.irsg.org (last visited 9/20/11).
[50] Id.

> The Commission looks to industry members to determine whether errors in the transmission, transcription, or compilation of public records and other publicly available information are sufficiently infrequent as to warrant no further controls.
> While the Commission believes the IRSG Principles address most areas of concern, certain issues remain unresolved. Most notably, the Principles fail to provide individuals with a means to access the public records and other publicly available information that individual reference services maintain about them. Thus, individuals cannot determine whether their records reflect inaccuracies caused during the transmission, transcription, or compilation of such information. The Commission believes that this shortcoming may be significant, yet recognizes that the precise extent of these types of inaccuracies and associated harm has not been established. An objective analysis could help resolve this issue. The IRSG Group has acknowledged the Commission's position, and has demonstrated its awareness of this problem by (1) stating that it will seriously consider conducting a study of this issue and (2) agreeing to revisit the issue in eighteen months. The Commission looks to industry members to undertake the necessary measures to establish whether inaccuracies and associated harm resulting from errors in the transmission, transcription, or compilation of public records and other publicly available information are sufficiently infrequent as to warrant no further controls.[51]

One of the IRSG principles called for an annual "assurance review" for compliance with IRSG standards.[52] The IRSG also required that a summary of the report and any subsequent actions taken be publicly available. While the IRSG website contains some evidence that at least some IRSG members conducted reviews, the IRSG did not make the reports public on its website so it is not possible to determine whether the reviews were properly conducted, comprehensive, or otherwise meaningful.[53]

Once the threat of regulation evaporated or diminished, the IRSG continued in existence for a few years. In September 2001, approximately four years after it was

---

[51] Federal Trade Commission, *Individual Reference Services, A Report to Congress* (1997) (Commission Recommendations), http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm (last visited 9/20/11).

[52] http://web.archive.org/web/20020210151622/www.irsg.org/html/3rd_party_assessments.htm (last visited 9/20/11).

[53] See http://web.archive.org/web/20020215163015/www.irsg.org/html/irsg_assessment_letters--2000.htm (last visited 9/20/11). Whether the reports were made public in other ways has not been explored.

established, the IRSG announced its termination.[54] The stated reason was that legislation made the self-regulatory principles no longer necessary.

> "We are operating in a much different regulatory environment than we were when the IRSG was created in 1997," said Ron Plesser with Piper Marbury Rudnick & Wolfe LLP, whose firm represents the IRSG. "It doesn't make sense to maintain a self-regulatory program when this information is now regulated under the Gramm-Leach-Bliley Act."[55]

However, the legislation cited as the reason for termination (The Gramm-Leach-Bliley Act) *did not in fact regulate IRSG members.* The Gramm-Leach-Bliley (GLB) Act provided that each *financial institution* has an "affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[56] A financial institution is a company that offers financial products or services to individuals, like loans, financial or investment advice, or insurance.[57] The IRSG companies – companies that provide information that *identifies* or *locates* individuals – are not financial institutions under GLB. It is also noteworthy that GLB became law almost two years before it was cited as the reason for the end of the IRSG. GLB was a fig leaf that covered the lack of continuing industry support for the IRSG.

Why did the IRSG issue a deceptive statement about the reason for its termination? According to reports current at the time, the members of IRSG lost interest in supporting an expensive self-regulatory organization because they no longer felt threatened by legislation or regulatory activities.

The IRSG.org website is now owned by a link farm.[58]

The Privacy Leadership Initiative

A group of industry executives with members including IBM, Procter & Gamble, Ford, Compaq, and AT&T established the Privacy Leadership Initiative (PLI) in June

---

[54] http://web.archive.org/web/20020202103820/www.irsg.org/html/termination.htm (last visited 9/20/11).
[55] Id.
[56] 15 U.S.C. § 6801(a).
[57] 15 U.S.C. § 6809(3). See also Federal Trade Commission, *In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act* (2002), http://business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act (last visited 9/20/11).
[58] See www.irsg.org (last visited 9/20/11).

2000.[59] PLI promptly began an ad campaign in national publications to promote industry self-regulation of online consumer privacy. According to a contemporary news account, the PLI initiative "follows a recent Federal Trade Commission recommendation that Congress establish legislation to protect online consumer privacy."[60]

A description of the PLI from its website in 2001 stated:

> The Privacy Leadership Initiative was formed by leaders of a number of different companies and associations who believe that individuals should have a say in how and when their personal information can be used to their benefit.
>
> The purpose of the PLI is to create a climate of trust which will accelerate acceptance of the Internet and the emerging Information Economy, both online and off-line, as a safe and secure marketplace. There, individuals can see the value they receive in return for sharing personally identifiable information and will understand the steps they can take to protect themselves. As a result of sharing, individuals will have the power to enhance the quality of their lives through personalized information, products and services.[61]

Another statement from the PLI website provides a more expansive statement of the origin and purpose of the organization:

> Why We Formed
>
> The PLI was formed to provide consumers with increased knowledge and resources to help them make informed choices about sharing their personal information. We also help businesses, both large and small — in all industries — develop and maintain good privacy practices. Trust and choice are the foundation of good privacy practices, yet research shows that there is currently a lack of trust between consumers and businesses. Individuals must trust responsible businesses to use personal information in ways that benefit them — such as better, less expensive and personalized products and services — while also providing them with choices about how much personal information is gathered and by whom. Through the establishment of a common understanding about the benefits

---

[59] See Marcia Savage, *New Industry Alliance Addresses Online Privacy*, Computer Reseller News (06/19/00), http://technews.acm.org/articles/2000-2/0621w.html#item13 (last visited 9/20/11).

[60] Id.

[61] http://web.archive.org/web/20010411210453/www.understandingprivacy.org/content/about/index.cfm (last visited 9/20/11).

> of exchanging personal information and how it can be safeguarded, the PLI will begin to restore consumer confidence.
>
> What We're Doing
>
> Given that privacy is a question of trust and behavior, the PLI is developing an "etiquette"--model practices for the exchange of personal information between businesses and consumers. We will help create this code of conduct by engaging in a multi-year, multi-level effort to educate consumers and businesses. Specifically, the PLI will:
> 1. Conduct original research to measure and track attitudes and behavior changes among consumers and to better understand how the flow of information affects the economy and people's lives on a day-to-day basis;
> 2. Compile and refine existing privacy guidelines and create The Privacy Manager's Resource Center, a new service for that assists businesses in developing their privacy programs
> 3. Design an interactive Web site — understandingprivacy.org — to make privacy simpler for consumers, businesses, trade groups, journalists, academics, policymakers and all other interested parties; and
> 4. Educate consumers about technology and tools that protect their interests without diminishing the benefits of exchanging personal preferences with responsible companies.
>
> Whether online or off, the flow of information is critical to the growth and success of our economy. Members of the PLI recognize that businesses must take an active role in ensuring that privacy practices evolve to meet consumer needs. While there is no simple answer for an issue this complex, for PLI members that means understanding what individuals want, tackling those challenges and initiating change, while being accountable and building confidence. These are the keys to creating a climate of trust between responsible businesses and consumers.[62]

Other accounts from the time support the notion that PLI was intended to promote self-regulation. A 2001 story on Internet privacy from a publication of the Wharton School at the University of Pennsylvania focused on the self-regulation goal:

> While Congress debates legislation on Capitol Hill, the business community is actively promoting other options. Chief among these is self-regulation.
>
> Earlier this month, for example, the Privacy Leadership Initiative (PLI) - a group of executives from such companies as AT&T, Dell Computer, Ford,

---

62 http://web.archive.org/web/20010419185921/www.understandingprivacy.org/content/about/fact.cfm (last visited 9/20/11).

> IBM and Procter & Gamble – announced a $30-$40 million campaign aimed at showing consumers how they can use technology to better protect their privacy online.[63]

By the middle of 2002, the threat of regulation has diminished enough so that PLI "transitioned" its activities to others. The BBBOnLine, a program of the Better Business Bureau system,[64] took over the PLI website (understandingprivacy.org). The BBBOnline privacy program, which lasted longer than the PLI, is no longer operational, and its details are discussed elsewhere in this paper.

By the middle of September 2002, the transition of the website to BBBOnLine appeared to be complete.[65] However, by January 2008, the understandingprivacy.org website had changed entirely, offering visitors an answer to the question *Can microwave popcorn cause lung disease?*[66] By the beginning of 2011, the understandingprivacy.org website was controlled by Media Insights, a creator of "content-rich Internet publications."[67] Other Media Insights websites include BunnyRabbits.org, Feathers.org and PetBirdReport.com.[68] It is an ignominious end point.

The Online Privacy Alliance

The Online Privacy Alliance[69] was created in 1998 by former Federal Trade Commissioner Christine Varney.[70] OPA's earliest available webpage described the

---

[63] *Up for Sale: How Best to Protect Privacy on the Internet*, Knowledge@Wharton (March 19, 2001), http://knowledge.wharton.upenn.edu/article.cfm?articleid=325 (last visited 9/20/11).

[64] Press Release, *Privacy Leadership Initiative Transfers Initiatives to Established Business Groups* (July 1, 2002), http://goliath.ecnext.com/coms2/gi_0199-1872940/Privacy-Leadership-Initiative-Transfers-Initiatives.html (last visited 9/20/11).

[65] http://web.archive.org/web/20020914095335/www.bbbonline.org/understandingprivacy (last visited 9/20/11).

[66] http://web.archive.org/web/20080118171946/http://www.understandingprivacy.org (last visited 9/20/11).

[67] http://www.mediainsights.com (last visited 9/20/11).

[68] Id.

[69] The main webpages for the organization are at www.privacyalliance.org. However, for a brief period starting in 2005, the Internet Archive shows that the organization also maintained webpages at www.privacyalliance.com. The first pages reported by the Internet Archive for www.privacyalliance.org are dated December 2, 1998.

organization as *a cross-industry coalition of more than 60 global corporations and associations.*[71]

The first paragraph of the background page on its website stated clearly its interest in promoting self-regulation:

> Businesses, consumers, reporters and policy makers at home and abroad are watching closely to see how well the private sector fulfills its commitment to create a credible system of self-regulation that protects privacy online. One of the most important signs that self-regulation works is the growing number of web sites posting privacy policies.[72]

In July 1998, OPA released a paper describing *Effective Enforcement of Self-regulation.*[73] In November 1999, a representative of the OPA appeared at an FTC workshop on online profiling and participated in a session on the role of self-regulation.[74] OPA self-regulatory principles were cited by industry representatives before the FTC and elsewhere.[75]

It is difficult to chart with precision the deterioration of the OPA. By all appearances, the OPA is defunct. It no longer accepts members, and the primary evidence of its activity is continuing small changes to their website. A review of webpages available at the Internet Archive shows a decline of original OPA activities starting in the early 2000s. For example, the first webpage available for 2004 prominently lists OPA news, but the first item shown is dated March 2002 and the next most recent item is dated November 2001.[76] The OPA news on the first webpage available for 2005 shows four press stories from 2004, but the most recent OPA item was still

---

[70] http://web.archive.org/web/19990209062744/www.privacyalliance.org/join/background.shtml (last visited 9/20/11).

[71] Id.

[72] http://web.archive.org/web/19990209062744/www.privacyalliance.org/join/background.shtml (last visited 2/8/11).

[73] http://web.archive.org/web/19981202200600/http://www.privacyalliance.org (last visited 9/20/11).

[74] http://www.ftc.gov/bcp/workshops/profiling/991108agenda.htm (last visited 9/20/11).

[75] See, e.g., Statement of Mark Uncapher, Vice President and Counsel, Information Technology Association of America, before the Federal Trade Commission Public Workshop on Online Profiling (October 18, 1999), http://www.ftc.gov/bcp/workshops/profiling/comments/uncapher.htm (last visited 9/20/11).

[76] http://web.archive.org/web/20040122052508/http://www.privacyalliance.org (last visited 9/20/11).

November 2001.[77] By 2008, The OPA news on the first webpage available for that year shows 2 news stories from 2006, and no reported OPA activity more recent than 2001.[78] There is little or no evidence after 2001 of OPA activities or participation at the Federal Trade Commission.[79] The threat that fostered the creation of the OPA apparently had disappeared. Wikipedia categorizes OPA under *defunct privacy organizations.*[80]

The OPA website continues to exist and appears to have been reformatted and updated at some time after 2008. The website has some links to recent new items, but a *More OPA News* link at the bottom connects to a webpage that shows no item more recent than 2001.[81] The main OPA webpage also includes links to old OPA documents such as *Guidelines for Online Privacy Policies* (approximately 533 words) and *Guidelines for Effective Enforcement of Self-Regulation* (approximately 1269 words). The website continues to offer old items, such as an OPA *Commentary to the Mission Statement and Guidelines* dated November 19, 1998.[82]

The list of members on its website as recently as May 2011 included at least one company (Cendant) that no longer existed at that time.[83] The membership page was not dated, and members number approximately 30, or less than half the number reported in 1998. The website now reports that membership is "closed".

The Network Advertising Initiative[84] (1999-2007 version)

The network advertising industry announced the formation of the Network Advertising Initiative at an FTC workshop in 1999. NAI issued its standards, a 21-

---

[77] http://web.archive.org/web/20050104085718/http://www.privacyalliance.org (last visited 9/20/11).
[78] http://web.archive.org/web/20080201111641/http://www.privacyalliance.org (last visited 9/20/11).
[79] www.ftc.gov (last visited 9/20/11)
[80] http://en.wikipedia.org/wiki/Online_Privacy_Alliance (last visited 9/20/11).
[81] http://www.privacyalliance.org/news (last visited 9/20/11).
[82] http://www.privacyalliance.org/news/12031998-4.shtml (last visited 9/20/11).
[83] http://web.archive.org/web/20110512024943/http://www.privacyalliance.org/members (last visited 9/20/11)
[84] This summary is adapted from a comprehensive review of the Network Advertising Initiative (NAI) published by the World Privacy Forum in 2007. The WPF report is THE NETWORK ADVERTISING INITIATIVE: Failing at Consumer Protection and at Self-Regulation. The WPF report contains citations and support for the conclusions presented here. http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf (last visited 9/20/11).

page document, the next year.[85] The core concept – the opt-out cookie – has been criticized as a technical and policy failure, and it remains highly controversial.[86] The NAI is of particular note because the Federal Trade Commission voted on its creation.

When it began, NAI membership consisted of 12 companies, which was a fraction of the industry engaging in behavioral ad targeting. By 2002, membership hit a low of two companies.[87] This was a significant lack of participation by the industry. When the NAI created a category of associate members who were not required to be in full compliance with the NAI standards, membership increased, with associate members outnumbering regular members by 2006. Eventually, NAI eliminated the associate membership category.[88]

The NAI delegated enforcement of its standards to TRUSTe, an unusual action given that TRUSTe was a member of NAI for one year.[89] Over several years, the scope of TRUSTe public reporting on NAI complaints decreased consistently until 2006, when separate reporting about NAI by TRUSTe stopped altogether.[90] There is no evidence that the audits of NAI members that were required by NAI principles were conducted. No information about audits of members was ever made public.[91]

Much of the pressure that produced the NAI came from the Federal Trade Commission. Industry reacted in 1999 to an FTC behavioral advertising workshop, and the NAI self-regulatory principles were drafted with the support of the FTC.[92] Pressure from the FTC diminished or disappeared quickly, and by 2002, only two NAI members remained. When the FTC again showed interest in online behavioral advertising in 2008, the NAI began to take steps to fix the problems that had developed with its 2000 principles.[93] One of those steps was "promoting more robust self-regulation by today opening a 45-day public comment period concurrent with the release of a new draft 2008 NAI Principles."[94] NAI never sought public comment on the original principles.

---

[85] Id. at 7-8.
[86] Id. at 14-16.
[87] Id at 28-29.
[88] Id. at 29-30.
[89] Id. at 25.
[90] Id. at 33-36.
[91] Id. at 37.
[92] Id. at 9.
[93] See, e.g., Network Advertising Initiative, *Written Comments in Response to the Federal Trade Commission Staff's Proposed Behavioral Advertising Principles* (April 2008), http://www.ftc.gov/os/comments/behavioraladprinciples/080410nai.pdf (last visited 9/20/11).
[94] Id.

Because we remain in a period of renewed Federal Trade Commission and congressional interest in privacy, it is too soon to evaluate the new NAI efforts. Only when the pressure for better privacy rules has faded will it be possible to evaluate the new NAI activities fairly.

There were substantive problems with the original NAI principles as well. The conclusion of the World Privacy Forum Report summarizes the NAI failures:

> The NAI has failed. The agreement is foundationally flawed in its approach to what online means and in its choice of the opt-out cookie as a core feature. The NAI opt-out does not work consistently and fails to work at all far too often. Further, the opt-out is counter-intuitive, difficult to accomplish, easily deleted by consumers, and easily circumvented. The NAI opt-out was never a great idea, and time has shown both that consumers have not embraced it and that companies can easily evade its purpose. The original NAI agreement has increasingly limited applicability to today's tracking and identification techniques. Secret cache cookies, Flash cookies, cookie re-setting techniques, hidden UserData files, Silverlight cookies and other technologies and techniques can be used to circumvent the narrow confines of the NAI agreement. Some of these techniques, Flash cookies in particular, are in widespread use already. These persistent identifiers are not transparent to consumers. The very point of the NAI self-regulation was to make the invisible visible to consumers so there would be a fair balance between consumer interests and industry interests. NAI has not maintained transparency as promised.
>
> The behavioral targeting industry did not embrace its own self-regulation. At no time does it appear that a majority of behavioral targeters belong to NAI. For two years, the NAI had only two members. In 2007 with the scheduling of the FTC's new Town Hall meeting on the subject, several companies joined NAI or announced an intention to join. Basically, the industry appears interested in supporting or giving the appearance of supporting self-regulation only when alternatives are under consideration. Enforcement of the NAI has been similarly troubled. The organization tasked with enforcing the NAI was allowed to become a member of the NAI for one year. This decision reveals poor judgment on the part of the NAI and on the part of TRUSTe, the NAI enforcement organization. Further, the reporting of enforcement has been increasingly opaque as TRUSTe takes systematic steps away from transparent reporting on the NAI. If the enforcement of the NAI is neither independent nor transparent, then how can anyone determine if the NAI is an effective self-regulatory scheme? The result of all of these and other deficiencies is that the protections promised to consumers have not been realized. The NAI self-regulatory agreement has failed to meet the goals it has stated, and it

> has failed to meet the expectations and goals the FTC laid out for it. The NAI has failed to deliver on its promises to consumers.[95]

The NAI self-regulatory effort that began in 1999 was a demonstrable failure within a few years.

BBBOnline Privacy Program

The BBBOnline Privacy Program began in 1998, in response to "the need identified by the Clinton Administration and businesses for a major self-regulation initiative to protect consumer privacy on the Net and to respond to the European privacy initiatives."[96] Founding sponsors included leading businesses, such as AT&T, GTE, Hewlett-Packard, IBM, Procter & Gamble, Sony Electronics, Visa, and Xerox.[97] The program was operated by the Council of Better Business Bureaus through its subsidiary, BBBOnLine. There may have been some consumer group participation in the development of the BBBOnLine privacy program.

The BBBOnline Privacy Program was much more extensive than many other efforts at the time. It included "verification, monitoring and review, consumer dispute resolution, a compliance seal, enforcement mechanisms and an educational component."[98] To qualify, a company had to post a privacy notice telling consumers what personal information is being collected, how it will be used, choices they have in terms of use. Participants also had to verify security measures taken to protect their information, abide by their posted privacy policies, and agree to an independent verification by BBB*OnLine*. Companies had to participate in the programs' dispute resolution service,[99] a service that operated under a 17-page set of detailed procedures.[100] The dispute resolution service also reported publicly

---

[95] World Privacy Forum *NAI Report* at 39.
[96] New Release, Better Business Bureau, *BBBOnLine Privacy Program Created to Enhance User Trust on the Internet* (June 22, 1998), http://www.bbb.org/us/article/bbbonline-privacy-program-created-to-enhance-user-trust-on-the-internet-163 (last visited 2/10/11).
[97] Id.
[98] The earliest web presence for the BBB Online Privacy Program appeared at the end of 2000. http://web.archive.org/web/20010119180300/www.bbbonline.org/privacy (last visited 9/20/11).
[99] http://web.archive.org/web/20010201170700/http://www.bbbonline.org/privacy/how.asp (last visited 9/20/11).
[100] http://web.archive.org/web/20030407011013/www.bbbonline.org/privacy/dr.pdf (last visited 9/20/11).

statistics about its operations.[101] As noted above, the BBBOnLine Privacy Program took over the Privacy Leadership Initiative website (understandingprivacy.org) when PLI ended operations in 2002. The BBBOnline Privacy Program was considerably more robust than most, if not all, of the contemporary privacy-self-regulatory activities.

It is difficult to determine how many companies participated in the BBBOnline privacy program. A 2000 Federal Trade Commission report on online privacy said that "[o]ver 450 sites representing 244 companies have been licensed to post the BBBOnLine Privacy Seal since the program was launched" in March 1999.[102] Whether the numbers increased in subsequent years is unknown, but the number reported in 2000 clearly represent a tiny fraction of websites and companies. It may be that the more rigorous requirements that BBBOnline asked its members to meet was a factor in dissuading many companies from participating.

BBBOnline stopped accepting applications for its privacy program sometime in 2007.[103] The specific reasons the program terminated are not clear, but it seems likely that it was the result of lack of support, participation, and interest. Self-regulation for the purpose of avoiding real regulation is one thing, but the active and substantial self-regulation offered by BBBOnline may have been too much for many potential participants. BBBOnline continues to operate other programs, including an EU Safe Harbor dispute resolution service,[104] but there is no evidence on its website of the original BBBOnline privacy program. Interestingly, some companies continue to cite the now-defunct BBBOnline privacy program in their privacy policies.[105]

---

[101] See, e.g., http://web.archive.org/web/20070124235138/www.bbbonline.org/privacy/dr/2005q3.asp (last visited 9/20/11). While the BBBOnline privacy program dispute procedures were better and more transparent than other comparable procedures, the BBBOnline dispute resolution service was controversial in various ways. In 2000, for example, questions were raised when the BBBOnline Privacy Program, under pressure from the subject of a complaint, vacated an earlier decision and substituted a decision more favorable to the complaint subject.

[102] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report To Congress* 6 (2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited 9/20/11).

[103] http://web.archive.org/web/20070830164536rn_1/www.bbbonline.org/privacy (last visited 2/10/11).

[104] http://www.bbb.org/us/european-union-dispute-resolution (last visited 9/20/11). It is not clear if BBBOnline has actually handled any US-EU Safe Harbor complaints.

[105] See, e.g., the Equifax Online Privacy Policy & Fair Information Principles, http://www.worldprivacyforum.org/pdf/equifaxprivacypolicydec5.pdf (last visited 9/20/11); Good Feet, http://goodfeet.com/about-us/privacy-policy (last visited 9/20/11).

III. Discussion: Government Privacy Self-Regulatory Activities

This section reviews several other privacy self-regulatory activities that share some characteristics with the industry self-regulatory programs discussed above, but these activities differ in various ways. The most noticeable differences are the role of the government in the programs. The Department of Commerce is involved in the Safe Harbor Framework, and the Federal Trade Commission is involved in the Children's Online Privacy Protection Act.

Department of Commerce Safe Harbor Framework[106]

The Safe Harbor Framework operated by the Department of Commerce started in 2000 with an agreement between the Department and the European Commission.[107] The Safe Harbor Framework differs somewhat from the other self-regulatory activities discussed in this report because of the role played by the Department. However, the Department's role in the Safe Harbor Framework did not prevent the deterioration of the Safe Harbor over time or stop the lack of compliance by companies that participated in the Safe Harbor.

With the adoption of the European Union's Data Protection Directive[108] in 1995 and its implementation in 1998, much of the concern about transborder data flows of personal information centered on the export restriction policies of the Directive. Article 25 of the Directive generally provides that exports of personal data from EU Member States to third countries are allowed if the third country *ensures an adequate level of protection*.[109]

---

[106] This summary is adapted from an analysis of the Department of Commerce's international privacy activities published by the World Privacy Forum in 2010. The WPF report is The US Department of Commerce and International Privacy Activities: Indifference and Neglect. The WPF report contains additional citations and support for the conclusions presented here. See: http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf (last visited 9/20/11).

[107] All Safe Harbor documents can be found at http://www.export.gov/safeharbor/eg_main_018237.asp (last visited 9/20/11).

[108] Council Directive 95/46, art. 28, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281/47), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited 9/20/11).

[109] Other grounds for data exports are not relevant here.

While the EU determined that some countries (e.g., Argentina, Canada, and Switzerland) provide an adequate level of privacy protection according to EU standards, the United States has never been evaluated for adequacy or determined to be adequate.

Restrictions on exports of personal data from Europe created some significant problems and uncertainties for both US and EU businesses, including online businesses. Pressured by the American business community, the Commerce Department intervened to resolve the threats to US business presented by the Data Protection Directive.

The Safe Harbor framework[110] was the result. It allows US organizations to publicly declare that they will comply with the requirements. An organization must self-certify annually to the Department of Commerce in writing that it agrees to adhere to the Safe Harbor's requirements. There are seven areas of privacy standards covering notice, choice, onward transfer (transfers to third parties), access, security, data integrity, and enforcement. Safe Harbor documentation describes the requirements and provides an interpretation of the obligations.[111] To qualify for the Safe Harbor, an organization can (1) join a self-regulatory privacy program that adheres to the Safe Harbor's requirements; or (2) develop its own self-regulatory privacy policy that conforms to the Safe Harbor. The Safe Harbor Framework has its own standards, voluntary certification, and some external method of enforcement so that it is similar to the self-regulatory activities considered earlier this report.

The International Trade Administration of the Department of Commerce now operates the Safe Harbor framework. The Commerce Department website maintains a list of organizations that filed self-certification letters. Only organizations that are subject to the jurisdiction of the Federal Trade Commission or the Department of Transportation are eligible to participate. This limitation means that many companies and organizations that transfer personal information internationally cannot qualify for participation either in whole or in part.

Three studies of the Safe Harbor Framework were conducted since the start of Safe Harbor. The first study was conducted in 2001 at the request of the European Commission Internal Market DG.[112] The second study, completed in 2004, was also conducted at the request the European Commission Internal Market DG. An international

---

[110] http://www.export.gov/safeharbor/eu/eg_main_018476.asp (last visited 9/20/11).

[111] http://www.export.gov/safeharbor/eu/eg_main_018493.asp (last visited 9/20/11).

[112] *The Functioning of the US-EU Safe Harbor Privacy Principles*, (September 21, 2001). This study was reportedly published by the European Commission, but a copy has not been located on the EU's data protection webpage or elsewhere on the Internet. The study author is not identified in the document, but a Commission official publicly identified Professor Joel R. Reidenberg, Fordham University Law School, as the author, and the 2004 Study also identified Professor Reidenberg as the author. See 2004 Study at note 2.

group of academics conducted the study.[113] The third study was prepared by Chris Connolly, director of an Australian management consulting company with expertise consultants in privacy, authentication, electronic commerce, and new technology.[114]

Overall, the three studies found the same problems with Safe Harbor. Companies that claim to meet the Safe Harbor requirements are not actually in compliance with those requirements. Evidence from the three reports suggests that the number of companies not in compliance has increased over time.

There is no evidence of improvement in the administration of the Department's Safe Harbor activities. Perhaps the most prominent response to the reports of noncompliance was the addition of a disclaimer on the Department's Safe Harbor website indicating that Department cannot guarantee the accuracy of the information it maintains.[115] It appears that the Department has made some changes to its website over the years, but there remains a lack of evidence of any substantive efforts by the Department to monitor or enforce compliance.

While the Safe Harbor Framework is not a pure industry-run self-regulatory activity because of the role of the Department of Commerce, it shares characteristics of industry self-regulatory activities, namely interest in the Safe Harbor Framework diminished over time, and business support and participation deteriorated. Enforcement has been rare, and the Department never conducted or required audits of participants.

The shortcomings of the Safe Harbor Framework have come to the attention of some data protection authorities in Europe. In April 2010, the Düsseldorfer Kreis, a working group comprised of the 16 German federal state data protection authorities with authority over the private sector, adopted a resolution applicable to those who export data from

---

[113] Safe Harbour Decision Implementation Study (2004), http://ec.europa.eu/justice/policies/privacy/docs/studies/safe-harbour-2004_en.pdf (last visited 9/20/11). As identified in the paper, the authors are Jan Dhont, María Verónica Pérez Asinari, and Prof. Dr. Yves Poullet (Centre de Recherche Informatique et Droit, University of Namur, Belgium) with the assistance of Prof. Dr. Joel R. Reidenberg (Fordham University School of Law, New York, USA) and Dr. Lee A. Bygrave (Norwegian Research Centre for Computers and Law, University of Oslo, Norway).

[114] *The US Safe Harbor - Fact or Fiction?* (2008), http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf (last visited 9/20/11).

[115] See https://www.export.gov/safehrbr/list.aspx (last visited 9/20/11) ("In maintaining the list, the Department of Commerce does not assess and makes no representations to the adequacy of any organization's privacy policy or its adherence to that policy. Furthermore, the Department of Commerce does not guarantee the accuracy of the list and assumes no liability for the erroneous inclusion, misidentification, omission, or deletion of any organization, or any other action related to the maintenance of the list.").

Germany to US organizations that self-certified compliance with the Safe Harbor Framework. The resolution tells German data exporters that they must verify whether a self-certified data importer in the US actually complies with the Safe Harbor requirements.[116]

Essentially, the action by the German state data protection authorities rejects in significant part the Safe Harbor Framework, particularly the self-certification as it appears on the Department of Commerce website. The Düsseldorfer Kreis makes this clear when it states that the reason for its action is that "comprehensive control of US-American companies' self-certifications by supervisory authorities in Europe and in the US is not guaranteed..."[117]

The Department has ignored repeated evidence that many or most Safe Harbor participants are not in compliance with the requirements. Instead, in a recent green paper, the Department claimed that the Safe Harbor Framework was "successful."[118] It is not clear what standard the Department used to measure the success of the Safe Harbor Framework. All available evidence strongly suggests a substantial lack of compliance with the Safe Harbor Framework.

Children's Online Privacy Protection Act (COPPA)

The safe harbor provision in the Children's Online Privacy Protection Act (COPPA)[119] is sometimes cited as a self-regulatory program. For that reason, COPPA is discussed here. However, it is crucial to note that COPPA self-regulation is significantly different from the others discussed in this report. The companies in a COPPA safe harbor must follow all the substantive standards established in the COPPA statute and FTC regulations, meaning that a participant in a safe harbor program must do everything that a non-participant must do *plus* bear the cost of the safe harbor. The standards cannot be changed by the participants in the self-regulatory program. The FTC formally oversees and approves COPPA safe harbor

---

[116] Supreme Supervisory Authorities for Data Protection in the Nonpublic Sector (Germany), *Examination of the Data Importer's Self-Certification According to the Safe-Harbor-Agreement by the Company Exporting Data* (revised version of Aug. 23, 2010), http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf?1285316129 (last visited 9/20/11).
[117] Id.
[118] Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* at 44 (undated; released in December 2010), http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf (last visited 9/20/11).
[119] 15 U.S.C. §§ 6501-6506.

programs, a characteristic that other self-regulatory programs reviewed here lacked.[120]

In effect, the COPPA safe harbor programs mostly engage in limited enforcement of the statute and relieve the Commission of some of the burden. This may have some benefits overall. It should not be surprising that industry participation in the safe harbor aspect of COPPA is limited. Whether COPPA self-regulation is a success or failure is a subject for reasonable debate, but COPPA has fewer characteristics of failure than the industry self-regulation discussed earlier. For example, there is a formal input procedure for consumers, the safe harbor program has not disappeared, and there has been COPPA enforcement by the FTC. The COPPA model does not appear to be a model in current use outside of this instance. The reason may be that self-regulatory activities under a legislative scheme have little attraction when the principal purpose of industry self-regulation for privacy has been avoidance of regulation in the first place.

IV. Discussion: Combination Self-Regulatory Efforts

The self-regulatory efforts in this category include projects that have many components, including input from government, industry, academia, and civil society.

Platform for Privacy Preferences Project (P3P)

The Platform for Privacy Preferences Project (P3P) is a technical standard for communicating the privacy policies of a website to those who use the website. A user can retrieve a standardized machine-readable privacy policy from a website and use the information to make a decision about how to interact with the website. Each user can match the privacy policy against the user's individual privacy preferences.

P3P allows a browser to understand a website privacy policy in a simplified and organized manner, without the need for a user to find and read a lengthy privacy policy. With the proper browser settings, P3P will automatically block any cookies from a website with a privacy policy that the user determined to be objectionable.

The Center for Democracy and Technology (CDT) supported the early work that eventually resulted in P3P.[121] CDT convened an Internet Privacy Working Group that drafted a mission statement, with companies, trade associations, and consumer

---

[120] 15 U.S.C. § 6503.

[121] For a fuller history of P3P and details on the actual technical standard, see Lorrie Faith Cranor, Web Privacy with P3P (2002).

groups participating. A presentation of a prototype was presented at an FTC Workshop in 1997.[122]

Later in the same year, P3P became a project of the World Wide Web Consortium (W3C), the main international standards organization for the World Wide Web. The working group included representatives of companies, academia, and government.[123] The work of drafting the formal specification took some time, and version 1.0 was finally published at the end of 2000.[124] A later specification was published in 2006.[125]

Microsoft included some support for P3P in its browser, Internet Explorer.[126] The Firefox browser from Mozilla also provides some support.[127] The E-Government Act of 2002[128] included a requirement that federal agency websites translate privacy policies into a standardized machine-readable format,[129] and P3P is the only specification that meets the requirements.[130] It was a promising start.

However, the extent to which commercial websites and even government websites attempted to implement P3P or succeeded in doing so in the long term is highly uncertain. A 2008 published review of P3P by Professor Lorrie Faith Cranor found P3P adoption increasing overall but that P3P adoption rates greatly vary across industries. Other findings are that P3P had been deployed on 10% of the sites returned in the top-20 results of typical searches, and on 21% of the sites in the top-20 results of e-commerce searches. Review of over 5,000 web sites in both 2003 and 2006 found that P3P deployment increased over that period, although there were decreases in some sectors. The review also found high rates of syntax errors among P3P policies, but much lower rates of critical errors that prevent a P3P user agent from interpreting them. Privacy policies of P3P-enabled popular websites were

---

[122] Id. at 45.
[123] Id. at 46.
[124] Id. at 53.
[125] http://www.w3.org/TR/P3P11 (last visited 9/20/11).
[126] See http://msdn.microsoft.com/en-us/library/ms537343%28VS.85%29.aspx (last visited 9/20/11).
[127] See http://www-archive.mozilla.org/projects/p3p (last visited 9/20/11).
[128] Public Law 107-347.
[129] See Office of Management and Budget, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (2003) (M-03-22), http://www.whitehouse.gov/omb/memoranda_m03-22 (last visited 9/20/11).
[130] See, e.g., Department of Health and Human Services, *HHS-OCIO Policy for Machine-Readable Privacy Policies* at 4.2 (Policy 2010-0001, 2010), http://www.hhs.gov/ocio/policy/hhs-ocio-2010_0001_policy_for_machine-readable_privacy_policies.html (last visited 9/20/11).

found to be similar to the privacy policies of popular websites that do not use P3P.[131]

An analysis published two years later by the CyLab at Carnegie Mellon University looked at over 33,000 websites using P3P compact policies and "detected errors on 11,176 of them, including 134 TRUSTe-certified websites and 21 of the top 100 most-visited sites."[132] The study also found thousands of sites using identical invalid compact policies (CP) that had been recommended as workarounds for Internet Explorer cookie blocking. Other sites had CPs with typos in their tokens, or other errors. Fully 98% of invalid CPs resulted in cookies remaining unblocked by Internet Explorer under its default cookie settings. The analysis concluded that it "appears that large numbers of websites that use [compact policies] are misrepresenting their privacy practices, thus misleading users and rendering privacy protection tools ineffective."[133] The study concluded that companies do not have sufficient incentives to provide accurate machine-readable privacy policies.[134]

In other words, the self-regulatory aspects of P3P do not appear to be working, with the CyLab study suggesting that lack of enforcement by regulators is a problem.[135] Neither P3P nor any industry trade association offers a P3P enforcement method.

P3P has some of the indicia of industry self-regulation in that it was inspired in part by FTC interest and motivated in part by an industry interest in avoiding legislation or regulation.[136] The involvement in P3P's development and promotion by consumer groups and the White House together with industry representatives differentiates P3P from the other industry efforts discussed earlier in this report. Another differentiator is the legislative requirement that federal agencies use P3P or similar technology. P3P shares sufficient characteristics with the self-regulatory programs discussed in this report to warrant its inclusion here.

---

[131] Lorrie Faith Cranor et al., *P3P Deployment on Websites*, 7 Electronic Commerce Research and Applications 274-293 (2008).
[132] Pedro Giovanni Leon et al, *Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens* (CMU-CyLab-10-014 2010), http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab10014.pdf (last visited 9/20/11).
[133] Id.
[134] Id. at 9.
[135] Id.
[136] See, e.g., Simson Garfinkel, *Can a labeling system protect your privacy?*, Salon (July 11, 2000), http://www.salon.com/technology/col/garf/2000/07/11/p3p (last visited 9/20/11) ("But P3P isn't technology, it's politics. The Clinton administration and companies such as Microsoft are all set to use P3P as the latest excuse to promote their campaign of "industry self-regulation" and delay meaningful legislation on Internet privacy.").

Some privacy groups opposed P3P from the beginning, largely because of concerns that it would prevent privacy legislation from passing. Company views of the project also varied.[137] It is not clear how much attention P3P has received in recent years from companies or privacy groups.

Unlike some of the self-regulatory activities discussed in Part II of this analysis, P3P remains in use. However, given the findings of the 2010 study of widespread misrepresentation of privacy policies by those using P3P, it is hard to call P3P any kind of success. Further, the study provides strong evidence of deliberate deception in implementation of P3P at some websites. Internet users appear to have little knowledge of P3P, although public awareness may not be essential since the controls are built into browsers and users appear to be concerned about the privacy policies that P3P is designed to convey.[138] Like the Commerce Department's Safe Harbor Framework, P3P continues to exist, but both programs are so lacking in rigor and compliance that neither is fulfilling its original purpose.

V. Conclusion

Is there any reason to think that privacy self-regulation will work today when it did not work in the past? Privacy self-regulation done in the same way that it has been done in the past, without sufficient consumer participation, and with the same goals of simply evading real regulation and effective privacy controls will continue to fail.

What should be done if privacy self-regulation cannot succeed is beyond the scope of this report. This report does not advocate for regulation or against improved self-regulation. The point is that there is no reason to believe that *this time will be different* when it comes to privacy self-regulation done in ways that have been proved to lead to failure. New approaches are needed if the goal is to offer consumer valuable, effective, and balanced privacy protections that last.

What is at stake: Implications for current privacy self-regulatory efforts

If privacy self-regulation today is constructed in the same way as in the past, will it fail in the same way as before? Questions abound. Should self-regulation cover website advertisers? Internet service providers? Data brokers? Social networking sites? Companies using location information? Apps providers? All websites? Defining the Internet universe is daunting, and even within slices of that universe, definitions and boundaries will be difficult to establish. The past history of even the

---

[137] Lorrie Faith Cranor, Web Privacy with P3P 56 (2002).
[138] See Serge Egelman et al., *Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators* (2009), http://www.guanotronic.com/~serge/papers/chi09a.pdf (last visited 9/20/11).

best-intentioned of self-regulatory efforts shows how quickly policy can be outdated by industry and Internet developments.

The web is changing too rapidly to expect that any given form of traditional industry-supported privacy self-regulation will make sense in a year or two. Companies track the activities of individuals today in ways that were not contemplated even a year or two ago. Companies often have no reason to expose to public view their data processing functions for definition or measurement lest they reveal a marketplace advantage.

In most areas of online activity that involve personal information, the number of companies is unknown and highly variable. To determine the penetration of self-regulation coverage, there has to be both a known, demonstrable denominator of companies that fall within the self-regulatory scheme and a numerator of those companies that are participating in the scheme. Without this basic information, there is no real way to measure the penetration of privacy self-regulation. For example, if a list of Internet advertising companies exists at all, that list will go out of date almost immediately. Thus, it is difficult to determine what percentage of the defined universe has agreed to any specific self-regulatory scheme. Even if it were possible to calculate these numbers for *past* privacy self-regulatory activities, the penetration would likely be low and highly variable over time.

Measuring activity though another measure (rather than the number of companies) would probably require access to information that industry would argue to be proprietary. Thus, it is harder than ever to even make basic judgments about the scope and effect of any industry-supported privacy self-regulation.

There is more at stake financially today. Revenues from personal data activities are huge. If a self-regulatory scheme had any real effect on revenues or profits, those who stayed out of the scheme could profit at the expense of those who participated. It is hard to see how a *race to the bottom* effect would be avoided. Still, because there are so many companies and so much money involved in the Internet space, only a small percentage of companies need to participate in a privacy self-regulatory scheme to provide an impressive amount of resources that will make the self-regulation look better than it is. Millions for show, but pennies for substance.

A poorly designed privacy self-regulation scheme that has limited market penetration and insufficient enforcement may be good enough to fool potential regulators once again. Industry is well aware that a little will go a long way for public relations purposes. Industry knows that it only needs to keep a self-regulatory program alive for a limited period. Current debates about privacy self-regulation do not place the burden on industry to prove how proposed self-regulatory privacy programs are going to be substantively different than past efforts, at least in public view.

The Federal Trade Commission has no effective means of issuing privacy regulations because of current limits on its statutory authority. This is a structural problem that essentially compels the agency to look favorably at self-regulation because it has no alternative to offer. The FTC can always recommend legislation, but it is not clear that an FTC recommendation will be influential, that privacy legislation can pass the Congress, or that the FTC can manage to support any legislative recommendation.

Privacy self-regulation as supported by industry today suffers from the same lack of tension as in the past. Without meaningful, independent participation (e.g., by privacy and consumer advocates) in the development and oversight of privacy self-regulation, the self-regulatory standards and enforcement will be just as insufficient as they were in the past. Industry-financed oversight will not succeed because industry does not want it to be effective. For-profit privacy standards will not succeed because the pressure for profits overwhelms the efforts of would-be enforcers.

Privacy self-regulation cannot be meaningful if companies are free to drop out of any self-regulatory scheme at will or to join a different self-regulatory scheme that has weaker standards.
Would-be self-regulators are not likely to sue former members. Privacy commitments typically come with a caveat that they can be changed at will at any time without notice. For-profit companies overseeing privacy standards will not be likely to discipline paying members effectively lest they lose revenues or deter participation from new players.

The threat of Federal Trade Commission action is loudly touted by self-regulators as an effective enforcement method. Reliance on Commission enforcement of self-regulation is a challenge, as industry knows that the Commission does not have the resources to enforce a self-regulation scheme covering hundreds or thousands of companies.

This is the case notwithstanding the absence of meaningful Commission activity against those who ignored or discontinued privacy self-regulation. How can the Commission take action against an industry-supported self-regulatory program that has lost all industry support?

The history lesson here poses challenges to the present efforts for codes of conduct or self-regulation. Self-regulation, done in the same ways as it has been done in the past, is not a hopeful way forward. However, the history lesson is not without hope. This report notes key factors that have been salient in the self-regulatory failures. These factors need to be studied *and* avoided. This report also notes factors that might lay groundwork for success, gleaned from observation of what has not worked. No matter what, one thing is quite certain: there is no need to repeat the past again.

What Could Improve the Process?

It is not the primary purpose of this report to put forward a set of criteria for a meaningful and effective privacy self-regulatory regime. However, it is clear from past experience that some approaches are more likely to produce more positive results and some are not likely to result in a change from the past. In looking at past challenges to success (lack of membership, short duration, no consumer representation, etc.) we are able to set out some basic qualities needed for improvement.

Tension in the Process

Successful privacy self-regulation requires standards responsive to the actual problems, robust policies, meaningful enforcement, and effective remedies. Privacy self-regulation of industry, by industry, and for industry will not succeed. Tension in self-regulation can be provided by a defined and permanent role for consumers who are the intended beneficiaries of privacy protection. Government may also be able to play a role, but government cannot be relied upon as the sole overseer of the process. The past has shown that the interest of the FTC waxed and waned with the political cycle, and the Department of Commerce did not provide sufficient oversight.

Scope

The scope of a self-regulatory regime must be clearly defined at the start. It must apply to a reasonable segment of industry, and it must attract a reasonable percentage of the industry as participants. There must be a method to assess the penetration of the self-regulatory regime in the defined industry.

Fair Information Practices

Any self-regulatory regime should be based on Fair Information Practices (FIPs). Implementation of FIPs will vary with the industry and circumstances, but all elements of FIPs should be addressed in some reasonable fashion.

Open Public Process

The development of basic policies and enforcement methods should take place to a reasonable degree in a public process open to every relevant perspective. The process for development of privacy self-regulatory standards should have a reasonable degree of openness, and there should be a full opportunity for public comment before any material decisions become permanent. Consumers must be able to select their own representatives. Neither government nor those who are to

be regulated should select consumer participants – the selection should be up to the consumers.

Independence

The organization that operates a privacy self-regulatory system needs to have some independence from those who are subject to the self-regulation. Those who commit to comply with privacy self-regulation must make a public commitment to comply for a term of years and a financial commitment for that entire period.

Benchmarks

Past self-regulatory efforts and codes of conduct lack benchmarks for success. What constitutes success? Is it membership? Market share? Is it actual enforcement of the program? Without specific benchmarks for a privacy program, it is much more difficult to gauge success in real-time. Without the ability to accurately assess activities within a current program, both success and failure are more difficult to ascertain and may only be gleaned in hindsight.

*****

A Note on Methods

This historical review of privacy self-regulation is based on an extensive literature review, both online and offline, and includes information that was publicly available. This report covers the leading self-regulatory efforts. Some self-regulatory efforts may have disappeared without leaving a public record. Also, privacy seal programs arose during the period of this review, but some disappeared entirely and none developed sufficient credibility or public recognition to warrant investigation in this report beyond those noted in the report. Some activities within existing trade associations are difficult or impossible to assess from evidence available to those outside the associations.

Publication Information

This report was published October 14, 2011. The full report is available at www.worldprivacyforum.org/pdf/WPFselfregulationhistory.pdf. Any updates to the report will be posted to this URL.

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 online 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. Yes, 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.

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 do.

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. OK. 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.

OK. 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. OK. So I have got four on that.

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

Second question: 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? OK. 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 it is going to have a——

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. Thank you.

Mrs. BONO MACK. The chair thanks the gentlelady and now recognizes 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. OK.

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 new.

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 one 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 rigidness, 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 the 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 thank you for giving us your time and 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, that 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 sym-

bol 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 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.

Mr. 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.

Mr. 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.

Mr. 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.

Mr. 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 care-

ful about separating out privacy issues from data breaches. And the data breach issues I think require some significant action by Congress.

Mr. 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.

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

Mr. 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.

Mr. 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.

Mr. 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.

Mr. 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?

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.

Mr. 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.

Mr. 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 car-

ries 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—oK, 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. OK.

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. OK. Let me go through the panel here. I have only got about 2–½ minutes left.

Mr. HINTZE. Yes. 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. Yes, 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 [continuing]. 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, OK. 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.

Mr. CASSIDY. Mr. Hintze, OK, 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——

Mr. 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——

Mr. 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.

Mr. CASSIDY. OK. 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. Yes, 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.

Mr. 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.

Mr. 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.

Mr. CASSIDY. OK. 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.

Mr. CASSIDY. OK. 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 hearing is now adjourned.

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

[Material submitted for inclusion in the record follows:]

CMT Subcommittee Hearing
"Understanding Consumer Attitudes About Privacy"
By Rep. Cliff Stearns
Thursday, October 13, 2011
(163 words)

Thank you, Madam Chairman.

I appreciate our focus today on consumers' expectations of privacy. I agree with Intuit that customers care about their data, customers want clear explanations and choices about the use of their data, and customers welcome data-driven innovation when the benefits are clear.

That is why I introduced the Consumer Privacy Protection Act of 2011 with Rep. Jim Matheson. H.R. 1528 constitutes baseline federal legislation that requires companies to create clear privacy policies. Such policies will empower customers who are overwhelmed by the fine print in lengthy privacy statements currently used today. Moreover, companies have every incentive to draft these types of policies. Intuit discovered that 60% of their customers felt *more* positive about the company after it created clear, simply-stated privacy principles.

H.R. 1528 also promotes strong self-regulatory methods, such as those put forth by our other witnesses today – Microsoft, Evidon, and the Digital Advertising Alliance. I commend the industry's work in this arena and look forward to learning more about their efforts.

Opening Statement of Rep. Henry A. Waxman
Ranking Member, Committee on Energy and Commerce

Hearing on "Understanding Consumer Attitudes About Privacy"
Subcommittee on Commerce, Manufacturing, and Trade
October 13, 2011

The purpose of today's hearing is to understand consumer attitudes about privacy.

I believe people care deeply about their privacy. This is the clear and consistent answer businesses, privacy experts, and advocates find when they ask consumers about privacy. Consumers want to know that their information will be protected and kept private. They want some say over the massive amounts of information that is being collected and aggregated about them by businesses – some of which they know about, and some of which they don't.

In fact, one of the witnesses on today's panel, Ms. Lawler of Intuit, sums things up in one sentence: "What came across loud and clear in [our] research was that people care deeply about privacy and how their data is used."

But if you move beyond the title and read the Republican staff memo about this hearing, you see that it isn't actually about consumer attitudes regarding privacy. I'm quoting here: "The purpose of this hearing is to examine consumers' attitudes toward privacy as reflected by their utilization and manipulation of existing privacy controls." In other words, the purpose of this hearing is to look at consumer actions to protect their privacy through existing opt-out programs, browser settings, and blocking tools.

Just as it's well-established that consumers say they care about privacy, it's also pretty well-understood that when it comes to privacy protection, attitudes don't match actions. Most consumers don't use opt-out program, browser settings, and blocking tools to prevent digital snooping.

Some in the data collection industry argue that consumers' expressed attitudes don't match their actions because they don't actually care about privacy. These companies say that consumers' expressed concerns are overblown and not real.

I disagree. One reason consumers' expressed attitudes don't match their actions is because they don't know to take action, they don't know what their options are, and even if they do, they don't fully understand them.

There is a gap between what consumers actually know and what they would need to know to protect their privacy. This gap in knowledge has been researched and documented by privacy experts, some of whom are on the witness panel today.

I hope that's what we can focus on today: What do consumers know about how to protect their privacy, and what would they need to know to protect their privacy.

If we're serious about moving forward with comprehensive privacy legislation, then we should explore the answers to these questions. And we should use them to help put together a well-crafted privacy bill that respects consumers' privacy expectations and allows innovation by business in how they use their customers' data.

But at some point the hearings have to come to end and we need to move ahead. This is our fourth hearing about privacy this year. There were six privacy hearings in this Subcommittee in the last Congress. CQ published an article yesterday titled, "No Signs of Movement on Online Privacy Legislation, Despite Interest." According to CQ, "For years the cycle has been episodic publicity about commercial data-handling practices, followed by congressional hearing and the introduction of bills." And then nothing.

I'm among those that are convinced we should enact privacy protections for consumer information. I hope we're nearing the end of this latest cycle of privacy hearings and can finally see some movement on this issue.

Thank you.

Statement of
Representative John D. Dingell
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
Hearing on "Understanding Consumer Attitudes about Privacy"

October 13, 2011

Thank you, Madam Chairman. I note that this is the fourth hearing our Subcommittee has held on data privacy and commend you for your thoroughness in examining this important issue.

Our witnesses' testimony today illustrates a troubling trend among consumers. Many Americans mistakenly believe that they are afforded explicit data privacy protections under law, and that is simply not true. All the same, I do recognize that the private sector is working collaboratively to educate consumers and provide them with choices about how best to protect their privacy online. Moreover, I recognize that overly prescriptive data privacy requirements in the European Union have had a negative effect on online advertising, whose economic importance is not lost on me. Many of the newspapers in my district owe their existence to revenues generated by online ads.

With this in mind, if we in Congress do act on data privacy legislation, such action should be measured and well considered. Further, privacy requirements should be designed with enough administrative flexibility to allow federal agencies to keep pace with developments in the fast-paced online economy. Finally, all stakeholders – including consumer groups, industry, regulators, and Congress – should be involved in designing reasonable, appropriate, and practicable requirements that build on the fine work the private sector has already begun.

I look forward to hearing from our witnesses this morning. Thank you for your courtesy, and I yield back the balance of my time.

THE COMMITTEE ON ENERGY AND COMMERCE
INTERNAL MEMORANDUM

TO: Subcommittee Members

FROM: Energy and Commerce Committee Staff

RE: Majority Memorandum for October 13, 2011, Subcommittee Hearing

I. Summary

On Thursday, October 13, 2011, the Commerce, Manufacturing, and Trade Subcommittee will hold a hearing entitled "Understanding Consumer Attitudes about Privacy" at 9:00 a.m. in room 2123 of the Rayburn House Office Building. Witnesses are by invitation only.

The purpose of this hearing is to examine consumers' attitudes toward privacy as reflected by their utilization and manipulation of existing privacy controls.

II. Witnesses

Barbara Lawler
Chief Privacy Officer
Intuit

Scott Meyer
Chief Executive Officer
Evidon

Michael Hintze
Associate General Counsel
Microsoft

Linda Woolley
Executive Vice President
Direct Marketing Association
on behalf of the Digital Advertising Alliance

Alessandro Acquisti
Associate Professor of Information Systems and Public Policy
Carnegie Mellon University

Pam Dixon
Executive Director
World Privacy Forum

III. Background

Privacy laws

There is no single Federal law expressly governing all data collection in the United States, nor a single regulator to enforce existing 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 regulator. For example, the collection and use of medical information is handled primarily by the Secretary of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA) and the collection and use of financial data is protected by the Gramm-Leach-Bliley Act and enforced by the financial regulators. Additionally, the Federal Trade Commission (FTC or Commission) enforces the Fair Credit Reporting Act, which regulates the collection and use of consumer information by credit reporting agencies and their practices related to consumer information.

The FTC arguably has the broadest jurisdiction of any Federal regulator to enforce general privacy violations under its section 5 authority defining unfair or deceptive acts or practices. The Commission has brought 34 cases under its section 5 authority since 2001 against companies that failed to protect consumer information, including when companies fail to adhere to their own stated privacy policy.

Consumer Attitudes and Expectations

Both policymakers and stakeholders have expressed increasing concern regarding the collection and availability of consumers' personal information online in recent years. Increased data collection and storage by such entities as websites, 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. For instance, data about consumers' online behavior can be used to target ads toward consumers whose preferences are aligned with a particular product or service, thereby increasing the likelihood of "conversion," or sale of the product. However, advocates have raised concerns regarding a lack of transparency and, in some cases, a lack of choice for the consumer to opt out of having their data collected and/or shared with unknown parties.

In 2010, the FTC staff and the Department of Commerce National Telecommunications and Information Administration (NTIA) separately issued reports on privacy and proposed regulatory frameworks.[1]

---

[1] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (2010) (available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf); Internet Policy Task Force, Department of Commerce, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (2010) (available at http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf).

In the course of roundtable forums conducted to inform the staff report, the FTC received comments indicating a wide range of consumer attitudes and behavior regarding privacy. While the FTC received survey data indicating consumers care about privacy, there was little or no data about the level of discomfort or the percentage of consumers willing to forgo benefits to avoid tracking.[2] The FTC stressed that a lack of transparency and a lack of consumer understanding about data collection practices could be a problem affecting consumer attitudes and their ability to make informed choices.[3] Similarly, the NTIA's report noted the lack of transparency as a problem weighing on consumer understanding and consumer trust.[4]

Industry Responses and Marketplace Developments

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, whose members include the Interactive Advertising Bureau, the Network Advertising Initiative, Direct Marketing Association, Association of National Advertisers, and the American Advertising Federation, developed and implemented the "About Ads" self-regulatory principles for online behavioral advertising program to provide consumers more information on why they are seeing a particular ad and to provide consumers a mechanism to opt out of future ads served to them based on behavioral advertising.

In its staff report, the FTC proposed a number of principles to enhance consumer choices regarding privacy. The Commission staff supported the concept of a mechanism whereby consumers could register their preference not to have their information collected, commonly referred to as a "Do-Not-Track" mechanism.

Since a Subcommittee hearing in the last Congress on "Do-Not-Track" legislation, the two most popular browser developers – Microsoft (Internet Explorer) and Mozilla (Firefox) - have designed a "Do-Not-Track" feature incorporated into their browsers.[5] These features are user-controlled so consumers choose to turn on the feature to prevent tracking.[6] Internet Explorer's tool blocks content from sites that are on tracking protection lists and that could otherwise use the content to collect information, while Mozilla's Firefox's "Do-Not-Track" feature broadcasts a signal to each website a consumer visits communicating the consumer's desire not to have his or her information collected. However, the effectiveness of this tool faces significant hurdles because every website that receives the signal from the consumer's browser

---

[2] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework For Businesses and Policymakers" FTC Staff Report, (December 2010), p.29.
[3] Id., p.25
[4] "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework", The Department of Commerce Internet Policy Task Force, p.33.
[5] Wingfield, Nick and Angwin, Julia "Microsoft Adds Do-Not-Track Tool to Browser" Wall Street Journal, available at http://online.wsj.com/article/SB10001424052748703363904576200981919667762.html (viewed October 4, 2011).
[6] See http://windows.microsoft.com/en-US/windows7/How-to-use-Tracking-Protection-and-ActiveX-Filtering and http://support.mozilla.com/en-US/kb/how-do-i-stop-websites-tracking-me.

must choose to honor the request; there is no requirement that websites must honor the request. Additionally there is no current standard for the signal that is broadcast from the user's browser. Therefore, compliance by website operators has reportedly been extremely low.

In addition to the built-in features of the browsers, both offer consumers the ability to download "add-on" extension tools. In the case of Mozilla, many free add-ons have been developed to provide users greater control over their privacy and security (see https://addons.mozilla.org/en-US/firefox/extensions/privacy-security/).

* * *

Please do not hesitate to contact Gib Mullan, Shannon Weinberg, or Brian McCullough at (202) 225-2927 if you have any questions with respect to this hearing.

Questions for the Record
November 14, 2011
Consumer Attitudes on Privacy
Questions for Ms. Barbara Lawler

The Honorable Mary Bono Mack

1. **Intuit offers its customers both paid services, such as Quicken and TurboTax, and free services, such as Mint. Which service has more users and is there a growth trend toward one or the other? How does Intuit offer Mint at no cost to the consumer? How is Mint user information used to underwrite the free service? Do Mint users understand the quid-pro-quo that funds the free service?**

Mint is our free online personal financial management product, and is offered in addition to our traditional paid service Quicken. Currently, 8 million people claim to use Quicken, while a little over 6 million use Mint. Intuit is committed to growing the new Mint platform over time, so we expect those numbers to increase. There is an alternative value exchange associated with Mint. Customers do not pay to use the service, but they agree in the provision of the service to receive relevant offers from third party financial institutions that may help them save money by securing a better interest rate or a cheaper loan. Those offers are presented within a unique page in the product. The customers' personal and financial data is not shared with the third party making the offers. Instead, Intuit maintains an in-house system for matching offers to potential customers. If a customer decides to take advantage of an offer, the customer themself makes a decision to interact directly with the third party at its website. This "beyond user paid" model is made explicitly clear to customers on our homepage when they first access for the service.

2. **Industry observers and users focus concern on the practice of behavioral advertising. Based on Intuit's consumer research, do you believe it is the behavioral advertising itself, the collection of information that drives the behavioral advertising, or the potential for sharing that information with unknown entities downstream that concerns most consumers?**

Based on Intuit's extensive research project gathering direct consumer feedback on data stewardship, we learned quite clearly that our customers' primary concern around privacy is the possibility that their data will be shared or sold to unknown third parties. In fact, those findings led us to specifically reiterate our long-standing commitment to safeguard all of our users' data. Additionally, we explicitly told them that we will not, without explicit permission, sell, publish or share data entrusted to us by a customer that identifies the customer or any person.

3. **Intuit offers its customers a variety of privacy options in its products. What percentage of Intuit customers view and manipulate the privacy options offered to them?**

One of Intuit's data stewardships commits that we will gives our customers choices about our use of data that identifies them. As such, we offer a range of choices in how customer data will be used and how we will communicate with them. We offer the ability to opt-out of marketing communication via postal mail, email, and telephone. The opt-out rates are generally very low, and differ according to the type of customer making the choice – traditionally, only .1 % our small business customers choose to opt out, while .25% of individuals consumers do so. (Do we

want to add data re: Opt –in in TurboTax based on 7216 requirements and how high that is? As written it sounds like we only offer opt-out. Need to somehow adjust this answer)

Moving forward, as our product and service offerings evolve we are expanding our current choice framework to additionally offer rich, in-context data use choices within our online and desktop products.

Understanding Consumer Attitudes Towards Privacy

Additional Questions for the Record

To: Mr. Michael Hintze, Associate General Counsel, Microsoft Corporation

From: The Honorable Mary Bono Mack

1. ***You testified more than 435,000 Microsoft users visit the "Advertisement Choice" webpage each month to adjust their preferences about the ads they see. You also testified that approximately 20 percent of these users choose to opt out of personalized ads. Do you believe the remaining 4 out of 5 Microsoft users who visit the preference webpage knowingly choose to receive targeted advertisements? Do you believe this is representative of most consumers' preferences?***

Microsoft Response: It is difficult to know why some users who visit the "Advertisement Choice" webpage choose to opt-out of personalized ads and some do not. Undoubtedly, some users who visit this page are simply looking for more information about how online advertising works. Some of those may conclude they prefer to see ads that are personalized and more relevant, or that they do not have an issue with receiving personalized ads. Others may decide to leave without making a choice with the anticipation of coming back later. Still other users may see the other controls available, such as the ability to modify interest categories, and choose to use those controls instead of opting out of personalized advertising altogether.

2. ***Some industry observers have opined that consumers may not be able to express their true privacy preferences because the choices presented are difficult to understand and often found only in a complicated and lengthy privacy policy, or because the tradeoff costs are in the future. Do you have any concern that some consumers become confused or are unable to understand the choices presented to them and therefore avoid making a decision? Do you have any consumer feedback on their level of understanding of the choices presented to them?***

Microsoft Response: Yes. Providing useful and understandable privacy-related information to consumers can be challenging – particularly when such information involves complex technologies and/or business models. We have learned over the years that while a detailed privacy statement is necessary, it is not sufficient as a means of providing the information consumers need to make informed decisions. This is why we have sought to provide information to consumers in a variety of ways – often influenced by user testing and consumer feedback about what is working and what is not.

For example, in order to provide useful information in a more consumable format, we were one of the first companies to adopt a so-called "layered" privacy notice – with a high level summary and key disclosures on a single page, with links to the longer, full privacy notice for those

consumers who want more detailed information. The design of our layered notice was based on the feedback from focus groups that we conducted with several groups of consumers.

We have also incorporated privacy information into our products and services in different ways, with an eye toward presenting information at the time in a context that it is relevant, understandable, and actionable. Sometimes this means providing information and presenting choices when a product is first installed. Sometimes it means doing so when a consumer chooses to use a particular feature for the first time.

While it remains an ongoing challenge to provide understandable and usable information to consumers, we believe that by utilizing multiple strategies to make that information available, we can help empower consumers to make more informed choices about the products and services they use and about how they use them. Microsoft will continue to explore way to improve the way we communicate and provide information to consumers with the goal of making that information understandable.

3. ***Regarding Internet Explorer's "Do Not Track" tool, you testified that certain content on websites provided by a third party, such as a map or web beacon, could still automatically send consumer information to a third party content provider. Please explain this technology, and why the Do Not Track tool is not an effective blockade against it. Please also explain whether this technology is a tool for websites to use third party content to intentionally circumvent information sharing blocking features, or a necessary feature to provide consumer content.***

Microsoft Response: Let me clarify. With the Tracking Protection feature of Internet Explorer 9, consumers are empowered to block content from any or all third parties on a website – thereby effectively preventing those third parties from automatically collecting any information from that consumer as a result of the visit to that website. Thus, Tracking Protection can be a very effective tool because it can prevent the connection to the third party and thereby block data collection – rather than merely sending a do-not-track signal and relying on the third party to read, interpret and respect that signal.

Whether any particular third party is able to automatically collect information directly from the user depends on whether that third party appears as a blocked domain on a Tracking Protection List that the user has chosen to install. So when a user visits a website, it is very possible that some third parties will be blocked (i.e. those that are blocked by a Tracking Protection List the user has installed) while other third parties appearing on that page will not be blocked and therefore remain able to automatically collect information.

More information on how the Tracking Protection feature works is available at: http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/features/tracking-protection.

4. ***You testified that data security is among the focal points of the Self Regulatory Program for Online Behavioral Advertising, and participating organizations must adhere to the security requirements and limit their data retention of information collected for behavioral advertising. What are the security requirements? What is the data retention time limit?***

Microsoft Response: The Self-Regulatory Program for Online Behavioral Advertising requires that "[e]ntities should maintain appropriate physical, electronic, and administrative safeguards to protect the data collected and used for Online Behavioral Advertising purposes." With regard to data retention, the Program does not set a particular timeframe, which is appropriate given that the retention needs can vary depending on the context or purposes for which the data was collected. Instead, it states that "[e]ntities should retain data that is collected and used for Online Behavioral Advertising only as long as necessary to fulfill a legitimate business need, or as required by law." The DAA, the organization that is administering the Self-Regulatory Program will be able to provide further clarification.

5. ***You described a new feature in your testimony, the Personal Data Dashboard, where consumers can adjust settings and decide how their information can be used. You also testified that 22,000 users visited their dashboard page in August. What percent of these users adjusted their settings?***

Microsoft Response: To use our most recent numbers, in October, there were approximately 32,000 visits to the Personal Data Dashboard. Of those, around 24% adjusted one or more settings.

EVIDON

November 14, 2011

VIA EMAIL

The Honorable Mary Bono Mack
Chairman
Subcommittee on Commerce, Manufacturing, and Trade
House Committee on Energy and Commerce

The Honorable G. K. Butterfield
Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade
House Committee on Energy and Commerce

Re: ***Response of Scott Meyer, CEO, Evidon, Inc., Hearing entitled "Understanding Consumer Attitudes About Privacy" Before the House Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, October 13, 2011***

Dear Chairman Bono Mack,

Thank you for the opportunity to appear before the Subcommittee to discuss consumer expectations in the context of online advertising. As requested, I am pleased to respond to the following questions for the record.

Rep. Bono Mack's Follow-Up Questions for the Record

1. **Evidon has a tool called "Ghostery" that users can download for their web browser and block third party tracking. Please describe how Ghostery works and how many consumers on average download the tool each month.**

Evidon's Ghostery is a free browser tool available for Firefox, Chrome, Safari, Opera, and Internet Explorer. Ghostery allows consumers to see which companies are tracking them on any web page they visit, and allows consumers easy access to more information about those companies, and links to their privacy policy and opt-out page, if available. Additionally, Ghostery provides users with the option to block any or all known trackers.

Ghostery works by scanning a webpage a user is visiting for scripts, pixels, and other elements that are responsible for placing cookies on the user's browser. It notifies the user of the companies whose code is present on the page. These page elements typically are not otherwise visible to the user, and often not detailed in the page source code. Ghostery presents information on these page elements in a more user-friendly format that allows users to learn more about these companies and their practices, and block detected page elements from loading if the user chooses. To help Ghostery identify new trackers, users can opt-in to a feature called GhostRank, which collects completely anonymous information about trackers that users encounter as they browse the Internet. Evidon uses data from GhostRank to assist advertisers to provide better

transparency and control to visitors to their websites and to populate relevant information used to deliver the AdChoices Icon.

Ghostery is currently downloaded approximately 140,000 times per month, and has been downloaded a total of over 4.5 million times.

2. When a consumer clicks on the ad icon and opts out of advertising by participating companies, what are they opting out of? Are they denying a cookie that would collect information, or are they simply opting out of the delivery of ads based on that information linked to their online behavior?

Companies use cookies in a variety of ways related to online advertising. It is important to note that cookies themselves do not actually collect any data. Rather, cookies typically contain information that is simply used to identify a particular web browser. Once a web browser is identified, companies may collect information about that browser for a variety of purposes. One purpose may be the collection of information relevant to the delivery of interest based advertising. Another purpose may be for advertising quality control, to ensure that the same browser is not served the same advertisement continuously. Other purposes include order tracking and user authentication, among a host of other non-advertising related activities.

Some companies will set separate cookies for separate tracking purposes, while others will reuse the same cookie for multiple purposes. Similarly, some companies may use data they collect solely for the delivery of interest based advertising, while others may also use that data for advertisement quality control or other purposes. Thus, opting-out of data collection for all purposes is generally unfeasible, as companies collect data about particular web browsers for a host of non-interest based advertising purposes.

When a consumer opts-out via the Advertising Option Icon, that consumer is opting-out of the *use* of data collected about them by a company to deliver interest based advertising. In many cases, that consumer is also opting-out of the collection of data about them for the purposes of delivering interest based advertising. In most cases, this opt out takes the form of a company-specific cookie that signals to that company that the consumer has opted-out. Generally, companies reading the cookie will honor the opt-out of data use, but many honor the opt-out of data collection as well.

Additionally, it is worth noting that on November 7, 2011, the Digital Advertising Alliance announced multi-site data collection principles that significantly expand the scope of industry self-regulation of online data collection beyond interest based advertising. The new principles establish comprehensive self-regulatory standards governing the collection and use of data collected from a particular computer or device regarding web viewing over time and across non-affiliated websites. The new Self-Regulatory Principles for Multi-Site Data can be found at http://www.aboutads.info/principles.

EVIDON

3. **In your testimony you stated that since October 2010, over 85 billion ads featured the "Advertising Option" icon. Of those impressions, consumers clicked the icon 4.5 million times and submitted 730,000 opt-out requests. Other than the consumers who have submitted the 730,000 opt out requests, can you tell whether the remainder of those who clicked on the icon explored beyond the initial click? In other words, do you know if consumers just "give up" after the initial click? Do you see any trends in how often consumers click the icon and how often they opt out?**

First, I would like to provide some updated numbers: We have now served over 105 billion Advertising Option Icons, which have been clicked on 5.5 million times. Of these 5.5 million clicks, 2 million proceed to the opt-out page, so far resulting in 828,000 opt-out requests from 110,000 consumers. Clicks on the Advertising Option Icon also have resulted in 1.7 million clicks going to the advertiser's privacy policy, and 740,000 clicks going to a site to learn more about interest based advertising. Although we do not know whether each click represents a different, unique consumer, our metrics suggest that many, if not most, consumers who click on the Advertising Option Icon do indeed explore beyond the initial click in some way and do not simply "give up" after the initial click.

Let me also note that approximately 76,000 consumers have visited Evidon's global opt-out page[1] directly, resulting in over 5 million additional opt-outs.

Evidon continues to conduct research on trends in our metrics. While we do not have any specific data ready to share at this time, we would be happy to update your staff as additional information becomes available.

****

Again, thank you for the opportunity to testify before the Subcommittee, and please feel contact me if you have additional questions.

Sincerely,

Scott Meyer
CEO
Evidon, Inc.

cc: The Honorable Fred Upton, Chairman,
House Committee on Energy and Commerce
Henry Waxman, Ranking Member,
House Committee on Energy and Commerce

[1] *Manage Your Online Profile*, EVIDON, http://www.evidon.com/consumers/profile_manager#tab3.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED TWELFTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225-2927
Minority (202) 225-3641

October 31, 2011

Ms. Linda Woolley
Executive Vice President
Washington Operations
Direct Marketing Association
1615 L Street, N.W., Suite 1100
Washington, D.C. 20036

Dear Ms. Woolley,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on October 13, 2011, to testify at the hearing entitled "Understanding Consumer Attitudes Towards Privacy."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for 10 business days to permit Members to submit additional questions to witnesses, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and then (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please email your responses, in Word or PDF format, to the legislative clerk (Alex.Yergin@mail.house.gov) by the close of business on Monday, November 14, 2011.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Mary Bono Mack

Mary Bono Mack
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: The Honorable G. K. Butterfield, Ranking Member,
Subcommittee on Commerce, Manufacturing, and Trade

Attachment

The Honorable Mary Bono Mack

1. **Do you believe the average consumer understands the relationship between Internet advertising and free web content?**

   We believe consumers do not fully understand or appreciate how online advertising supports their Internet experience or funds the development of new services and products. Revenues from online advertising support and facilitate e-commerce and subsidize the cost of content and services that consumers value, such as online newspapers, blogs, social networking sites, mobile applications, email, and phone services.

   To help consumers understand how online advertising supports their access to wealth of online resources for free or at a low cost, the Digital Advertising Alliance (DAA) is developing an educational campaign to explain how advertising supports the vibrant online experience that consumers have come to expect and demand.

2. **Do you know how many consumers take advantage of the opt-outs available on your members' individual websites?**

   Since the launch of the program, visits to www.AboutAd.info (DAA's website) has significantly increased and the Advertising Option Icon has become the predominant driver of this traffic to the web site. In December 2010, there were about 4,300 page views per week, with close to 36% of visitors to Aboutads.info coming from a referral (presumably an icon or an interstitial linked from the icon). In November 2011, there are more than 65,000 page views per week, and 87% of these visitors to AboutAds.info come from a referral site. This is an increase of more than 1500% and is tied directly to the broad adoption and proliferation of the icon. There are more 300 companies licensed to use the icon. There have been more than 2.7 million pages views since the launch, about 26% have resulted in a consumer exercising choice through the DAA program. Very soon, the DAA will launch a consumer education campaign around the Advertising Option Icon. We expect that through this campaign, consumers will come to better understand that entities involved with delivering a particular ad are subject to a self-regulatory code that provides effective consumer transparency and choice.

3. **We heard both Professor Acquisti and Intuit's Chief Privacy Officer testify that consumers believe privacy policies are too complicated and, consequently, they do not read the policies because it takes too much time to read through them or they often do not understand them. While some argue companies should move toward shorter and simpler privacy policies, we hear concerns from privacy advocates that there is a lack of transparency in shorter and simpler policies. What is industry doing to bridge the gap and provide full disclosure without alienating the average consumer who is not a privacy professional?**

   We believe privacy policies should be easy to find, read, and understand. For this reason, the DAA's Self-Regulatory Principles for Online Behavioral Advertising ("Principles") call for companies to provide consumers with clear, meaningful, and prominent notice on their

websites of their data collection and use practices. Furthermore, to make notices easier to locate, the DAA Principles call for companies to provide enhanced notice via the Advertising Option Icon that links directly to a disclosure about the company's advertising practices. Embedding notice in the ad pulls notice out of the privacy policy and makes disclosures easily detectable to consumers.

With the DAA's Self-Regulatory Program now underway, the icon is becoming a ubiquitous sight across the Internet. Based on information from participating companies, we estimate that tens of billions of icons are being delivered to consumers every single day; the icon was served in over 600 billion ad impression in August alone.

4. **The information sharing principles you described in your testimony seem to align with the results of the direct consumer research Ms. Lawler described in her testimony. However, principles are only effective if companies abide by them and if consumers trust that companies will abide by them. How can consumers have confidence that their information is being treated properly and with respect for consumers' stated privacy preferences when stories of the opposite are frequent (e.g., the recent stories on super cookies that remove a consumer's ability to choose whether or not to be tracked)?**

The DAA prohibits companies from using technology to subvert preferences expressed by consumers. Participants in the DAA Program should provide consumers with control over the collection of data and how it is used; and participants should honor these preferences.

Consumers can be confident that the DAA program is backed by credible accountability programs to help ensure participants are adhering the Principles. The Direct Marketing Association (DMA) and the Council of Better Business Bureaus (CBBB) have longstanding, effective and respected compliance programs that are being leveraged to enforce compliance with the Principles. The DMA and CBBB enforcement programs are alerted to concerns through a combination of technological monitoring across the Internet and complaints that may be filed by consumers, competitors, government agencies, and others. Based on these alerts, the programs examine complaints and evidence, and then work with companies to help them come into compliance with the Principles. Decades of self-regulation show that this is an effective and efficient way to change company behavior.

Since the hearing, six enforcement actions have been brought against and settled with companies engaged in online behavioral advertising.[1] Both accountability programs continue to receive and investigate complaints

[1] http://www.bbb.org/us/article/accountability-program-achieves-voluntary-compliance-with-online-behavioral-advertising-self-regulation-30529.

5. **You referenced in your testimony the concerns of some Members of Congress that information gathered for the purpose of driving targeted ads could be used for other, more sensitive purposes as employment, credit, or health coverage decisions. You emphasized that these do not reflect actual business practices. However, while we often hear that the information collected to drive ads is anonymized, recent news stories regarding Visa and MasterCard plans to target online ads to consumers based on offline credit purchase habits suggest that the information collected is personally identifiable to some extent. Is the data your members use to target ads anonymized? If so, at what point in the data custody chain?**

   The DAA's Principles do not distinguish between personally identifiable information and non-personally identifiable information. Instead, DAA chose to design its principles more broadly to apply to all data collected and used for online behavioral advertising purposes. We chose this approach because the data collected online for advertising purposes is not personally identifiable information. We wanted to ensure the types of data used for online advertising was appropriately covered. To the extent personally identifiable information is accessible, as a practice, companies routinely use de-identification process (e.g., hashing data elements) to remove personally identifiable information from the data chain prior to developing segments for advertising purposes.

   In addition, on November 7, 2011, the DAA released "Principles for Multi-Site Data" that significantly expand the scope of self-regulation of online data collection beyond online behavioral advertising (OBA). The new Principles establish comprehensive self-regulatory standards governing the collection and use of Multi-Site Data, data collected from a particular computer or device regarding Web viewing over time and across non-affiliated Websites. In addition, these new principles also codify existing industry practices prohibiting the collection or use of Multi-Site Data for the purpose of any adverse determination concerning employment, credit, health treatment or insurance eligibility.

6. **How does Internet advertising support small businesses? Do you think government regulation would disproportionately impact small businesses?**

   Internet advertising is vital for new start-up companies and small businesses to reach potential customers. Smaller websites cannot afford to employ sales personnel to sell their advertising space, and may be less attractive to large brand-name advertising campaigns. Internet advertising, and in particular interest-based advertising, helps small companies to overcome these challenges. In the online advertising ecosystem, small website publishers can increase their revenue by featuring advertising that is more relevant to their users. In turn, advertising-supported resources help other small businesses to grow.

Internet advertising has also opened larger markets to small business by lowering the barriers to entry, and has created national markets for previously local, regional, or niche business models. This increased competition encourages innovation and leads to lower prices, all to the direct benefit of consumers.

Government regulation could negatively impact small business as well as the Internet economy as a whole. Small businesses, with a lack of resources to manage complex regulatory mandates, would likely forgo many rich online opportunities.

We believe self-regulation and education constitute the most effective framework for protecting consumer privacy while ensuring the Internet remains a platform for innovation. We also believe that legislative solutions inevitably would be too inflexible to respond appropriately to the rapidly developing technological environment, thus seriously impeding innovation. In addition, laws should not dictate a framework or impose requirements for the operation of self-regulatory mechanisms. Such an approach would inhibit industry's ability to efficiently respond to a developing marketplace and foster innovation on the Internet.

7. **What role, if any, do you see the government playing in the enforcement of the self-regulatory program?**

Government currently plays a vital enforcement role for self-regulation. If a company fails to cooperate voluntarily with the accountability programs, the programs can publicize the violation and refer the issue to government authorities for further investigation. Companies that claim to adhere to the Self-Regulatory Principles, but fail to do so, risk liability for deceptive acts or practices.

* * *

November 14, 2011

Dr. Alessandro Acquisti
Associate Professor of Information Technology and Public Policy
Heinz College
Carnegie Mellon University
5000 Forbes Avenue HBH 2105C
Pittsburgh, PA 15213

Dear Dr. Acquisti,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on October 13, 2011, to testify at the hearing entitled "Understanding Consumer Attitudes Towards Privacy."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for 10 business days to permit Members to submit additional questions to witnesses, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and then (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please email your responses, in Word or PDF format, to the legislative clerk (Alex.Yergin@mail.house.gov) by the close of business on Monday, November 14, 2011.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Mary Bono Mack
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: The Honorable G. K. Butterfield, Ranking Member,
Subcommittee on Commerce, Manufacturing, and Trade

Attachment

The Honorable Mary Bono Mack

1. **In your testimony, you referenced "privacy enhancing technologies" that can be used to protect, aggregate, and anonymized consumer data. Do you believe most consumers are comfortable with websites collecting their information if it is truly protected and anonymized?**

AA: It is likely that consumers would be *more* comfortable if they knew that the information websites collected about them was handled anonymously, rather than being identified. This belief is based on the results of numerous recent surveys, reporting significant and widespread distrust across US consumers towards tracking technologies that individually identify them, and the companies that use those technologies.[1] Since privacy enhancing technologies allow personal data to be protected (for instance, through anonymization or aggregation) without jeopardizing the main purpose of an application or a transaction, consumers are likely to be more comfortable with websites that adopt those technologies.

2. **Do you believe the average consumer understands the relationship between Internet advertising and free web content?**

AA: The relationship between free content and advertising is actually rather complex – hence, I believe that consumers have only limited information about, and awareness of, that relationship. Economists like to say that there is no such thing as a free lunch. In fact, web content is not really free for the end consumer. First, consumers are aware that the pay to *access* the Internet: monthly subscriptions to ISPs, data plans with mobile carriers, charges for wi-fi spots in public locations, employers' Internet plans, and so forth. Second, when accessing online content, Internet users pay as *consumers*: through the products and prices that they are nudged to accept, based on the information firms have about them.

The Honorable G. K. Butterfield

1. **At the hearing, Linda Woolley of the Digital Adverting Alliance testified that the cost to the U.S. economy from adoption of a European style privacy regime, including "Do Not Track" and "do not use cookies," would be "$33 billion a year."**

---

[1] Consider, for instance, J. Tsai, P. Kelley, L. Cranor, and N. Sadeh, 2009. "Location-Sharing Technologies: Privacy Risks and Controls." Telecommunications Policy Research Conference (TPRC); J. Turow, J. King, C. Hoofnagle, A. Bleakley, and M. Hennessy, 2009. "Americans Reject Tailored Advertising and Three Activities That Enable It." Available At SSRN: http://ssrn.com/abstract=1478214; and A.M. McDonald, and L.F. Cranor, 2010. "Americans' Attitudes About Internet Behavioral Advertising Practices." Workshop On Privacy In The Electronic Society (WPES).

a. **At a hearing on Sept. 15 titled "Internet Privacy and the EU," Prof. Catherine Tucker provided a similar figure spread over a five-year period that she stated was derived by another group based on her study of the effects of the e-Privacy Directive on advertising effectiveness. Prof. Tucker stated:**

b. **"The first key finding is that the e-Privacy Directive was associated with a 65 percent decrease in online advertising performance, the advertisers that I studied. This is a sizeable decrease, and I think the best way of understanding it is that if an ad is not targeted appropriately, consumers online are really very good at ignoring it. . . . [W]hat does this 65 percent mean in real terms for American businesses? Well, the public policy group NetChoice took the estimates of my study to project that EU style regulation could cost U.S. businesses $33 billion over the next 5 years. So this is obviously a large negative effect."**

c. **NetChoice's projections can be found at www.netchoice.org/library/estimate-of-us-revenue-loss-if-congress-mandated-opt-in-for-interest-based-ads.**

2. **Assuming that Ms. Woolley and Prof. Tucker were both referring to the same projections, and to the extent you are familiar with Prof. Tucker's original study, please discuss your concerns with both of these estimates and whether they provide any real information about the potential impact to the U.S. economy from the specific regulatory mechanism under consideration in that study.**

AA: I will provide separate answers for Professor Tucker and Professor Goldfarb's original study, which is a well-researched, rigorous, peer-reviewed manuscript, and NetChoice's calculations, which lack those traits.

I did not find NetChoice estimates credible. As NetChoice states, the estimates are based upon "taking a forecast of US online interest-based ad revenue, then reducing that by the decline in advertising effectiveness experienced in the EU." In my opinion, this approach is flawed for a number of reasons:

- NetChoice claims that "American websites would lose" $33 billion over the next 5 years. However, Tucker and Goldfarb's study merely focused on the fact that "privacy regulation decreased the effectiveness of online advertising by about 65 percent." Clearly, this statement does not imply that advertising revenues (or sales of goods for that matter) will decrease by 65% - as implied by NetChoice's estimates. In fact, NetChoice's estimates assume that changes in advertising efficacy will not cause any change in advertisers' aggregate behavior. In reality, as Tucker and Goldfarb (the authors of the original study) carefully and correctly note, advertisers could react by spending more (from $8B to $14.8B) in advertising (hence, bringing more money to websites), in order to obtain the same increase in stated purchase intentions; or they could react by spending less (from $8B to $2.8B).

- The estimate also makes unrealistic predictions about the growth of ad revenues over time. The estimates assume that ad revenues will more than double in just 5 years (2010-2015) –

which is implausible, considering that ad revenues have been increasing at about 11% per year.[2]

- Furthermore, the $33 billion estimate was presented as a cost "to the American economy" during the hearing. This statement is predicated around the incorrect assumption that, without targeted ads, $33 billion dollars would have just evaporated from the economy. In reality, consumers would still spend that money on other goods (for instance, purchasing products advertised via more traditional online technologies), or save them and invest them into other channels.

3. To the extent you are familiar with Prof. Tucker's study, are there any other thoughts regarding the study that you would like to share with the Subcommittee?

AA: The methodology employed in Tucker and Goldfarb's study is rigorous, and the authors have been careful in properly framing their results. Some industry reports, however, have stretched those results, reaching unwarranted conclusions.

First, the study is based on stated purchase intentions: purchase intentions are poor predictors of actual purchases. Hence, the magnitude of the effects reported could be radically different (for instance, dramatically smaller) in terms of actual sales.

Second, as noted above, based on the estimated 65 percent decrease in advertising effectiveness, the study presents one scenario, which the authors rightly and carefully label "worst-case" scenarios. Advertisers could spend more (from $8B to $14.8B) in order to obtain the same increase in stated purchase intentions. However, as the authors note, the advertisers could also ending up spending less (from $8B to $2.8B). The reason for this ambiguity is that the actual economic impact of the purported decrease in ads effectiveness cannot be estimated without an equilibrium model. Hence, the numerical estimates presented in the paper represent one single scenario – as the authors correctly pointed out. Among the other possible scenarios, some predict a decrease in the advertising expenditures, and yet others predict no net change.

Third, and most importantly, the reported impact on advertising effectiveness is limited to a specific, and narrow, set of ads. As the authors carefully point out, the conditions under which lack of behavioral tracking was found to reduce advertising effectiveness were limited to cases in which: the page on which the ads appeared was general-content, instead of domain/topic specific-content; or, the ad was small; or, ad was static (rather than dynamic or media-rich). This implies that regulation did not have any negative impact on advertising effectiveness for a large proportion of ads considered in the study: that is, larger ads, dynamic and/or media-rich ads, or ads on content-specific pages (i.e., contextual ads that are targeted to consumers based on the content of the site – e.g. car ads on car websites).

[2] See http://mashable.com/2010/10/12/internet-ad-revenues-2010/.

4. **At the hearing, you were asked to discuss a study you contributed to that combined *off-the-shelf* facial recognition technology and publicly available information to infer more sensitive information about individuals. As you described it, you started with nothing more than a picture of a face; you matched that face picture to a face picture on a profile on a social networking site like Facebook, which in turn allowed you to infer a name and to uncover personal demographic information such as a date of birth and hometown; and these bits of information lead finally to the inference of sensitive information: a social security number.**

   This is one of the studies you have contributed to that demonstrates that consumers' ability to make rational and fully informed decisions about their privacy preferences is constrained both by humans' limited ability to (1) process the information available to us, and (2) understand or predict the implications of advances in technology.

   At the hearing, there was a discussion about other existing ways of uncovering the same personal demographic information from which sensitive information could be inferred and a suggestion was put forth that this new technology may not create new privacy problems.

   a. **To the extent you were constrained by the time allowed to respond at the hearing, can you please explain why the combination of new technologies, the speed of their deployment, and the easy and widespread access to information about individuals online do create new privacy concerns that are distinguishable and more significant than when the same information is available offline?**

AA: First, our study highlighted the increasing ability of online firms to extract sensitive information starting from publicly available, or merely non-sensitive, information. The field of statistical re-identification, in recent years, has shown that it is possible to start from personal but not sensitive data about a person, and infer from that more private, and much more personal, information. This is possible because consumers activities are tracked across different sites; those different trails of data can be then combined, and sophisticated statistical models can be applied to form detailed pictures of an individual's behavior, traits, preferences, and desires.

Second, the scenario we discussed in our study (in which we started from a photo of an individual and ended up predicting her SSN) is just one example of many others sensitive predictions which are becoming possible based on publicly available data, or on data advertisers and websites collect about Internet users. More generally, our results show that it is possible to start from an anonymous face in the street, use face recognition to compare that face to identified online photos (from services such as Facebook, Linkedin, and so forth) in order to assign a name to that face; then use online "white pages" services to find information about that person (for instance, demographic information, or social media profiles – what we may call "public data"); and finally, make much more sensitive statistical inferences based on said public data (for instance, that person's SSNs, but also – potentially - her credit score, her sexual orientation, and so forth; what we may call the "inferable information").

Third, our experiment shows that it is possible to do these inferences in real time, cheaply, and on end-consumers device (such as smartphones). This is what we referred to, in our study, as the

"democratization" of surveillance. The converge of different technologies (online disclosures and online tracking; face recognition; statistical re-identification) is bringing us closer to a world where individuals in the street may infer personal, private, and even sensitive information about each other in real time, simply using a smartphone connected to the Internet. Due to the speed at which these technologies are evolving, what we realized as a proof of concept today, may become available as a mass-scale consumer product tomorrow.

These scenarios raise particular concerns because they challenge our natural expectation of being anonymous in a crowd or among strangers. As consumers, we are likely unprepared for these developments for two reasons: we are not used to expect that strangers in the street could know our names; and we are not used to expect that innocent pieces of information we revealed about ourselves can be combined to make much more sensitive inferences about our behavior, preferences, and desires.

b. **If consumers do not know and cannot know everything they need to know to make effective decisions about their privacy, do you have any thoughts about what can be done either at a technological design or policy level so that consumers' true privacy preferences can be carried out?**

AA: In terms of policy, it would be helpful to consider a regulatory framework which 1) fosters the development and the deployment of privacy enhancing technologies by online firms and in end users' services; 2) establishes consequences for the abuse of consumer data which can act as actual deterrents of privacy violating behaviors (as opposed to merely being internalized as the cost of doing business with consumer data).

5. **At the hearing, members of the Subcommittee raised the question of what the harm was to consumers from having their online activities tracked, aggregated, and profiled. In particular, one line of questions asked about what harms could come if an individual went online to search out information about Alzheimer's. That line of questioning was raised again later in the hearing, and an additional issue was put into the mix: "when does reputational harm then translate into physical harm?"**

   a. **To the extent that you, other privacy experts, or consumers believe that privacy is a right, can you please discuss why harm to consumers should not be a precondition to requiring that consumers' privacy be protected? In addition, if privacy is a right, can you please discuss why the erosion of privacy and how much we value privacy is itself a harm?**

AA: Privacy is becoming less about the control over personal information, and more about the control that others can have over you, if they have information about you. If information is power, then control over person information can imply the potential for control over the person.

Such power may not necessarily be used maliciously. However, in absence of clear safeguards, we cannot be sure that this power will be always be used in favor of the consumer, either.

Expecting a quantifiable harm as a prerequisite for consumer's protection ignores this dimension of privacy protection as a protection against control, and abuse. Furthermore, many privacy harms are, in actuality, hard to quantify: some privacy harms may be invisible to the consumer (for instance, price discrimination); some privacy violations may lead to economic damage only later in time (for instance, when identity theft happens several months after a database has been breached).

As for the issue of how "privacy is a right, can you please discuss why the erosion of privacy and how much we value privacy is itself a harm?," in a series of experiment at Carnegie Mellon University we have found that the erosion of privacy can also negatively impact individuals' valuations of privacy, creating a self-fulfilling circle of privacy "devaluations."[3] Specifically, in one of our experiments, the number of subjects willing to reject cash offers for their data was both significant in absolute terms and much larger in relative terms when the subjects felt that their data was, by default, protected, than when they believed that their data would be, by default, revealed. The latter condition is arguably the one more likely to reflect consumers' actual beliefs and fears about the current state of privacy protection. Our results therefore imply that when consumers feel that their privacy is protected, they value it much more than when they feel their data has already been, or may be, revealed.

b. Setting aside that privacy is a right, can you please discuss other harms that could result from the online collection, aggregation, and profiling of consumers, with or without their knowledge, including such things as boxing, differential pricing, and lost employment, housing, and other economic opportunities?

AA: The Alzheimer's quote from the hearing offers a good example of the hidden potential costs of privacy. A health insurer who gets access to my search records and discovers my interest in Alzheimer may increase my insurance premium, because it conjectures that I am an individual at risk. An employer may decide not to hire me, as it conjectures that soon I may not be productive. A lender may decide not to give me credit, as it conjectures that I may not be able to repay my debts. An advertiser may repeatedly target me with ads about expensive remedies with dubious efficacy, catching me when I am most credulous, and vulnerable.

Since most of these things can happen without the individual even knowing how much information has been gathered by different sites, how that information has been combined across sites, and then how it has been used, it becomes difficult for consumers to make "good" decisions about their data. It becomes also difficult for the law to prove that acts of

[3] "What is Privacy Worth?," Alessandro Acquisti, Leslie John, and George Loewenstein. Workshop on Information Systems and Economics (WISE), 2009.

discrimination have taken place, since the process through which the discrimination became possible may well remain invisible to the consumer herself.

c. **Ms. Woolley suggested that privacy and data security are separate issues, stating: "we need to be very careful about separating out privacy issues from data breaches. . . . data breach issues I think require some significant action by Congress." Can you please discuss why consumer privacy and data security are actually closely connected?**

AA: Data breaches are example of security incidents which lead to privacy invasions. For instance, breached data is later used for identity theft, blackmailing, and abuse.

This means that poor security leads to poor privacy. Hence, the two concepts are intimately connected.

Privacy can be strengthened with more data security. Furthermore, it is not necessarily the case that increased security must come at the cost of less privacy: As discussed in my testimony, privacy enhancing technologies can increase the security of a system while at the same time protecting identifying or sensitive data of the users of the system.

6. **At the hearing, the following question was posed to all the witnesses on the panel: "[I]s 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?" Unfortunately, you did not have an opportunity to respond.**

   a. **Can you please provide an answer to this question? In doing so, please elaborate as necessary to fully explain your answer, including providing any other information you believe would help the Subcommittee understand the role of online tracking and behavioral advertising in supporting the availability of free online content.**

AA: First, free content proliferated online before the advent of the more intrusive practices associated with behavioral targeting and targeted advertising. This suggests that the existence of free online content is not predicated around the existence of practices such as targeted advertising.

In fact, we are not aware of empirical investigations determining how much, and in what proportions, behavioral tracking and online tracking are benefitting the sellers (that is, companies that sell product), the buyers (that is, consumers, in the form of more free content or lowered search costs for products) or, in fact, the middlemen.

As for the issue of 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, two studied we conducted at CMU show that consumers, under proper conditions, will pay for privacy and to avoid being tracked. One such experiment was cited above.[4] The second experiment was mentioned as part of my testimony: In an experiment with actual cash incentives and real privacy/monetary trade-offs, my co-authors and I investigated whether more prominent, salient, and straightforward information comparing the data handling strategies of different merchants will cause consumers to incorporate privacy considerations into their online purchasing decisions. We designed an experiment in which a shopping search engine interface clearly and compactly compared privacy policy information for different merchants. When such information was made available, consumers tended to purchase from online retailers who better protected their privacy. In fact, our experiment indicated that when comparative privacy information was made more salient and accessible, consumers were willing to pay a *premium* to purchase from more privacy protective websites.[5]

The question was prefaced by the comment that the Federal Trade Commission has in its ongoing work regarding consumer privacy received comments suggesting the lack of a clear consensus about how consumers feel about online privacy protections.

b. **While there is no one uniformly held consumer attitude about online privacy, I understand that there are some consensus, and even widely-held, views by consumers about privacy and data collection practices. Can you please discuss these consensus and widely-hold views?**

AA: In general terms, consumers can hold heterogeneous preferences towards privacy. For instance, Alan Westin famously suggested that some consumers are privacy "fundamentalist" (they strongly believe that privacy is a right that and corporations and governments are interfering with); some are "unconcerned" (they see their lives as an open book); and some are "pragmatist" (they care for privacy, but expect to have to share information to function in modern society).

In reality, however, certain practice met the unambiguous disapproval of a vast majority of US consumers. For instance, there is a consensus among US consumers in terms of the concerns raised by tracking technologies. In a survey of 587 US adults about attitudes towards location-tracking techniques, Tsai et al. found widespread and elevated concerns about the control over data about individuals' location; generally, "respondents [felt that] the risks of using location-sharing technologies outweigh[ed] the benefits."[6] In a nationally representative survey about online behavioral targeting by marketers, Turow et al. found that 66% of US consumers did not

[4] See footnote 3.

[5] J. Tsai, S. Egelman, L. Cranor, and A. Acquisti, 2011. "The Effect Of Online Privacy Information On Purchasing Behavior: An Experimental Study." Information Systems Research, 22, 254-268.

[6] J. Tsai, P. Kelley, L. Cranor, and N. Sadeh, 2009. "Location-Sharing Technologies: Privacy Risks and Controls." Telecommunications Policy Research Conference (TPRC).

want marketers to tailor advertisements to their interests, and that the majority "mistakenly believe[d] that current government laws restrict companies from selling wide-ranging data about them."[7] Very similar findings were reported in a different study by CMU researchers about targeted advertising.[8]

5. **At the hearing, a member stated he was concerned that a study released in early October found that numerous websites were leaking identifying information to third-parties. That study by Stanford University law and computer science student Jonathan Mayer found that the majority of websites most heavily visited by Americans that offered a sign-up feature leaked personal information like user IDs, full names, or email addresses to third parties.**

   Ms. Woolley of the Digital Advertising Alliance dismissed this study, stating: "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."

   a. **Can you please explain what the problem of "leakage" is, including how long the problem has been known, its implications for consumers, the key findings in the literature on this topic, and what this latest study has contributed to the understanding of this problem?**

   b. **Can you please respond to Ms. Woolley's criticism of this study?**

AA: The study referred by Ms. Woolley is an empirical investigation of how personally identifying information can get "leaked" from first-party websites to third-party websites. This means, for instance, that merely viewing a local ad on the Home Depot website causes "the user's first name and email address [to be sent] to 13 companies," while "[c]licking the validation link in the Reuters signup email sent the user's email address to 5 companies."[9] This happens without the individual's knowledge or consent, and in some cases also in violation of the first-party site's privacy policy.

It is true that the study is not peer reviewed. However:

- It is not true that there was no methodology to the study. The methodology employed by the author was clearly described in the document made available by the author.
- Over the years, many other studies (including peer-reviewed ones) have found very similar results, highlighting how online consumer data is being tracked and combined across different online services in order to create more complete profiles of a given Internet visitor.

---

[7] J. Turow, J. King, C. Hoofnagle, A. Bleakley, and M. Hennessy, 2009. "Americans Reject Tailored Advertising and Three Activities That Enable It." Available At SSRN: http://ssrn.com/abstract=1478214.

[8] A.M. McDonald, and L.F. Cranor, 2010. "Americans' Attitudes About Internet Behavioral Advertising Practices." Workshop On Privacy In The Electronic Society (WPES).

[9] Tracking the Trackers: Where Everybody Knows Your Username by Jonathan Mayer, posted on October 11, 2011. http://cyberlaw.stanford.edu/node/6740.

For instance, Krishnamurthy et al (2011) examined "over 100 popular non-OSN Web sites [...] to see if these sites leak private information to prominent aggregators," and found that 56% of the sites directly leaked "pieces of private information with this result growing to 75% if we also include leakage of a site userid." For instance, "[s]ensitive search strings sent to healthcare Web sites and travel itineraries on flight reservation sites [were also found to be] leaked in 9 of the top 10 sites studied for each category."[10]

- Other studies have shown that websites deliberately circumvent P3P privacy policies,[11] or use "flash" cookies to 'respawn' or re-instantiate HTTP cookies deleted by the user.[12]
- In other words, there exists, unfortunately, a long list examples suggesting that self-regulatory approaches fail in limiting online firms' attempts at tracking and combining consumers data without consumers' knowledge and consent.

[10] See, for instance, Krishnamurthy, B., Naryshkin, K., & Wills, C. E., Privacy leakage vs. Protection measures: the growing disconnect, presented at W2SP 2011: Web 2.0 Security and Privacy 2011 (2011), available at http://www.cs.wpi.edu/~cew/papers/w2sp11.pdf; Krishnamurthy, B., & Wills, C., Privacy diffusion on the web: A longitudinal perspective, Proceedings of the 18th ACM international conference on World wide web (2009)(p. 541-550), available at http://portal.acm.org/citation.cfm?id=1526782.

[11] Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens, Pedro Giovanni Leon, Lorrie Faith Cranor, Aleecia M. McDonald, Robert McGuire, ACMWorkshop on Privacy in the Electronic Society (WPES 2010), October 2010.

[12] Soltani, Ashkan, Canty, Shannon, Mayo, Quentin, Thomas, Lauren and Hoofnagle, Chris Jay, Flash Cookies and Privacy (August 10, 2009). Available at SSRN: http://ssrn.com/abstract=1446862.