AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

BALANCING PRIVACY AND INNOVATION: DOES THE PRESIDENT'S PROPOSAL TIP THE SCALE?

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

MARCH 29, 2012

Serial No. 112–135

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

U.S. GOVERNMENT PRINTING OFFICE
81–441 PDF WASHINGTON : 2013

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

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
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
JOHN P. SARBANES, Maryland

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
JOHN P. SARBANES, Maryland
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. Fred Upton, a Representative in Congress from the State of Michigan, opening statement	7
Prepared statement	9
Hon. Marsha Blackburn, a Representative in Congress from the State of Tennessee, opening statement	11

WITNESSES

Lawrence E. Strickling, Assistant Secretary for Communication and Information, Department of Commerce	12
Prepared statement	14
Answers to submitted questions	200
Jon Leibowitz, Chairman, Federal Trade Commission	37
Prepared statement	39
Answers to submitted questions	210
Berin Szoka, President, TechFreedom	91
Prepared statement	94
Answers to submitted questions	216
Jonathan Zuck, President, Association for Competitive Technology	121
Prepared statement	123
Answers to submitted questions	246
Pam Horan, President, Online Publishers Association	137
Prepared statement	139
Answers to submitted questions	252
Michael Zaneis, Senior Vice President and General Counsel, Interactive Advertising Bureau	146
Prepared statement	148
Answers to submitted questions	256
Justin Brookman, Director, Consumer Privacy, Center for Democracy & Technology	162
Prepared statement	164
Answers to submitted questions	261

SUBMITTED MATERIAL

Statement, dated March 29, 2011 [sic], of the Consumer Electronics Association, submitted by Mrs. Blackburn	65
Statement, dated March 26, 2012, of Commissioner J. Thomas Rosch, Federal Trade Commission, submitted by Mrs. Bono Mack	187
White House report, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," dated February 2012, submited by Mr. Butterfield [1]	
Federal Trade Commission report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," dated March 2012, submitted by Mr. Butterfield [2]	

[1] The report is available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[2] The report is available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

BALANCING PRIVACY AND INNOVATION: DOES THE PRESIDENT'S PROPOSAL TIP THE SCALE?

THURSDAY, MARCH 29, 2012

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

The subcommittee met, pursuant to call, at 9:05 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, Harper, Lance, Cassidy, Guthrie, Olson, Pompeo, Kinzinger, Barton, Upton (ex officio), Butterfield, Gonzalez, Sarbanes, Waxman (ex officio), and Markey.

Staff present: Paige Anderson, Commerce, Manufacturing, and Trade Coordinator; Charlotte Baker, Press Secretary; Michael Beckerman, Deputy Staff Director; Andy Duberstein, Deputy Press Secretary; Kirby Howard, Legislative Clerk; Brian McCullough, Senior Professional Staff Member, Commerce, Manufacturing, and Trade; Gib Mullan, Chief Counsel, Commerce, Manufacturing, and Trade; Shannon Weinberg, Counsel, Commerce, Manufacturing, and Trade; Michelle Ash, Democratic Chief Counsel, Commerce, Manufacturing, and Trade; Felipe Mendoza, Democratic Senior Counsel; and Will Wallace, Democratic Policy Analyst.

Mrs. BONO MACK. The subcommittee will now come to order.

Good morning. Let me begin by saying thank you and welcome to our distinguished guests, FTC Chairman John Leibowitz and Assistant Commerce Secretary Lawrence Strickling.

I really enjoyed spending time with you recently at the White House, and I hope you both feel the same way about me after your getting grilled today. But seriously, though, you have been great to work with, and at the end of the day, we all want the same thing, to better safeguard consumer privacy. And the chair now recognizes herself for an opening statement.

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

Today, as we continue our yearlong series of hearings into online privacy, we are rapidly reaching the point where the rubber hits the road. When it comes to the Internet, how do we, as Congress,

as the administration and as Americans, balance the need to remain innovative with the need to protect privacy? And how hard of a shove would it take to tip that critically important balance in a way that hurts the U.S. economy, American consumers, or both?

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, but other times, it is not. After six privacy hearings, we have covered a lot of ground, and we have learned a lot about consumer concerns.

But today, I am still not certain legislation is necessary. I am still sceptical of the motives of both industry and government, and still leery that advancements like Do Not Track and eraser-button technology will work as intended.

Frankly, despite the recent highly publicized privacy initiatives undertaken by several companies, I don't believe industry is doing enough on its own to protect American consumers, while the government, as we all know, has this really bad habit of overreaching when it comes to new regulations. And the prospect of that hearing again looms very large in this debate, which brings us to today's hearing.

At first blush, how can anyone oppose the administration's seven privacy principles, such as individual control, transparency and accountability? It is simply Mom and apple pie.

I want to applaud Chairman Leibowitz and Secretary Strickling for your tireless efforts and commitment to this issue; you have done a great job. The privacy framework that you have put forward reflects a lot of time, effort, and careful thought when it comes to the question facing us today: How do we better protect privacy in the future?

I really look forward to discussing this important issue with you.

But given Washington's addiction to regulation, I am very concerned that the White House's privacy bill of rights could morph one day into another big government's rules of the road, complete with red-light cameras, speed traps and traffic cops trying to meet ever-increasing quotas. Talk about stopping the Internet dead in its tracks.

This all reminds me of Joseph Heller's great satirical World War II novel "Catch-22," which is based on the premise of a bureaucratic, no-win situation or a double bind. Today we could be facing a similar paradox if we are not very, very careful about how we proceed.

In Heller's book, the main character, an Air Force B–25 bombardier flying over the Mediterranean Sea, blurts out at one point, "The enemy is anybody who is going to get you killed, no matter what side he is on." Sound familiar? I bet it does to consumers. Today we might be facing a similar sort of circular logic, our very own Catch-22.

Some people say we must regulate the Internet to protect privacy. Others say if we go too far to protect privacy, we could her the Internet. Or is there a middle ground, a sweet spot between too much regulation and no regulation at all? I believe finding that sweet spot is a challenge we are facing today.

Clearly, we are making progress on the privacy front. Yet on the other hand, our rapid technological advance is simply creating a new, different and more complex set of problems. And how capable are regulators of keeping abreast of these changes without always winding up a day late and a dollar short?

Too much is at stake for to us get this wrong. That is why I have advocated since the beginning of these hearings that we need to move forward with an abundance of caution. And to me, the reason is crystal clear: Even though it serves billions of users worldwide, and e-commerce last year in the U.S topped $200 billion for the first time, the Internet pretty much remains a work in progress.

Still, in just 25 years, the Internet has already spurred transformative innovation. It has incalculable value. It has become part of our daily lives, and it has unlimited potential to effect positive social and political change, as the world dramatically witnessed during the Arab Spring.

So, before we do any possible harm to the Internet, we need to understand what harm is actually being done to consumers, and where is the public outcry for legislation? Today I am simply not hearing it. I haven't gotten a single letter from anyone back home urging me to pass a privacy bill. They want data protection, but no one is beating down my door about the broader privacy issues. That may change, and it probably will if industry doesn't come up with better safeguards for consumers in the future. But right now, we should resist the urge to rush to judgment because we feel a compelling need to do something, even if we are not exactly sure what that should be.

And now I recognize the ranking member of our subcommittee, Mr. Butterfield of North Carolina, for his opening.

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

Statement of the Honorable Mary Bono Mack
Chairman, Subcommittee on Commerce, Manufacturing, and Trade
"Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?"
March 29, 2012

Today, as we continue our year-long series of hearings into online privacy, we are rapidly reaching the point where the rubber hits the road.

When it comes to the Internet, how do we – as Congress, as the Administration, and as Americans – balance the need to remain innovative with the need to protect privacy? And how hard of a shove would it take to tip that critically important balance in a way that hurts the U.S. economy, American consumers or both?

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.

After six privacy hearings, we have covered a lot of ground, and we've learned a lot about consumer concerns. But today, I'm still not certain legislation is necessary...still skeptical of the motives of both industry and government…and still leery that advancements like Do Not Track and eraser button technology will work as intended.

Frankly – despite the recent, highly-publicized privacy initiatives undertaken by several companies – I don't believe industry is doing enough on its own to protect American consumers, while the government, as we all know, has this really bad habit of overreaching whenever it comes to new regulations. And the prospect of that happening again looms large in this debate.

Which brings us to today's hearing. At first blush, how can anyone oppose the Administration's seven privacy principles, such as individual control…transparency…and accountability? It's so "mom and apple pie."

I want to applaud Chairman Leibowitz and Secretary Strickling for your tireless efforts and commitment to this issue. You've done a great job. The privacy framework that you have put forward reflects a lot of time, effort and careful thought when it comes to: "how do we better protect consumer privacy in the future?" I really look forward to discussing this important issue with you today.

But.....

Given Washington's addiction to regulation, I'm very concerned that the White House's Privacy Bill of Rights could morph one day into another Big Government Rules of the Road – complete with red light cameras…speed traps and traffic cops trying to meet ever-increasing quotas. Talk about stopping the Internet dead in its tracks.

This all reminds me of Joseph Heller's great, satirical World War II novel Catch 22, which is based on the premise of a bureaucratic, no-win situation or a "double bind". Today, we could be facing a similar paradox if we're not very, very careful about how we proceed.

In Heller's book, the main character – an Air Force B-25 bombardier flying over the Mediterranean Sea – blurts out at one point: "The enemy is anybody who's going to get you killed – no matter what side he's on." Sound familiar? I bet it does to consumers.

Today, we may be facing a similar sort of circular logic…our very own Catch 22. Some people say we must regulate the Internet to protect privacy. Others say if we go too far to protect privacy, we could hurt the Internet.

Or is there a middle ground – a sweet spot – between too much regulation and no regulation at all? I believe finding that sweet spot is the challenge we are facing today. Clearly, we're making progress on the privacy front. Yet – on the other hand – are rapid technological advancements simply creating a new, different and more complex set of problems? And how capable are regulators of keeping abreast of these changes, without always winding up "a day late and a dollar short?"

Too much is at stake for us to get this wrong. That's why I have advocated since the beginning of these hearings that we need to move forward with an abundance of caution.

To me, the reason is crystal clear.

Even though it serves billions of users worldwide – and e-commerce last year in the United States topped $200 billion for the first time – the Internet pretty much remains a work in progress.

Still, in just 25 years, the Internet already has spurred transformative innovations.

It has incalculable value. It has become part of our daily lives. And it has unlimited potential to affect positive social and political change, as the world dramatically witnessed during The Arab Spring.

So before we do any possible harm to the Internet, we need to understand what harm is actually being done to consumers. Where is the public outcry for legislation? Today, I'm simply not hearing it. I haven't gotten a single letter from anyone back home, urging me to pass a privacy bill.

That may change – and it probably will – if industry doesn't come up with better safeguards for consumers in the future. But right now, we should resist the urge to "rush to judgment," because we feel a compelling need to do something – even if we're not exactly sure…what that should be.

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

Mr. BUTTERFIELD. I thank the chairman.

Also thank the witnesses for coming forward today with your testimonies. We are going to try to get right through this and get right to your testimony and hopefully have some good questions and answers will follow.

Let me begin by thanking the Department of Commerce and FTC for their initiatives to address the serious issue of consumer privacy. These two documents sketch out, with varying degrees of specificity, steps that should be taken to protect consumers' privacy. The White House privacy report suggests starting with the implementation of high level principles contained in its consumer privacy bill of rights. The report recommends that industry implement the consumer privacy bill of rights through voluntarily adopted business codes of conduct.

I commend those in industry that are supporting this effort. Consumers and industry must engage each other for this process to work. The White House privacy report also recognizes that there must be a backstop, and it must be a baseline, that consumers need bottom-line privacy protections spelled out in Federal law. I, therefore, support the administration and strongly believe that in order to provide companies and consumers with legal certainty, we need to enact a comprehensive, flexible and balanced Federal consumer privacy law.

The FTC report that was released earlier this week starts from a more concrete and substantive place, suggesting best practices for industry that it believes will result in better privacy protection for consumers. I want to be clear, these recommendations are not law; they are not even regulations. They are not legally binding on anyone. And they aren't legally enforceable by anyone. Nonetheless, these were carefully considered recommendations. And to the extent they can, I hope companies will make the FTC's recommendations part of their everyday business practices.

It makes good business sense for companies to keep privacy at the forefront as they develop new products and services. It is also good business practice to incorporate data security from the beginning and throughout the development process. And consumers have more confidence in those businesses that are transparent about their data collection practices.

The FTC, like the White House, is also now calling on us here in Congress to pass consumer privacy legislation.

Madam Chair, I agree that we must take of privacy legislation now. The White House has called on Congress to act. The FTC has called on Congress to act, and many members of the subcommittee believe that we must act now.

I feel strongly 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. To that end, I believe any privacy legislation should contain at least the minimum requirements, ensure Americans have context-appropriate access to their information; number two, transparency with regard to who is collecting their data; three, affirmative consent prior to personal

data being shared with a third party; and number four, that personal data be protected through reasonable security safeguards.

I would like to thank the witnesses for being here today. Madam Chair, I would like to reiterate that I stand ready to work with you on a commonsense privacy piece of legislation that will ensure the greatest protection for consumers.

Thank you, and I yield back.

Mrs. BONO MACK. Thank you, Mr. Butterfield.

And the chair now recognizes Mr. Upton for 5 minutes for his opening statement.

Mr. UPTON. Well, good morning, Madam Chair.

Mrs. BONO MACK. Good morning.

OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. UPTON. I would like to welcome back Chairman Leibowitz and Assistant Secretary Strickling as well as the distinguished witnesses that we will hear from on the second panel.

Privacy is not a new topic for Congress. Through the decades, we have passed statutes protecting electronic communications, financial information, health information, credit information, movie and book rental information and information gathered about children. But the lightening fast development of Internet and mobile technology presents issues that were not anticipated even 5 years ago.

Smartphones, tablets, connected entertaining devices and all of the aps are today's modern marble, but who knows what will replace them in about another 5 years.

I am highly skeptical of Congress' or government regulators' ability to keep up with the innovative and vibrant pace of the Internet without breaking it. Consumers and the economy as a whole will not be well served by government attempts to wrap the Web in red tape. And we cannot ignore that Internet companies have a strong incentive to protect their users; it is called consumer choice. Today's online consumers are savvy customers who will not be loyal to a company that puts their personal information at risk. The next big thing is just around the virtual corner.

The development and success of the Internet economy in the U.S. Is due in large part to the freedom that our entrepreneurs have to dream and build. The world's leading Internet companies and innovators have created a vibrant sector of the economy that continues to expand, adding lots of jobs for multinationals and small businesses alike.

According to a recent study by Boston Consulting Group, the Internet sector accounted for a 4.7 percent of our GDP in 2010, $684 billion, and it is growing faster in that the rest of the economy that is for sure.

Apple released a study earlier this month estimating that it alone created or supported 514,000 jobs in the U.S. from engineers, to manufacturing, to sales clerks.

At its heart, the Internet is a tool that promotes information exchanges, whether for conducting consumers, entertainment, education or social interaction. And many of the benefits and attractions of the Internet are a product of its capacity to provide cus-

tomized services to individuals, but that often requires exchanging, identifying personal information.

How that information is treated, who has access to it, and the degree of consumer control are important questions that need to be answered. Whether the President's plan that we are discussing today can be successful in developing consensus codes of conduct that protect privacy is an open question and perhaps the most important aspect on which the administration's framework success or failure hinges.

The administration recognizes that industry developed standards have proved successful in addressing technical standards for the Internet as well as in other areas of commerce. I am most interested to hear how those examples will serve as a template for the multi-stakeholder process that the NTIA will convene to move this process forward.

And I would yield to either Mr. Olson or Mr. Kinzinger if they have any additional comments.

[The prepared statement of Mr. Upton follows:]

Statement of the Honorable Fred Upton
Chairman, Committee on Energy and Commerce
Hearing before the Subcommittee on Commerce, Manufacturing and Trade
"Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?"
March 29, 2012

Thank you, Chairman Bono Mack. I welcome back Chairman Leibowitz and Assistant Secretary Strickling as well as the distinguished witnesses we will hear from on the second panel.

Privacy is not a new topic for Congress. Through the decades we have passed statutes protecting electronic communications, financial information, health information, credit information, movie and book rental information, and information gathered about children. But the lightning-fast development of Internet and mobile technology presents issues that were not anticipated even five years ago. Smartphones, tablets, connected entertainment devices and all of the accompanying applications (or "apps") are today's modern marvel, but who knows what will replace them in another five years.

I am highly skeptical of Congress' or government regulator's ability to keep up with the innovative and vibrant pace of the Internet without breaking it. Consumers and the economy as a whole will not be well served by government attempts to wrap the web in red tape. And we cannot ignore that Internet companies have a strong incentive to protect their users – it's called consumer choice. Today's online consumers are savvy customers who will not be loyal to a company that puts their personal information at risk. The next big thing is just around the virtual corner.

The development and success of the Internet economy in the United States is due in large part to the freedom our entrepreneurs have to dream it and build it. The world's leading Internet companies and innovators have created a vibrant sector of the economy that continues to expand, adding jobs for multinationals and small business alike. According to a recent study by the Boston Consulting Group, the Internet sector accounted for 4.7 percent of our GDP in 2010—$684 billion—and is growing faster than the rest of the economy. Apple released a study earlier this month estimating that it alone created or supported 514,000 jobs in the U.S., from engineers to manufacturing to sales clerks.

At its heart, the Internet is a tool that promotes information exchanges, whether for conducting commerce, entertainment, or social interaction. Many of the benefits and attractions of the Internet are a product of its capacity to provide customized services to individuals, but that often requires exchanging identifying or personal information. How that information is treated, who has access to it, and the degree of consumer control are important questions.

Whether the President's plan we are discussing today can be successful in developing consensus codes of conduct that protect privacy is an open question, and perhaps the most important aspect on which the Administration framework's success or failure hinges. The Administration recognizes that industry-developed standards have proved successful in

addressing technical standards for the Internet as well as in other areas of commerce. I am interested to hear how those examples will serve as a template for the multi-stakeholder process the NTIA will convene to move this process forward.

I have additional questions and comments and look forward to discussing them with our witnesses. I yield back the balance of my time.

Mrs. BONO MACK. If the gentleman would yield to Ms. Blackburn.

Mr. UPTON. I am sorry. I yield back the balance of my time.

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

Mrs. BLACKBURN. Thank you, Mr. Chairman.

And I want to welcome our witnesses.

Just a couple of quick thoughts. The administration has basically put forward two different privacy frameworks, but each of these reports would encompass a massive expansion of government. And in my opinion, it would put some limits on our individual liberties.

We have to remember we live in a data-driven information age. And what happens when you follow the European privacy model and take information out of the information economy? Those are the questions that we are going to be asking because I think it is a pretty simple answer, and you can look at Europe and see, revenues fall, innovation stalls, and you lose out to innovators who chose to work elsewhere.

So we are concerned about technology mandates, concerned about a Do Not Track system and if that would lead to disincentives in the system. We are also seeing some larger companies embrace privacy regulation as a weapon to stifle competition and grow monopoly power; that is of concern. So let's better define the contours of the debate that is in front of us.

As I continue to say, please, identify the harm and then let's talk about what needs to be done to address that specific harm.

I thank the chairman for the hearing today.

I thank the witnesses.

And I yield back.

Mrs. BONO MACK. Thank you, Ms. Blackburn.

And I would like to thank you for chairing the hearing last week while I was away. I heard you did a fantastic job. I hope you found this chair comfortable but not too comfortable.

At this point, we will turn our attention to the panel. We have two panels 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.

On our first panel, we have the Honorable Lawrence Strickling, Assistant Secretary for Communication and Information at the U.S. Department of Commerce. And we also have the Honorable John Leibowitz, Chairman of the Federal Trade Commission.

Good morning, gentlemen.

Thank you again for coming. You will each be recognized for the 5 minutes and the timers—I think you know the drill. The timers are in front of you. When the light turns yellow, you will have 1 minute left to begin wrapping up your remarks.

And please, just make sure the microphone is close to your mouth as you begin, and there is an on button. It is important that the audience at home can hear you as well.

So, with that, we are happy to recognize you, Mr. Strickling, for 5 minutes.

STATEMENTS OF LAWRENCE E. STRICKLING, ASSISTANT SECRETARY FOR COMMUNICATION AND INFORMATION, DEPARTMENT OF COMMERCE; AND JON LEIBOWITZ, CHAIRMAN, FEDERAL TRADE COMMISSION

STATEMENT OF LAWRENCE E. STRICKLING

Mr. STRICKLING. Thank you, Chairman Bono Mack, and Ranking Member Butterfield and Vice Chair Blackburn.

I am pleased to be here to testify on the administration's consumer privacy framework, and I am especially pleased to be here with my colleague Chairman Leibowitz, who has provided such strong and decisive leadership at the Federal Trade Commission to protect consumers and promote economic growth.

The question for today's hearing is whether the administration's framework for protecting privacy and promoting innovation tips the scale that balances privacy and innovation. My response is an emphatic no. The administration's proposals strikes the right balance to preserve the flexibility businesses need to innovate while addressing the broad array of privacy harms that consumers face in our network world.

Certainly, we all know that the misuse of personal data can cause financial harm. Personal data lost through security breaches can lead to identity theft and financial fraud. And the financial costs of these incidents are quite apparent. But it is equally apparent that consumers suffer harms that are more difficult to quantify. They can suffer severe embarrassment from having their names or online identities associated with certain Web sites. They have been surprised and shocked to find that information about them spreads rapidly from one place to another on the Internet. It is no wonder that consumers express concern about how companies handle personal data, and they tend to avoid those that fail to meet their expectations.

This state of affairs does not serve consumers well, but just as importantly, it does not serve our businesses either. If consumers no longer trusted their information will be protected on the Internet, we risk undermining the growth and innovation that has characterized the Internet economy. And accordingly, in developing the administration's policy, we felt that adequately protecting consumer privacy needed to be done in a way that also protected innovation so that the result would be a win-win for consumers and for businesses.

The blueprint includes four key measures. First is the Consumer Privacy Bill of Rights, these rights general statements of basic and globally recognized privacy principles. We carefully avoided making these principles read like regulations intended to cover every possible contingency that might arise because we knew that doing so would threaten the flexibility businesses need to have to innovate on the Internet.

The Consumer Privacy Bill of Rights recognizes that businesses need to collect personal data simply to do business. And it also recognizes that much of this data collection occurs within the context of a direct relationship between consumers and companies. On the whole, the Consumer Privacy Bill of Rights provides a baseline to protect consumers from the wide range of privacy harms that arise

in our networked economy. The administration believes this basic set of principles should be enacted into law, and we are eager to work with the committee to that end.

From there, we had a choice; we could have as so much legislation does propose that a regulatory agency engage in lengthy rulemaking proceedings to provide more detail and definition for these basic principles. We did not do so.

Our second key aspect of our blueprint is that we looked to the private sector, businesses and consumer advocates working together to take the lead on implementation by developing legally enforceable codes of conduct that apply the Privacy Bill of Rights to specific business settings.

My agency NTIA will convene the various stakeholders and facilitate their discussions, but we will not substitute our judgement for the consensus reached by stakeholders. And since I am not a regulator, we will not impose these codes on businesses but will leave it to companies to decide on their own whether to adopt a particular code, developed through this multi-stakeholder process.

Once a company adopts a code, we believe it will be enforceable by the Federal Trade Commission under its authority to protect consumers from unfair and deceptive trade practices, just as it does today with privacy policies adopted by companies. And this strong enforcement of company commitments to protect privacy is the third key piece of the administration's policy.

Fourth and finally, the United States has a unique opportunity to be a leading voice in global discussions of consumer privacy. Our efforts in this regard will provide American businesses with a stronger position by which to expand globally with our trading partners by providing better interoperability between privacy regimes around the world.

We are actively engaging our international partners to promote these principles and to make it easier for American businesses to succeed in the global marketplace. I want to thank you again for your time and for holding today's hearing, and I look forward to answering your questions.

[The prepared statement of Mr. Strickling follows:]

Testimony of Lawrence E. Strickling

Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce

Hearing on "Privacy and Innovation: Does the President's Proposal Tip the Scale?"
Subcommittee on Commerce, Manufacturing and Trade
Committee on Energy and Commerce
United States House of Representatives

March 29, 2012

I. Introduction

Chairman Bono Mack, Ranking Member Butterfield, and distinguished Committee Members, thank you for the opportunity to testify about the Administration's views on consumer data privacy in the digital economy. This hearing comes at a pivotal time in the development of privacy policies in the United States and throughout much of the world. The Administration appreciates your interest in these issues, and I welcome this opportunity to discuss how we can protect consumers' privacy and promote innovation in our networked world.

Last month, the Administration released its blueprint for consumer data privacy policy in the 21st Century ("Privacy Blueprint").[1] The Privacy Blueprint is the result of more than two years of work by the Department of Commerce ("Department") Internet Policy Task Force, as well as extensive discussions with stakeholders in the private sector and the government. The Privacy Blueprint sets forth a four-part approach to protecting consumer privacy. The first pillar is the Consumer Privacy Bill of Rights, which tells consumers what they should expect from companies that handle data about them and provides companies with guidelines to help them meet those expectations. Second, the Privacy Blueprint outlines a stakeholder-driven approach to apply the Consumer Privacy Bill of Rights in developing enforceable, context-specific codes of conduct that companies may choose to adopt. Third, the Privacy Blueprint emphasizes that continued vigorous enforcement by the Federal Trade Commission (FTC) and State Attorneys General is crucial to protecting consumers while maintaining the flexibility that companies need to innovate. Fourth, the Privacy Blueprint sets forth global interoperability, based on recognition

[1] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in a Global Digital Economy*, Feb. 2012, *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("Privacy Blueprint"). The Privacy Blueprint builds on the Department of Commerce Internet Policy Task Force's report, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, Dec. 2010, *available at* http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

of common privacy values, enforceable codes of conduct, and enforcement cooperation, as a guiding principle for protecting consumer privacy and promoting innovation in a global digital economy that will continue to be governed by different privacy laws and regulations.

My testimony today has three purposes. First, I will explain how the Consumer Privacy Bill of Rights establishes a baseline of privacy protections that Congress should enact in legislation. Second, I will explain why the multistakeholder approach outlined in the Privacy Blueprint provides the right approach to apply the Consumer Privacy Bill of Rights in specific markets or business settings. Third and finally, I will discuss the steps that the National Telecommunications and Information Administration (NTIA) is taking now to implement the Privacy Blueprint.

II. The Consumer Privacy Bill of Rights Addresses Real Harms and Will Preserve Consumer Trust

A. The Importance of Recognizing a Broad Array of Consumer Privacy Interests

Americans cherish their privacy. From the Fourth Amendment's recognition of a right to be free from unreasonable invasions of our homes and papers, to statutory guarantees of privacy in the mails enacted in the early years of the Republic, to the Supreme Court's recognition of a right to anonymous political speech, the United States has recognized that appropriate privacy protections promote commerce, encourage political discussion, and allow individuals to form and strengthen social bonds.

Privacy is also an important element of the trust that sustains digital commerce. As the President stated in introducing the Consumer Privacy Bill of Rights, citizens who have "confidence that companies will handle information about them fairly and responsibly, . . . have turned to the Internet to express their creativity, join political movements, form and maintain

friendships, and engage in commerce."[2] These results are evident in the rapid growth of online commerce,[3] the adoption of smartphones,[4] the explosion of mobile applications that run on them,[5] and the integral role that Internet-based business-to-business transactions play in the U.S. economy.[6] The United States leads the world in developing and providing many of these services. Maintaining this position depends, in part, on maintaining consumer trust.

Unfortunately, companies do not always meet this expectation of fair and responsible handling of personal data. As a result, consumers suffer individual harms. These harms range from minor inconveniences, to damaged reputations and severe embarrassment, to identity theft and financial harm. Breaches involving certain types of personal data may lead to identity theft and other crimes that inflict financial harm on consumers and companies.[7] Severe embarrassment can come from something as simple as associating individuals' names, which could be gleaned from leaked email addresses or other account identifiers, with the content of a website.[8] And inconveniences arising from managing personal data in the absence of consistent baseline principles can frustrate or even mislead consumers. For example, consumers may find

---

[2] Privacy Blueprint at i.

[3] Online retail sales provide one measure of this growth. In 2000, online retail sales in the United States totaled $29 billion. U.S. Census Bureau, *E-Stats*, at 3, Mar. 18, 2002, *available at* http://www.census.gov/econ/estats/archives.html. According to preliminary estimates, in 2011, online retails sales could total around $200 billion. *See* U.S. Census Bureau, Quarterly Retail E-Commerce Sales – 4th Quarter 2011, at 2, Feb. 16, 2012, *available at* http://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

[4] Smartphone ownership among U.S. adults increased by 11 percent between May 2011 and February 2012. Pew Internet & American Life Project, 46% of American Adults Are Smartphone Owners, at 4, Mar. 1, 2012, *available at* http://www.pewinternet.org/~/media//Files/Reports/2012/Smartphone%20ownership%202012.pdf.

[5] *See* Gartner, Inc., Gartner Says Worldwide Mobile Application Store Revenue Forecast to Surpass $15 Billion in 2011, Jan. 26, 2011, *available at* http://www.gartner.com/it/page.jsp?id=1529214.

[6] *See, e.g.*, U.S. Census Bureau, *E-Stats*, at 2, May 26, 2011, *available at* http://www.census.gov/econ/estats/2009/2009reportfinal.pdf (reporting that business-to-business digital commerce transactions totaled $3.1 trillion in 2009, the latest year for which final statistics are available).

[7] *See* Sasha Romanosky, Richard Sharp, and Alessandro Acquisti, *Data Breaches and Identity Theft: When Is Mandatory Disclosure Optimal?* at 1, Ninth Workshop on the Economics of Information Security (WEIS 2010), *available at* http://weis2010.econinfosec.org/papers/session1/weis2010_romanosky.pdf (asserting and provideing citations showing that information obtained through data breaches "can then be used to commit crimes" such as filing fraudulent unemployment claims and tax returns and committing various types of financial fraud).

[8] *See* Timothy Stenowick, YouPorn: Up To 1 Million Adult Chat Users' Email Addresses and Passwords Exposed, The Huffington Post, Feb. 22, 2012, *available at* http://www.huffingtonpost.com/2012/02/22/youporn-hacked-email-addresses-passwords_n_1294502.html.

that they need to go through cumbersome or repetitive procedures to opt out of certain kinds of personal data collection or use.[9] This kind of process may be manageable in small doses, but it does not provide a workable template for consumers to exercise control over personal data in the modern Internet environment, in which hundreds of different entities may collect information about them.

In areas of commercial activity that are not covered by existing Federal data privacy laws, consumers have few guideposts to inform them of how information about them is collected and used. Consumers have been surprised to learn—often after a security breach—of the variety of companies that hold personal data about them.[10] They express concern about having their Internet use tracked[11] and face a steady stream of reports indicating that they are caught in an arms race for personal data.[12] Consumers also report avoiding companies that do not sufficiently protect their privacy.[13] These concerns are spread across age groups,[14] and they are spreading to new domains, such as mobile computing.[15] In addition to providing a basis for enforcement under Section 5 of the FTC Act, privacy policies are the principal mechanism to inform

---

[9] *See, e.g.*, In re *Chitika, Inc.*, FTC Docket No. C-4324, June 17, 2011, *available at* http://www.ftc.gov/os/caselist/1023087/110617chitikacmpt.pdf (alleging that an online advertising network's opt-out was effective for only 10 days).

[10] *See, e.g.*, United States v. ChoicePoint, Inc., No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006), http://www.ftc.gov/os/caselist/choicepoint/stipfinaljudgement.pdf; *see also* FTC Preliminary Staff Report, Dec. 2010, at 9-11 (reviewing FTC data security cases).

[11] *See* Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley and Michael Hennessy, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities That Enable It*, at 3-4 (Sept. 2009), http://ssrn.com/abstract=1478214.

[12] *See generally* Wall St. Journal, *What They Know*, *available at* http://online.wsj.com/public/page/what-they-know-digital-privacy.html (last visited Mar. 21, 2012).

[13] *See* Harris Interactive/TRUSTe Privacy Index: Q1 2012 Consumer Confidence Edition, Feb. 13, 2012, *available at* http://www.truste.com/about-TRUSTe/press-room/news_truste_launches_new_trend_privacy_index.

[14] *See* Harris Interactive/TRUSTe Privacy Index: Q1 2012 Consumer Confidence Edition, Feb. 13, 2012, *available at* http://www.truste.com/about-TRUSTe/press-room/news_truste_launches_new_trend_privacy_index (reporting survey results showing that U.S. adults who avoid doing business with companies that do not protect their privacy ranges from 82%, among 18-34 year olds, to 93%, among adults 55 years old and older).

[15] *See TRUSTe, More Consumers Say Privacy—Over Security—is Biggest Concern When Using Mobile Applications on Smartphones,* Apr. 27, 2011 (reporting results of survey of top 340 free mobile apps conducted jointly with Harris Interactive), *available at* http://www.truste.com/blog/2011/04/27/surveyresults-are-in-consumers-say-privacy-is-a-biggerconcern-than-security-on-smartphones/.

consumers of a company's privacy practices. Unfortunately, many privacy policies do not address consumers in an intelligible manner and have even further to go in the mobile realm. Clearer policies will help consumers understand what they can expect from companies that handle data about them and allow them to more meaningfully assess their choices.

Consumers and American businesses share a strong interest in better defining and protecting privacy interests in the digital age to maintain the trust that is necessary to keep the Internet growing and supporting innovation. Consumers should not be subject to constant uncertainty about what information is collected about them and how it may be used. They need and deserve a baseline set of protections. Conversely, companies should have clear obligations to meet, and companies that handle personal data responsibly should not be disadvantaged by those who behave carelessly.

B. Addressing Consumer Privacy Harms Through the Consumer Privacy Bill of Rights

The Consumer Privacy Bill of Rights provides these guidelines. It addresses the highly diverse privacy interests that consumers have (and, consequently, the diverse harms they may experience) and the fact that these interests change quickly, in two main ways. First, it articulates a set of rights which provides a baseline of principles to identify and analyze consumer privacy interests. Second, it outlines a multistakeholder approach to develop specific practices that implement these guidelines on a timescale that matches changes in technology, markets, and consumer expectations.

The Consumer Privacy Bill of Rights provides the right foundation for consumer privacy in the digital age. Each element of the Consumer Privacy Bill of Rights addresses consumers directly and affirmatively, to give consumers a stronger sense of what they should expect from

companies. In addition, each right explains how companies that handle personal data can implement the right through their data practices.

The Consumer Privacy Bill of Rights includes:[16]

- **Individual Control**: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- **Transparency**: Consumers have a right to easily understandable and accessible information about privacy and security practices.
- **Respect for Context**: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- **Security**: Consumers have a right to secure and responsible handling of personal data.
- **Access and Accuracy**: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
- **Focused Collection**: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- **Accountability**: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

C. The Consumer Privacy Bill of Rights Adapts Globally Recognized Fair Information Practice Principles to the Digital Economy

The Consumer Privacy Bill of Rights is based on globally recognized Fair Information Practice Principles (FIPPs), which originated in the Department of Health, Education and

[16] For brevity, we provide only the consumer-directed portion of each right. For the full statement of the Consumer Privacy Bill of Rights, see Privacy Blueprint, App. A, at 47-48.

Welfare's 1973 report, *Records, Computers, and the Rights of Citizens*.[17] Congress incorporated these principles into the Privacy Act of 1974.[18] Since then, a consistent set of FIPPs has become the foundation for global privacy discussions through, for example, the Organization for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("OECD Privacy Guidelines")[19] and the Asia-Pacific Economic Cooperation's Privacy Framework.[20] The Administration sought to remain consistent with these existing FIPPs as it developed the Consumer Privacy Bill of Rights.[21]

At the same time, many individuals and organizations that commented on the Department's Privacy and Innovation Green Paper noted that the digital economy, which is data-intensive, dynamic, and increasingly driven by consumers' active participation, requires some adaptation of existing statements of the FIPPs.[22]

The most significant adaptations to traditional FIPPs are found in the Individual Control, Respect for Context, Focused Collection, and Accountability principles.

1. Individual Control

---

[17] Department of Health, Educ., and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of* Citizens, July 1973, *available at* http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm (outlining a Code of Fair Information Practices that would create "safeguard requirements" for certain "automated personal data systems" maintained by the Federal Government).

[18] *See* Privacy Act of 1974, Pub. L. No. 93-579 (codified at 5 U.S.C. § 552a).

[19] The OECD Privacy Guidelines are available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[20] The APEC Privacy Framework is available at http://publications.apec.org/publication-detail.php?pub_id=390.

[21] *See* Privacy Blueprint, Appendix B, at 49-52 (mapping the Consumer Privacy Bill of Rights to the OECD Privacy Guidelines, the APEC Privacy Framework, and a generalized version of the Department of Homeland Security's Privacy Policy).

[22] *See, e.g.*, AT&T Comment on the Privacy and Innovation Green Paper, at 7 (warning against adopting an "unduly prescriptive iteration" of FIPPs); CCIA Comment on the Privacy and Innovation Green Paper, at 14-15 (raising concerns about traditional principles of purpose specification and use limitation and advocating "a middle way that recognizes the value in these principles but still gives a data collector some latitude to develop novel and beneficial uses for the data"); GE Comment on the Privacy and Innovation Green Paper, at 2 (asserting that the purpose specification and use limitation principles are "a logical extension of transparency").

The principles of Individual Control encompasses two signature traits of the networked world.[23] First, networked technologies offer an increasing number of ways to allow consumers to assert control over what personal data is collected. Companies should take advantage of these technologies by offering to consumers, at the time of collection, usable tools and clear explanations of their choices about data sharing, collection, use, and disclosure. Second, the Individual Control principle calls on consumers to understand their responsibilities for controlling personal data collection, particularly in situations in which consumers actively share data about themselves, such as online social networks. In these cases, control over the initial act of sharing is critical. Consumers can take significant steps to reduce harms associated with the misuse of their data by gaining a better understanding of what personal data they are disclosing and using the increasing number of tools available to control this data.

2. Respect for Context

The second noteworthy way in which the Consumer Privacy Bill of Rights adapts traditional FIPPs is through the Respect for Context principle.[24] The basic premise of this principle is simple: The relationship between consumers and a company—that is, the context of personal data use[25]—should help determine whether a specific use is appropriate and what kinds of consumer choices may be necessary. Factors such as what consumers are likely to understand about a company's data practices based on the products and services it offers, how a company explains the roles of personal data in delivering these products and services, research on consumers' attitudes and understandings, and feedback from consumers should also enter these

[23] *See* Privacy Blueprint at 11-14.
[24] *See* Privacy Blueprint at 15-19.
[25] For simplicity, this discussion refers to personal data uses. The discussion applies equally to personal data collection and disclosure.

assessments. Personal data should flow relatively freely to support the purposes that consumers seek to achieve in a given context.

For example, suppose an online social network holds out its service as a way for individuals to connect with people they know and to form ties with others who share common interests. In connection with providing this service, asks new users to provide biographical information about themselves as well as information about their acquaintances. As consumers use the service, they may provide additional information through written updates, photos, videos, and other content they choose to post. The online social network's use of this information to suggest connections that its users might wish to form is integral to the service and obvious from the social networking context. Seeking consumers' affirmative consent to use personal data for the purpose of facilitating connections on the service is not necessary. By contrast, if the online social network uses this information to achieve purposes that fall outside the social networking context, such as employment screening or credit eligibility, the Respect for Context would call for prominent, explicit notice and meaningful opportunities for consumer choice. The Respect for Context principle will help protect consumers against these real harms that can arise when information is lifted out of one context and used unexpectedly in another.

The sophistication of a company's customers is also an important element of context. In particular, the unique characteristics of children and teenagers may warrant different privacy protections than are suitable for adults. Children, in particular, are particularly susceptible to privacy harms. The Administration looks forward to exploring with stakeholders whether more stringent applications of the Consumer Privacy Bill of Rights—such as an agreement not to create individual profiles about children, even if online services obtain the necessary consent to collect personal data—are appropriate to protect children's privacy.

3. Focused Collection

Third, the Focused Collection principle adapts the "data minimization" and "collection limitation" principles found in traditional FIPPs. Some existing versions of these principles provide a strict standard that makes personal data collection permissible only when it is kept to the minimum necessary to achieve specific purposes. Such a strict standard is unworkable for the networked technologies that support the digital economy. Familiar and increasingly essential Internet services, such as search engines, collect a wide range of personal data and use it in a wide variety of ways. Such services may be consistent with the Focused Collection principle, provided they reflect careful decisions about what kinds of personal data are necessary to provide the services, how long the data needs to be retained, and what measures may be available to make retained data less likely to be associated with specific consumers. Focused collection will help protect consumers from harm associated with misuse of data that never needed to be collected or retained to begin with. The Focused Collection principle, however, does not relieve companies of any independent legal obligations, including law enforcement orders, that require them to retain personal data.

4. Accountability

Finally, the Accountability principle emphasizes that the measures companies take to educate employees about using personal data, prevent lapses in their privacy commitments and detect and remedy any lapses that occur are crucial to protecting consumer privacy. Accountability also assures that when consumers feel harmed by the way their data is handled, their complaints can go to the entity responsible for handling that data. Accountability mechanisms also may provide a route toward greater global interoperability. The Administration is actively exploring how accountability mechanisms, which could be developed through a

privacy multistakeholder process, could ease privacy compliance burdens for companies doing business globally.[26]

D. The Administration Supports Enacting the Consumer Privacy Bill of Rights into Law

Congress should act to protect consumers from violations of the rights defined in the Administration's Consumer Privacy Bill of Rights. These rights provide clear protection for consumers and define rules of the road for the rapidly growing marketplace for personal data. As framed in the Privacy Blueprint, the Consumer Privacy Bill of Rights would provide a set of standards that many responsible companies are already capable of meeting. Legislation would put these companies on a level playing field with those who are less careful with personal data, and it would provide stronger and more specific consumer protections.

Enacting the Consumer Privacy Bill of Rights in a manner that provides sufficiently clear legal obligations will require drafting beyond the text offered in Consumer Privacy Bill of Rights itself. Accordingly, the Administration is committed to working with Congress to develop legislation that captures the flexibility and comprehensiveness of the Consumer Privacy Bill of Rights.

The Privacy Blueprint provides other recommendations for legislation based on the Consumer Privacy Bill of Rights.[27] Specifically, the Administration recommends that legislation:

- Permit the Federal Trade Commission (FTC) and State Attorneys General to directly enforce the statutory Consumer Privacy Bill of Rights.

[26] *See* Privacy Blueprint at 31-33.
[27] *See* Privacy Blueprint at 35-39.

- Authorize the FTC to review codes of conduct based on the statutory Consumer Privacy Bill of Rights, and grant an enforcement safe harbor for companies under its jurisdiction that adhere to an approved code of conduct.
- Preempt State laws to the extent they are inconsistent with the Consumer Privacy Bill of Rights as enacted in statute.
- Preserve existing sector-specific Federal laws that effectively protect personal data, to minimize the duplication of legal requirements and provide consumers with a clear sense of what protections they have and who enforces them.
- Set a uniform national standard for requiring companies to notify consumers of unauthorized disclosures of certain kinds of personal data.
- Enable enforcement that builds on the FTC's expertise and current role as the Federal Government's leading consumer privacy enforcement authority.

Just as importantly, the Administration recommends that consumer data privacy legislation incorporate certain limitations. Specifically, such legislation should avoid:[28]

- Adding duplicative or overly burdensome regulatory requirements on companies that are already adhering to legislatively adopted privacy principles.
- Prescribing technology-specific means of complying with the law's obligations.
- Precluding new business models that are consistent with the Consumer Privacy Bill of Rights in general but may involve new uses of personal information not contemplated at the time the statute is written.
- Altering existing statutory or regulatory authorities pursuant to which the government may obtain information necessary to assist in conducting border searches, investigating

[28] Privacy Blueprint at 35-36.

criminal conduct or other violations of law, or protecting public safety and national security.

- Contravening the ability of law enforcement to investigate and prosecute criminal acts and ensure public safety.Altering existing statutory, regulatory, or policy authorities that apply to the government's information practices.

The Administration has begun to think carefully about how the Consumer Privacy Bill of Rights can best be put into law, and we look forward to working with this Committee, and with the entire Congress, to that end.

III. Promoting Adoption of the Consumer Privacy Bill of Rights Through Stakeholder-Developed, Enforceable Codes of Conduct

Implementing the general principles in the Consumer Privacy Bill of Rights—as envisioned in the legislation discussed above and as planned in the processes that NTIA will pursue in parallel with legislative discussions—across the wide range of innovative uses of personal data requires a flexible, fast-paced process to determine how to define concrete practices that embody the broader principles in a specific setting. This process must be capable of addressing consumer privacy issues that arise and change as quickly as networked technologies and the products and services that depend on them. In addition, it should focus on specific business settings to help stakeholders address concrete privacy issues and business requirements, leading to practices that protect privacy without discouraging innovation. In addition, The process must also allow the broad range of stakeholders affected by personal data collection, use, and disclosure to participate meaningfully in determining how the Consumer Privacy Bill of Rights ought to apply in specific contexts. Finally, the process should be capable of producing practices that apply globally.

The Administration supports the use of multistakeholder processes, rather than rulemakings under the Administrative Procedure Act, to achieve these goals. Specifically, the Privacy Blueprint directs NTIA to convene interested stakeholders to address consumer privacy issues in transparent, consensus-based processes that are open to all interested stakeholders. The expected outputs of these processes are context-specific codes of conduct that companies may choose to adopt, rather than government regulations. Once a company publicly commits to follow a code of conduct, however, the Administration expects that this commitment will be enforceable by the FTC and State Attorneys General. Thus, the privacy multistakeholder approach will strike a balance between certainty for companies, strong protections for consumers, and the flexibility that is necessary to promote continued innovation.

This vision draws from several successful examples of Internet policy development. Private-sector standards-setting organizations, for example, are at the forefront of setting Internet-related technical standards. Groups such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) use transparent multistakeholder processes to set Internet-related technical standards. These processes are successful, in part, because stakeholders share an interest in developing consensus-based solutions to the underlying challenges. Successful government-convened Internet policymaking efforts in the past also provide precedents for the multistakeholder approach proposed in the Privacy Blueprint. For example, the Executive Branch led the privacy discussions of the 1990s and early 2000s, which continue to be central to advancing consumer data privacy protections in the United States. More recently, the FTC has encouraged multistakeholder efforts to develop a "Do Not Track"

mechanism, which would afford greater consumer control over personal data in the context of online behavioral advertising.[29]

Stakeholders have ample incentives to participate in this process under existing law. For companies, it is a way to build consumer trust and gain certainty as to what consumers expect from companies' personal data practices. For consumer and privacy advocates, the privacy multistakeholder process provides an opportunity to influence these practices through direct engagement with companies.

Still, consumer data privacy legislation could provide a significant boost to this flexible approach. Under the Administration's recommended framework, companies would face a choice: Follow the general principles of the statutory Consumer Privacy Bill of Rights, or commit to following a code of conduct that spells out how those rights apply to their businesses. If this code of conduct sufficiently implements the Consumer Privacy Bill of Rights in the context in which a company (or group of companies) plans to use it, the FTC should forbear from enforcing the Consumer Privacy Bill of Rights against it, so long as the company lives up to its commitment. The latter course would provide greater certainty for companies and stronger incentives for all stakeholders to work toward consensus on codes of conduct, but it requires Congress to act.

The legislative approach that the Administration recommends could also expand international recognition of codes of conduct. Baseline consumer privacy legislation would clarify the legal standards that underlie codes of conduct as well as their enforceability. This approach to legislation could have a broader influence on global Internet policy debates. It is important to demonstrate to our international partners that a principles-based framework,

---

[29] *See* World Wide Web Consortium, Tracking Protection Working Group, *available at* http://www.w3.org/2011/tracking-protection/ (last visited Mar. 21, 2012).

combined with a stakeholder-driven process to create more specific guidelines, can effectively address consumer data privacy issues. More generally, demonstrating that the government can facilitate the development of effective policy solutions without imposing top-down regulations will send a strong message to other countries that are increasingly turning to this approach. Still, even without baseline legislation, enforceable codes of conduct play an important role in global interoperability. For example, the U.S.-EU and U.S.-Swiss Safe Harbor Agreements are a source of legally enforceable privacy commitments and will continue to play a key role in facilitating transatlantic trade.[30]

IV. NTIA's Plans to Implement the Administration's Privacy Blueprint

A. Developing Privacy Codes of Conduct Through Multistakeholder Processes

NTIA has already begun to initiate stakeholder-driven processes to develop codes of conduct based on the Consumer Privacy Bill of Rights. Our first step was to seek comment from stakeholders on two sets of questions: which substantive issue is suitable for an initial effort to develop an enforceable code of conduct, and what procedures should the process follow.[31] NTIA suggested a number of substantive issues that are relatively well-definable and have the potential to deliver significant benefits to consumers if they are addressed through a code of conduct. Our request asked stakeholders to comment on the pros and cons of these candidates and to offer others that meet the criteria of definability and potential consumer benefit. We also asked for input on procedures that will make the process manageable while also open to all interested stakeholders' participation, transparent, and consensus-based.

---

[30] *See* International Trade Administration, Safe Harbor, *available at* http://export.gov/safeharbor/ (last updated Mar. 22, 2012).

[31] *See* NTIA, Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct, 77 Fed. Reg. 13098, Mar. 5, 2012, *available at* http://www.ntia.doc.gov/federal-register-notice/2012/multistakeholder-process-develop-consumer-data-privacy-codes-conduct.

The comment period closes next Monday, April 2, following which we will move promptly to select a substantive issue and convene an initial public meeting to begin developing a code of conduct. Part of the business of this initial meeting will be for stakeholders to reach agreement on the procedures they will use to work together. While NTIA will likely provide some guidance and perspective, based on its participation in other multistakeholder processes as well as its review of comments on this process, we will avoid imposing our judgment on the group. In other words, NTIA's role will be to convene stakeholders and facilitate discussions that ensure all voices are heard, but we will not be the decision-maker on the substantive elements of privacy codes of conduct.

B. Engaging Our International Partners

NTIA is also actively involved in implementing the international recommendations of the Privacy Blueprint. Consumer privacy is an increasingly important trade issue. Companies that do business globally face a complex set of privacy challenges, and complying with disparate privacy laws across the world imposes significant costs on U.S. enterprises. Moreover, these laws are in flux, as many of our trading partners in Europe, Asia, and Latin America are developing or revising their privacy frameworks.[32] Though the United States shares many privacy values with other countries, we expect that differences will remain between our consumer data privacy framework and those of our international partners.

[32] *See, e.g.*, European Commission, Commission Proposes a Comprehensive Reform of the Data Protection Rules, Jan. 25, 2012, *available at* http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm; Hunton & Williams, Mexico Issues New Privacy Regulations Effective December 22, 2011, Privacy and Security Law Blog, Dec. 21, 2011, available at http://www.huntonprivacyblog.com/2011/12/articles/mexico-issues-new-privacy-regulations-effective-december-22-2011/; ABS-CBN News, Senate Approves Data Privacy Act on 3rd Reading, Mar. 20, 2012, *available at* http://www.abs-cbnnews.com/business/03/20/12/senate-approves-data-privacy-act-3rd-reading (reporting on legislation in the Philippines); Kevin Kwang, Singapore Seeks Input for Data Protection Law, ZDNet, Sept. 14, 2011, *available at* http://www.zdnetasia.com/singapore-seeks-input-for-data-protection-law-62302071.htm.

As a result, the Privacy Blueprint recommends pursuing a course of creating greater interoperability—based on mutual recognition of common privacy values, shared efforts to develop internationally recognized codes of conduct, and enforcement cooperation—with other privacy frameworks, rather than seeking uniformity or full harmonization.[33] As the Joint Statement issued on March 19 by Secretary Bryson and European Commission Vice-President Viviane Reding states, "[t]he European Union and the United States are global leaders in protecting individual freedoms, including privacy, while at the same time fostering innovation and trade that are so critical to the world economy, notably in the present times. Stronger transatlantic cooperation in the field of data protection will enhance consumer trust and promote the continued growth of the global Internet economy and the evolving digital transatlantic common market."[34]

We at NTIA are working closely with our counterparts in the Department and throughout the Executive Branch to pursue greater interoperability of privacy frameworks. An important activity for NTIA over the next year will be to promote the privacy multistakeholder approach internationally. We expect that a diverse array of stakeholders will participate in the processes we will convene and welcome those stakeholders who have a practical perspective on global

[33] The Department's International Trade Administration (ITA) has played an integral role in establishing frameworks for interoperability. For example, the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks establish significant interoperability between the United States and Europe. These Frameworks allow companies to self-certify that they comply with requirements under the EU Data Protection Directive, subject to FTC enforcement of these representations. More than 3,000 companies have participated in the Safe Harbor Frameworks, enabling them to transfer personal data from the EU to the United States. As a result, the Safe Harbor Frameworks have effectively reduced barriers to personal data flow and thereby support trade and economic growth. *See generally* Department of Commerce, Export.gov – Safe Harbor, *available at* http://export.gov/safeharbor/ (last visited Mar. 16, 2012). In addition, ITA, along with the FTC, is helping to implement the Asia-Pacific Economic Cooperation's (APEC) voluntary system of Cross Border Privacy Rules, which will facilitate transnational mutual recognition among APEC's 21 member economies. *See* APEC, Electronic Commerce Steering Group, *available at* http://apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx (last visited Mar. 16, 2012).

[34] U.S.-EU Joint Statement on Privacy from EU Commission Vice-President Viviane Reding and U.S. Commerce Secretary John Bryson, Mar. 19, 2012, *available at* http://www.commerce.gov/news/press-releases/2012/03/19/us-eu-joint-statement-privacy-eu-commission-vice-president-viviane-re. The full text of the Joint Statement is included as an attachment to this testimony.

privacy compliance challenges. Finally, we will continue to coordinate with our U.S. Government counterparts to keep a close watch on legal developments in Europe and other regions and to participate in privacy discussions in forums such as the OECD and APEC.[35]

V. Conclusion

Thank you again for the opportunity to articulate the Administration's consumer data privacy policy and to discuss the steps NTIA is taking to put this policy into practice. NTIA is eager to bring stakeholders together to address privacy issues through practices that protect consumers, provide businesses with greater certainty, and allow continuing innovations that benefit our economy. We also look forward to working with you and other stakeholders to work toward the enactment of the Consumer Privacy Bill of Rights into law. I welcome any questions you have for me.

[35] These objectives of encouraging international cooperation for effective commercial data privacy protections and promoting and enhancing multistakeholder venues to discuss Internet policy issues are important elements of the Administration's overall cyberspace policy framework. *See* The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, at 22, 24, May 2011, *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Attachment: U.S.-EU Joint Statement on Privacy from EU Commission Vice-President Viviane Reding and U.S. Commerce Secretary John Bryson

Today's High Level Conference on Privacy and Protection of Personal Data, held simultaneously in Washington and Brussels with the participation of Vice-President Viviane Reding and Secretary John Bryson, represents an important opportunity to deepen our trans-Atlantic dialogue on commercial data privacy issues. The United States and the European Union clearly share a commitment to promoting the rights of individuals to have their personal data protected and to facilitating interoperability of our commercial data privacy regimes.

The European Union and the United States are global leaders in protecting individual freedoms, including privacy, while at the same time fostering innovation and trade that are so critical to the world economy, notably in the present times. Stronger trans-Atlantic cooperation in the field of data protection will enhance consumer trust and promote the continued growth of the global Internet economy and the evolving digital trans-Atlantic common market. This work will also encourage innovation and entrepreneurship and support the jobs and growth agenda as outlined by President Obama and Presidents Van Rompuy and Barroso at the November 28, 2011 U.S.-EU Summit.

This is a defining moment for global personal data protection and privacy policy and for achieving further interoperability of our systems on a high level of protection. On January 25, 2012, the European Commission adopted legislative proposals to reform and strengthen the fundamental right to data protection and unify the EU's data protection laws and enforcement rules. On February 23, 2012, the United States released its privacy blueprint, including the Consumer Privacy Bill of Rights. President Obama emphasized the administration's commitment to privacy in the U.S., and called for Congress to pass legislation that applies the Consumer

Privacy Bill of Rights to commercial sectors not subject to existing Federal data privacy laws and development of enforceable codes of conduct through multistakeholder processes.

Stakeholders in the U.S. are very interested in the ongoing data protection reform in the European Union–notably in the proposal for a "one-stop-shop" and a consistent regulatory level playing field across all EU Member States. Additionally, as expressed in the Obama administration's privacy blueprint, the United States is committed to engaging with the European Union and other international partners to increase interoperability in privacy laws and regulations, and to enhance enforcement cooperation. The European Union is following new privacy developments in the United States closely. Both parties are committed to working together and with other international partners to create mutual recognition frameworks that protect privacy. Both parties consider that standards in the area of personal data protection should facilitate the free flow of information, goods and services across borders. Both parties recognize that while regulatory regimes may differ between the U.S. and Europe, the common principles at the heart of both systems, now re-affirmed by the developments in the US, provide a basis for advancing their dialog to resolve shared privacy challenges. This mutual interest shows there is added value for the enhanced EU-U.S. dialogue launched with today's data protection conference.

We hope to also work with international stakeholders towards a global consensus on how to tackle emerging privacy issues.

In line with the objectives of increasing trade and regulatory cooperation outlined by our leaders at the U.S.-EU Summit, the United States and the European Union reaffirm their respective commitments to the U.S.-EU Safe Harbor Framework. This Framework, which has been in place since 2000, is a useful starting point for further interoperability. Since its inception,

over 3,000 companies have self-certified to the Framework to demonstrate their commitment to privacy protection and to facilitate transatlantic trade. The European Commission and the Department of Commerce look forward to continued close U.S.-EU collaboration to ensure the continued operation and progressive updates to this Framework. As the EU and the United States continue to work on significant revisions to their respective privacy frameworks over the next several years, the two sides will endeavor to find mechanisms that will foster the free flow of data across the Atlantic. Both parties are committed to work towards solutions based on non-discrimination and mutual recognition when it comes to personal data protection issues which could serve as frameworks for global interoperability that can promote innovation, the free flow of goods and services, and privacy protection around the world. The EU and the United States remain dedicated to the operation of the Safe Harbor Framework-as well as to our continued cooperation with the Commission to address issues as they arise-as a means to allow companies to transfer data from the EU to the United States, and as a tool to promote transatlantic trade and economic growth.

While this conference was convened to discuss commercial data privacy questions and not issues of exchanges of information related to law enforcement, we note that our presidents announced at the November 2011 summit that the US and the EU are determined to finalize negotiations on a comprehensive EU-U.S. data privacy and protection agreement that provides a high level of privacy protection for all individuals and thereby facilitates the exchange of data needed to fight crime and terrorism.

Mrs. BONO MACK. Thank you very much, Mr. Strickling.

Mr. Leibowitz, you are recognized for 5 minutes.

STATEMENT OF JON LEIBOWITZ

Mr. LEIBOWITZ. Thank you, Chairman Bono Mack, Ranking Member Butterfield, Chairman Upton, Vice Chair Blackburn, Mr. Gonzalez, Mr. Kinzinger, and Mr. Olson for the opportunity to comment the commission's testimony on consumer privacy.

I am particularly pleased to be along side Larry Strickling of Department of Commerce, who has done a terrific job. And we at the commission look forward to working with him and the department on privacy codes of conduct as well as with this committee on a variety of privacy issues.

This is a decisive moment for consumer privacy. The collection of personal data has lead to great benefits for consumers. We all want and need these benefits to continue but not at the expense of individual privacy. So after careful consideration, earlier this week, the Federal Trade Commission, the Nation's privacy protection agency, released a report that lays out what we in the public and private sectors must do to make sure that the right to privacy for all Americans remains robust.

The answer is simple: Consumers should have control of their personal data. And to ensure that control, our report lays out three powerful principles for companies to follow: First, incorporate privacy protections into products as you are developing them, that is the privacy by design; second, offer consumers choice about how their data is collected and used; and third, provide more transparency, that is better explanations to consumers about how information is handled.

The best companies are already following these principles, but baseline privacy legislation, if we can hit what you, Chairman Bono Mack, called the sweet spot would help them with clear rules of the road and ensure that the best privacy practices don't put companies at a competitive disadvantage.

Let me highlight perhaps one the most important recommendations we make in the report, that all stakeholders should continue to push forward to complete a Do Not Track system. Do Not Track is a one-stop mechanism that lets consumers control whether their online activities are tracked across Web sites. It is not run by the government but by companies themselves. It is voluntary. An effective Do Not Track system would going beyond merely allowing consumers to opt out of receiving targeted ads. It would allow them to opt out of third-party collection of behavioral data, other than data gathered for operational purposes, like preventing click fraud.

Because your computer is your property, no one should have the right to put anything in it that you don't want. And going back to Ms. Blackburn's point, that is a very conservative notion.

I am optimistic that companies can get Do Not Track done by the end of the year. To their enormous credit, since we issued our call for Do Not Track in 2010, online advertisers, major browser companies and the World Wide Web Consortium, an Internet standards-setting group have all made strides towards putting in place the foundation or Do Not Track system. Why? Because really, going back to the point that Chairman Upton made, they recognize that

Do Not Track will help build consumer confidence in the Internet, and that in turn will spur greater Internet commerce.

We also will continue working with them to implement fully a system in which all consumers can easily and effectively choose not to be tracked in cyberspace.

Our final privacy report also recommends that data brokers, who often hold a wealth of information about consumers but remain invisible to them, improve transparency. We renew our call for targeted legislation giving consumers reasonable access to consumer data that these brokers maintain; that is, access that is proportionate to the sensitivity of the data and its intended use.

In addition, we will be holding workshops in 2012, to explore two other issues, mobile privacy disclosures or dot-com disclosures and data platforms like social media, ISPs and operating systems.

Now while policy is an important component of our work, enforcement remains the commission's priority. We are not, as you know, a regulatory agency. The commission has brought more than 100 spam and spyware cases; 80 cases against those violating the Do Not Call rule; more than 30 data security cases; and 18 cases involving the children's online privacy protection act. As you know, we are in the process of updating the COPPA rules to account for changes in technology.

We have also obtained orders against numerous companies from making deceptive claims about privacy protections, including the recently highly publicized privacy cases against Google and Facebook, which, combined, protect the privacy of more than 1 billion users worldwide.

Just this week, we announced a settlement with RockYou, which is a popular social media gaming company. The FTC charged that the company failed to use adequate security measures to protect consumers private data. As a result, hackers gained access to personal information of more than 32 million customers. The commission also charged RockYou with collecting personal information from children it knew to be under 13 without parental consent; that is a COPPA violation. Under the commission's settlement, RockYou must implement a data security program, undergo audits every other year, and pay a $250,000 civil penalty.

Finally, the commission promotes privacy and data security through consumer and business education. For example, we sponsor Onguard Online, a Web site that educates consumers about basic computer security. Since its launch in 2005, Onguard Online and its Spanish language counterpart, Alerta en Linea, have had more than 25 million visitors.

Chairman, thank you for inviting me here today. We look forward to continuing to work with Congress, the administration industry and other stakeholders on privacy issues in the future, and I am happy to answer questions.

[The prepared statement of Mr. Leibowitz follows:]

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

BALANCING PRIVACY AND INNOVATION:

DOES THE PRESIDENT'S PROPOSAL TIP THE SCALE?

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

March 29, 2012

I. Introduction

Chairman Bono Mack, Ranking Member Butterfield, and members of the Subcommittee, I am Jon Leibowitz, Chairman of the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on consumer privacy.

I am pleased to be testifying today alongside Administrator Lawrence Strickling of the National Telecommunications and Information Administration. The Commission supports the recent efforts and approach developed by the Department of Commerce regarding privacy issues. The FTC looks forward to working together with the Department of Commerce and the Administration as they move forward in their efforts in this arena.

This is a decisive moment for consumer privacy. New and refined approaches to privacy protection are emerging in the United States and around the world. After careful consideration, earlier this week the Commission released its final privacy report that sets forth best practices for businesses to protect consumer privacy while ensuring that companies can continue to innovate.[2]

---

[1] The views expressed in this statement represent the views of the Commission, with Commissioner J. Thomas Rosch dissenting. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any other Commissioner.

[2] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf. Commissioner Rosch dissented from the issuance of the Final Privacy Report. He agrees that consumers ought to be given a broader range of choices and applauded the Report's call for targeted legislation regarding data brokers and data security. However, Commissioner Rosch has four major concerns about the privacy framework because he believes that: 1) in contravention of our promises to Congress, it is based on "unfairness" rather than deception; 2) the current state of "Do Not Track" still leaves unanswered many important questions; 3) "opt-in" will necessarily be selected as the de facto method of consumer choice for a wide swath of entities; and 4) although characterized as only "best practices," the Report's recommendations may be construed as federal requirements. *See* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf at Appendix C.

The Commission urges industry to use this guidance to improve privacy practices and accelerate the pace of self-regulation. Importantly, we have seen promising developments by industry toward a Do Not Track mechanism and we ask the Committee to continue to encourage industry to move towards full implementation.

Members of Congress and this Committee on both sides of the aisle have demonstrated that they understand how important it is that consumers' personal data be treated with care and respect. The Commission commends the leadership this Committee has shown on consumer privacy issues. Just last month, the Administration released its final "White Paper" on consumer privacy, recommending that Congress enact legislation to implement a Consumer Privacy Bill of Rights.[3] Today we recommend that Congress consider enacting general privacy legislation. We reiterate our call on Congress to enact legislation requiring companies to implement reasonable security measures and to notify consumers in the event of certain security breaches,[4] as well as targeted legislation that would provide consumers with access to information about them held by

---

[3] *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[4] The Commission has long supported such federal laws. *See, e.g.*, Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong. (June 15, 2011), *available at* http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf; Prepared Statement of the FTC, *Protecting Social Security Numbers From Identity Theft: Hearing Before the Before the H. Comm. on Ways and Means, Subcomm. on Social Security*, 112th Cong. (Apr. 13, 2011), *available at* http://ftc.gov/os/testimony/110411ssn-idtheft.pdf; FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), *available at* http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf; and President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), *available at* http://www.idtheft.gov/reports/IDTReport2008.pdf.

data brokers.[5]

Privacy has been an important part of the Commission's consumer protection mission for more than 40 years.[6] During this time, the Commission's goal in the privacy arena has remained constant: to protect consumers' personal information and ensure that they have the confidence to take advantage of the many benefits offered by the dynamic and ever-changing marketplace. To meet this objective, the Commission has undertaken substantial efforts to promote privacy in the private sector through law enforcement, education, and policy initiatives. For example, since 2001, the Commission has brought 36 data security cases; more than 100 spam and spyware cases; and 18 cases for violation of the Children's Online Privacy Protection Act ("COPPA").[7] The Commission has also brought recent highly publicized privacy cases against companies such as Google and Facebook. The Commission has distributed millions of copies of educational materials for consumers and businesses to address ongoing threats to security and privacy. And the FTC continues to examine the implications of new technologies and business practices on consumer privacy through ongoing policy initiatives, such as the Commission's recently-released report on consumer privacy.

This testimony begins by describing the Commission's final privacy report. It then offers an overview of other recent policy efforts in the areas of privacy and data security and concludes

---

[5] The Commission supports legislation similar to that contained in several of the data security bills introduced in the 112th Congress. *See* Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011).

[6] Information on the FTC's privacy initiatives generally may be found at business.ftc.gov/privacy-and-security.

[7] 15 U.S.C. §§ 6501-6508.

by noting the Commission's recent enforcement and education efforts.

II. Privacy Report

Earlier this week, the FTC released its final privacy report ("Final Report"), setting forth best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. To the extent these best practices exceed existing legal requirements, they are not intended to serve as a template for law enforcement or regulations under laws currently enforced by the FTC.

The Final Report continues to support the three main principles laid out in the preliminary staff report.[8] *First*, companies should adopt a "privacy by design" approach by building privacy protections into their everyday business practices. Such protections include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer in use, and implementing reasonable procedures to promote data accuracy.

Second, companies should provide simpler and more streamlined choices to consumers

---

[8] In December 2010, the Commission issued a preliminary staff report to address the privacy issues associated with new technologies and business models. *See A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. Commissioners Kovacic and Rosch issued concurring statements available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf at Appendix D and Appendix E, respectively. The preliminary staff report set forth a proposed framework to guide policymakers and other stakeholders regarding best practices for consumer privacy and included a number of questions for public comment. The Commission received over 450 public comments from various stakeholders in response to the preliminary report. These comments informed the Commission as it refined the framework to best protect consumer privacy and innovation in today's dynamic and rapidly-changing marketplace.

about their data practices. Companies do not need to provide choice before collecting and using consumers' data for practices that are consistent with the context of the transaction, the company's relationship with the consumer, or as required or specifically authorized by law. For all other data practices, consumers should have the ability to make informed and meaningful choices at a relevant time and context and in a uniform and comprehensive way. The Commission advocated such an approach for online behavioral tracking – often referred to as "Do Not Track" – that is discussed in more detail below.

Third, companies should take steps to make their data practices more transparent to consumers. For instance, companies should improve their privacy disclosures and work toward standardizing them so that consumers, advocacy groups, regulators, and others can compare data practices and choices across companies, thus promoting competition among companies. Consumers should also have reasonable access to the data that companies maintain about them, particularly for non-consumer-facing entities such as data brokers, as discussed in more detail below. The extent of access should be proportional to the volume and sensitivity of the data and to its intended use.

In addition, the Final Report supports the development of general privacy legislation to ensure basic privacy protections across all industry sectors, and the Report can inform Congress, should it consider such legislation. The Commission recommends that any such legislation be technologically neutral and sufficiently flexible to allow companies to continue to innovate. In addition, the Commission believes that any legislation should allow the Commission to seek civil penalties to deter statutory violations. Such legislation would provide businesses with the certainty they need to understand their obligations and the incentive to meet those obligations, while also assuring consumers that companies will respect their privacy. We believe this

approach would foster an environment that allows businesses to innovate and consumers to embrace those innovations without fear of sacrificing their privacy. We look forward to working with Congress and other stakeholders to craft this legislation.

The Report's recommendations broadly address the commercial use of consumer information, both online and offline, by all manner of businesses. Below, we highlight two specific issues addressed in the Report – Do Not Track and data brokers.

A. Do Not Track

The final report advocates the continued implementation of a universal, one-stop mechanism to enable consumers to control the tracking of their online activities across websites, often referred to as "Do Not Track," which the Commission first called for in December 2010 and members of Congress have sought through legislative proposals.[9]

The Commission commends recent industry efforts to improve consumer control over behavioral tracking in response to those calls. As industry explores technical options and implements self-regulatory programs, and as Congress examines Do Not Track, the Commission continues to believe that an effective Do Not Track system should include five key principles. *First*, a Do Not Track system should be implemented universally to cover all parties that would track consumers. *Second*, the choice mechanism should be easy to find, easy to understand, and easy to use. *Third*, any choices offered should be persistent and should not be overridden if, for example, consumers clear their cookies or update their browsers. *Fourth*, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of

[9] Do Not Track is intended to apply to third-party tracking of consumers because third-party tracking is inconsistent with the context of a consumer's interaction with a website; most first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice.

behavioral tracking through any means and not permit technical loopholes.[10] *Fifth*, an effective Do Not Track system should go beyond simply opting consumers out of receiving targeted advertisements; it should opt them out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction (*e.g.*, preventing click-fraud or frequency capping for ads).[11]

Early on, the companies that develop web browsers stepped up to the challenge to give consumers choice about how they are tracked online, sometimes known as the "browser header" approach. When consumers enable Do Not Track, the browser transmits the header to all types of entities, including advertisers, analytics companies, and researchers, that track consumers online. Just after the FTC's call for Do Not Track, Microsoft developed a system to let users of Internet Explorer prevent tracking by different companies and sites.[12] Mozilla introduced a Do Not Track privacy control for its Firefox browser that an impressive number of consumers have adopted.[13] Apple subsequently included a similar Do Not Track control in Safari.[14] Google has

---

[10] For example, the FTC recently brought an action against a company that told consumers they could opt out of tracking by exercising choices through their browsers; however, the company used Flash cookies for such tracking, which consumers could not opt out of through their browsers. *In the Matter of ScanScout, Inc.*, FTC Docket No. C-4344 (Dec. 21, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023185/111221scanscoutdo.pdf.

[11] Such a mechanism should be different from the Do Not Call program in that it should not require the creation of a "Registry" of unique identifiers, which could itself cause privacy concerns.

[12] Press Release, Microsoft, *Providing Windows Customers with More Choice and Control of Their Privacy Online with Internet Explorer 9* (Dec. 7, 2010), *available at* www.microsoft.com/presspass/features/2010/dec10/12-07ie9privacyqa.mspx;

[13] The Mozilla Blog, *Mozilla Firefox 4 Beta, Now Including "Do Not Track" Capabilities* (Feb. 8, 2011), blog.mozilla.com/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/; Alex Fowler, *Do Not Track Adoption in Firefox Mobile is 3x Higher than Desktop*, MOZILLA PRIVACY BLOG (Nov. 2, 2011),

taken a slightly different approach – providing consumers with a tool that persistently opts them out of most behavioral advertising.[15]

In another important effort, the online advertising industry, led by the DAA, has implemented a behavioral advertising opt-out program. The DAA's accomplishments are notable: it has developed a notice and choice mechanism through a standard icon in ads and on publisher sites; deployed the icon broadly, with reportedly over 900 billion impressions served each month; obtained commitments to follow the self-regulatory principles from advertisers, ad networks, and publishers that represent close to 90 percent of the online behavioral advertising market; and established an enforcement mechanism designed to ensure compliance with the principles.[16] More recently, the DAA addressed one of the long-standing criticisms of its approach – how to limit secondary use of collected data so that the consumer opt-out extends beyond simply blocking targeted ads and to the collection of information for other purposes. The DAA has released new principles that include limitations on the collection of tracking data

---

http://blog.mozilla.com/privacy/2011/11/02/do-not-track-adoption-in-firefox-mobile-is-3x-higher-than-desktop/.

[14] Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser*, WALL ST. J., Apr. 13, 2011, *available at* http://online.wsj.com/article/SB10001424052748703551304576261272308358858.html.

[15] Sean Harvey & Rajas Moonka, *Keep Your Opt Outs*, GOOGLE PUBLIC POLICY BLOG (Jan. 24, 2011), http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html.

[16] Peter Kosmala, *Yes, Johnny Can Benefit From Transparency & Control*, SELF-REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING, http://www.aboutads.info/blog/yes-johnny-can-benefit-transparency-and-control (Nov. 3, 2011); *see also* Press Release, Digital Advertising Alliance, *White House, DOC and FTC Commend DAA's Self-Regulatory Program to Protect Consumers Online Privacy* (Feb. 23, 2012), *available at* http://www.aboutads.info/resource/download/DAA%20White%20House%20Event.pdf.

and prohibitions on the use or transfer of the data for employment, credit, insurance, or health care eligibility purposes.[17] Just as important, the DAA recently moved to address some persistence and usability criticisms of its icon-based opt out by committing to honor the tracking choices consumers make through their browser settings.[18]

At the same time, the World Wide Web Consortium ("W3C"), an Internet standards-setting body, has gathered a broad range of stakeholders to create an international, industry-wide standard for Do Not Track, including DAA member companies; other U.S. and international companies; industry groups; and public interest organizations. The W3C group has done admirable work to flesh out how to make a Do Not Track system practical in both desktop and mobile settings as reflected in two public working drafts of its standards.[19] Some important issues remain, and the Commission encourages all of the stakeholders to work within the W3C group to resolve these issues.

While work remains to be done on Do Not Track, the Commission believes that the developments to date are significant and provide an effective path forward. The advertising industry, through the DAA, has committed to deploy browser-based technologies for consumer control over online tracking, alongside its ubiquitous icon program. The W3C process, thanks in part to the ongoing participation of DAA member companies, has made substantial progress

---

[17] Digital Advertising Alliance, *About Self-Regulatory Principles for Multi-Site Data* (Nov. 2011), *available at* http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

[18] Press Release, Digital Advertising Alliance, *DAA Position on Browser Based Choice Mechanism* (Feb. 22, 2012), *available at* http://www.aboutads.info/resource/download/DAA.Commitment.pdf.

[19] *See* Press Release, W3C, *W3C Announces First Draft of Standard for Online Privacy* (Nov. 14, 2011), *available at* http://www.w3.org/2011/11/dnt-pr.html.en.

toward specifying a consensus consumer choice system for tracking that is practical and technically feasible.[20] The Commission anticipates continued progress in this area as the DAA members and other key stakeholders continue discussions within the W3C process to work to reach consensus on a Do Not Track system in the coming months.

B. Data Brokers

The Final Report recommends that companies provide consumers with reasonable access to the data maintained about them. The extent of such access should be proportionate to the sensitivity of the data and the nature of its use.

The Final Report addresses the particular importance of consumers' ability to access information that data brokers have about them. Data brokers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information for a variety of purposes, including verifying an individual's identity, differentiating one consumer's records from another's, marketing products, and preventing financial fraud. Such entities often have a wealth of information about consumers without interacting directly with them. Consumers are often unaware of the existence of these entities, as well as the purposes for which they collect and use data.[21]

The Commission has monitored data brokers since the 1990s, hosting workshops, drafting reports, and testifying before Congress about the privacy implications of data brokers'

---

[20] A system practical for both businesses and consumers would include, for users who choose to enable Do Not Track, significant controls on the collection and use of tracking data by third parties, with limited exceptions such as security and frequency capping. As noted above, first party sharing with third parties is not consistent with the context of the interaction and would be subject to choice. Do Not Track is one way for users to express this choice.

[21] As noted above, first-party sharing with third parties is not consistent with the context of the interaction and would be subject to choice.

practices.[22] Following a Commission workshop, data brokers created the Individual References Services Group (IRSG), a self-regulatory organization for certain data brokers.[23] Although industry ultimately terminated this organization, a series of public breaches – including one involving ChoicePoint – led to renewed scrutiny of the practices of data brokers.[24] There have nonetheless been no meaningful broad-based efforts to implement self-regulation in this area in recent years.

To improve the transparency of the practices of data brokers, the Final Report proposes that data brokers, like all companies, provide consumers with reasonable access to the data they maintain. Because most data brokers are invisible to consumers, however, the Commission makes two additional recommendations as to these entities.

First, since 2009, the Commission has supported legislation giving access rights to consumers for information held by data brokers.[25] During the 111th Congress, the House

---

[22] *See, e.g.*, Prepared Statement of the FTC, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before the Senate Comm. on Banking, Housing, and Urban Affairs*, 109th Cong. (Mar. 10, 2005), *available at* http://www.ftc.gov/os/testimony/050310idtheft.pdf; *see also* FTC Workshop, *The Information Marketplace: Merging & Exchanging Consumer Data* (Mar. 13, 2001), *available at* http://www.ftc.gov/bcp/workshops/infomktplace/index.shtml; FTC Workshop, *Information Flows: The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information* (June 18, 2003), *available at* http://www.ftc.gov/bcp/workshops/infoflows/030618agenda.shtm.

[23] *See* FTC, *Individual Reference Services, A Report to Congress* (1997), *available at* http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm.

[24] *See* Prepared Statement of the FTC, *Protecting Consumers' Data: Policy Issues Raised by ChoicePoint: Hearing before H. Comm. on Energy & Commerce, Subcomm. on Commerce, Trade, and Consumer Protection, Comm. on Energy & Commerce*, 109th Cong. (Mar. 15, 2005), *available at* http://www.ftc.gov/os/2005/03/050315protectingconsumerdata.pdf.

[25] *See, e.g.*, Prepared Statement of the FTC, *Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act: Hearing Before*

approved a bill that included provisions to establish a procedure for consumers to access information held by data brokers.[26] The Commission continues to support legislation in this area to improve transparency of the industry's practices.[27]

Second, the Commission recommends that the data broker industry explore the idea of creating a centralized website where data brokers could identify themselves to consumers and describe how they collect consumer data and disclose the types of companies to which they sell the information. Additionally, data brokers could use the website to explain the access rights and other choices they offer consumers, and could offer links to their own sites where consumers could exercise such options. This website would improve transparency and enhance consumer control over the data practices of companies that maintain and share data about them for marketing purposes. It could also provide consumer-facing entities such as retailers a means for ensuring that the information brokers from which they purchase consumer information have instituted appropriate transparency and control mechanisms. Indeed, the consumer-facing

---

the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer Protection, 111th Cong. (May 5, 2009), *available at* http://www.ftc.gov/os/2009/05/P064504peertopeertestimony.pdf.

[26] Data Accountability and Trust Act, H.R. 2221, 111th Congress (as passed by House, Dec. 8, 2009).

[27] *See, e.g.*, Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong. (May 4, 2011), *available at* http://www.ftc.gov/opa/2011/05/pdf/110504datasecurityhouse.pdf; Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong.(June 15, 2011), *available at* http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf; Prepared Statement of the FTC, *Protecting Consumers in the Modern World: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 112th Cong. (June 29, 2011), *available at* http://www.ftc.gov/os/testimony/110629privacytestimonybrill.pdf.

entities could provide consumers with a link to the centralized website, after having made sure that the data brokers from which they buy data participate in such a system. The Commission staff intends to discuss with relevant companies how this mechanism could be developed and implemented voluntarily, to increase the transparency and give consumers tools to opt out.[28]

III. Other Policy Initiatives

In addition to conducting policy reviews, such as through the Final Report, the Commission has conducted public workshops and issued reports to examine the implications of new technologies and business practices on consumer privacy. Four examples are of note.

First, in February 2012, the Commission released a staff report on mobile applications ("apps") for children.[29] The report found that in virtually all cases, neither app stores nor app developers provide disclosures that tell parents what data apps collect from children, how apps share it, and with whom. The report recommends that all members of the children's app ecosystem – the stores, developers and third parties providing services – should play an active role in providing key information to parents.[30] The report also encourages app developers to provide information about data practices simply and succinctly. The Commission has already

---

[28] The current website of the Direct Marketing Association (DMA) offers an instructive model for such a mechanism. The DMA – which consists of data brokers, retailers, and others – currently offers a service through which consumers can opt out of receiving marketing solicitations via particular channels, such as direct mail, from DMA member companies. *See* DMAChoice, http://www.dmachoice.org/dma/member/home.action.

[29] FTC Staff Report, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), *available at* http://www.ftc.gov/opa/2012/02/mobileapps_kids.shtm

[30] News reports indicate that some companies, like Apple, are already working to limit certain types of data collection via apps. *See, e.g.*, Kim-Mai Cutler, *Amid Privacy Concerns, Apple Has Started Rejecting Apps That Access UDID*, TECHCRUNCH (Mar. 24, 2012), http://techcrunch.com/2012/03/24/apple-udids/.

reached out to work with industry to provide parents with the information they need.

To discuss how members of the mobile and online ecosystems can best disclose their data collection and sharing practices to consumers, the Commission plans to host a public workshop in May 2012.[31] The workshop will address the technological advancements and marketing developments that have emerged since the FTC first issued its online advertising disclosure guidelines known as "Dot Com Disclosures."[32] The workshop will examine whether and how to revise the Dot Com Disclosures in the current online and mobile advertising environment and will include a specific panel on mobile privacy disclosures.

Second, the FTC hosted a workshop in December 2011 that explored facial recognition technology and the privacy and security implications raised by its increasing use.[33] Facial detection and recognition technology has been adopted in a variety of new contexts, ranging from online social networks to digital signs and mobile apps. The FTC workshop gathered key stakeholders to focus on the current and future commercial applications of these technologies, discuss an array of current and future uses and benefits, and explore potential privacy and security concerns. Since then, Commission staff sought comments on the issues raised during the workshop and will issue a report in the coming months.

Third, as discussed in the Final Report, the FTC intends to examine the practices of large platforms such as Internet browser companies, mobile operating system providers, Internet

---

[31] FTC Workshop, *Dot Com Disclosures* (May 30, 2012), *available at* http://www.ftc.gov/opa/2012/02/dotcom.shtm.

[32] FTC, *Dot Com Disclosures* (2000), *available at* http://www.ftc.gov/os/2000/05/0005dotcomstaffreport.pdf

[33] FTC Workshop, *Face Facts: A Forum on Facial Recognition Technology* (Dec. 8, 2011), *available at* http://www.ftc.gov/bcp/workshops/facefacts/.

Service Providers, and large social media platforms that can collect data from numerous sources to build extensive profiles about consumers. Commission staff will host a workshop in the second half of 2012 to examine questions about the scope of such data collection practices, the potential uses of the collected data, and related issues.

Finally, the Commission is undertaking a comprehensive review of the COPPA Rule in light of rapidly evolving technology and changes in the way children use and access the Internet.[34] In September 2011, the Commission proposed modifications to the Rule intended to update the Rule to meet changes in technology, assist operators in their compliance obligations, strengthen protections over children's data, and provide greater oversight of COPPA safe harbor programs.[35] For example, the Commission proposed adding geolocation information and cookies used for behavioral advertising to the definition of "personal information," which would have the effect of requiring parental consent for collection. In addition, the Commission proposed adding a new provision addressing data retention and deletion. The Commission received over 350 comments on its proposed amendments to the COPPA Rule, which are being reviewed by FTC staff.

IV. Enforcement

In addition to its engagement on the policy front, enforcement remains a top priority for the agency. In the last 15 years, the Commission has brought 36 data security cases; almost 80

---

[34] *See* Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 75 Fed. Reg. 17,089 (Apr. 5, 2010), *available at* http://www.ftc.gov/os/fedreg/2010/april/P104503coppa-rule.pdf.

[35] The Commission's Notice of Proposed Rulemaking can be found at 76 Fed. Reg. 59,804 (Sept. 15, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-27/pdf/2011-24314.pdf.

cases against companies for improperly calling consumers on the Do Not Call registry;[36] 86 cases against companies for violating the Fair Credit Reporting Act ("FCRA");[37] 97 spam cases; 15 spyware or nuisance adware cases; 18 COPPA cases; and numerous cases against companies for violating the FTC Act by making deceptive claims about the privacy and security protections they afford to consumer data. Where the FTC has authority to seek civil penalties, it has aggressively done so. It has obtained $60 million in civil penalties in Do Not Call cases; $21 million in civil penalties under the FCRA; $5.7 million under the CAN-SPAM Act;[38] and $6.6 million under COPPA. Where the Commission does not have authority to seek civil penalties, as in the data security and spyware areas, it has sought such authority from Congress.

Two recent privacy cases – against Internet giants Google and Facebook – will benefit more than one billion consumers worldwide. The Commission charged Google with deceiving consumers by taking previously private information – the frequent contacts of Gmail users – and making it public in order to generate and populate a new social network, Google Buzz.[39] This, the Commission alleged, was done without the users' consent and in contravention of Google's privacy policy. Significantly, as part of the Commission's decision and consent order, Google must protect the privacy of consumers who use Gmail and Google's many other products and services. Under the order, if Google changes a product or service in a way that makes consumer information more widely available to third parties, it must seek affirmative express consent to

---

[36] 16 C.F.R. Part 310.

[37] 15 U.S.C. §§ 1681e-i.

[38] 15 U.S.C. §§ 7701-7713.

[39] *Google, Inc.*, Docket No. C-4336 (Oct. 13, 2011) (final decision and consent order), *available at* http://www.ftc.gov/opa/2011/10/buzz.shtm.

such a change. This provision applies to any data collected from or about consumers. In addition, the order requires Google to implement a comprehensive privacy program and obtain independent privacy audits every other year for the next 20 years.

The FTC's case against Facebook alleged a number of deceptive and unfair practices.[40] These include the 2009 changes made by Facebook so that information users had designated private – such as their "Friends List" or pages that they had "liked" – became public. The complaint also charged that Facebook made inaccurate and misleading disclosures relating to how much information about users' apps operating on the site can access. For example, Facebook told users that the apps on its site would only have access to the information those apps "needed to operate." The complaint alleges that in fact, the apps could view nearly all of the users' information, regardless of whether that information was "needed" for the app's functionality. The Commission further alleged that Facebook made promises that it failed to keep: It told users it would not share information with advertisers, and then it did; and it agreed to take down photos and videos of users who had deleted their accounts, and then it did not. Similar to the Google Buzz order, the Commission's consent order against Facebook prohibits the company from deceiving consumers with regard to privacy; requires it to obtain users' affirmative express consent before sharing their information in a way that exceeds their privacy settings; and requires it to implement a comprehensive privacy program and obtain outside audits. In addition, Facebook must ensure that it will stop providing access to a user's information after she deletes her account.

Further, the Commission continues to be active on the data security and children's

---

[40] *Facebook, Inc.*, Matter No. 0923184 (Nov. 29, 2011) (proposed consent agreement), *available at* http://www.ftc.gov/opa/2011/11/privacysettlement.shtm.

privacy front. Just this week, it announced a settlement with RockYou, a company that allowed consumers to upload and store photos and slideshows.[41] Consumers who registered with RockYou were required to provide their email addresses and the password to their email accounts. Despite its claims to have reasonable security, RockYou allegedly failed to use reasonable and appropriate security measures to protect consumers' private data, resulting in hackers gaining access to 32 million email addresses and RockYou passwords. In addition, the Commission charges that RockYou collected personal information from approximately 179,000 children it knew to be under 13 without providing notice or gaining parental consent, as required by COPPA and in spite of claims to the contrary. Under the Commission's settlement, RockYou must implement a data security program and undergo audits every other year for the next 20 years and pay a $250,000 civil penalty.

V. Education

The FTC conducts outreach to businesses and consumers in the area of consumer privacy. The Commission's well-known OnGuard Online website educates consumers about many online threats to consumer privacy and security, including spam, spyware, phishing, peer-to-peer ("P2P") file sharing, and social networking.[42] Furthermore, the FTC provides consumer education to help consumers better understand the privacy and security implications of new technologies. For example, last year the Commission issued a guide that provides consumers with information about mobile apps, including what apps are, the types of data they can collect

---

[41] *See United States v. RockYou, Inc.*, No. CV 12 1487 (N.D. Cal. filed Mar. 26, 2012) (consent decree).

[42] *See* www.onguardonline.gov. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alerta en Línea have attracted more than 25 million visits.

and share, and why some apps collect geolocation information.[43]

The Commission has also issued numerous education materials to help consumers protect themselves from identity theft and to deal with its consequences when it does occur. The FTC has distributed over 3.8 million copies of a victim recovery guide, *Take Charge: Fighting Back Against Identity Theft*, and has recorded over 3.5 million visits to the Web version.[44] In addition, the FTC has developed education resources specifically for children, parents, and teachers to help children stay safe online. In response to the Broadband Data Improvement Act of 2008, the FTC produced the brochure *Net Cetera: Chatting with Kids About Being Online* to give adults practical tips to help children navigate the online world.[45] In less than one year, the Commission distributed more than 7 million copies of *Net Cetera* to schools and communities nationwide.

Business education is also an important priority for the FTC. The Commission seeks to educate businesses by publicizing its complaints and orders and issuing public closing and warning letters. For example, the Commission recently sent letters to the marketers of six mobile apps that provide background screening services.[46] The letters state that some of the apps included criminal record histories, which bear on an individual's character and general reputation and are precisely the type of information that is typically used in employment and

---

[43] *See* Press Release, FTC, *Facts from the FTC: What You Should Know About Mobile Apps* (June 28, 2011), *available at* http://www.ftc.gov/opa/2011/06/mobilcapps.shtm.

[44] *See Take Charge: Fighting Back Against Identity Theft, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

[45] *See* Press Release, FTC, *OnGuardOnline.gov Off to a Fast Start with Online Child Safety Campaign* (Mar. 31, 2010), *available at* www.ftc.gov/opa/2010/03/netcetera.shtm.

[46] Press Release, FTC, *FTC Warns Marketers that Mobile Apps May Violate Fair Credit Reporting Act* (Feb. 7, 2012), *available at* http://www.ftc.gov/opa/2012/02/mobilcapps.shtm.

tenant screening. The FTC warned the apps marketers that, if they have reason to believe the background reports they provide are being used for employment screening, housing, credit, or other similar purposes, they must comply with the FCRA. The Commission made no determination as to whether the companies are violating the FCRA, but encouraged them to review their apps and their policies and procedures to ensure they comply with the Act.

Another way in which the Commission seeks to educate businesses is by developing and distributing free guidance. For example, the Commission developed a widely-distributed guide to help small and medium-sized businesses implement appropriate data security for the personal information they collect and maintain.[47] The Commission also creates business educational materials on specific topics – such as the privacy and security risks associated with P2P file-sharing programs and companies' obligations to protect consumer and employee information from these risks[48] and how to properly secure and dispose of information on digital copiers.[49] These publications, as well as other business education materials, are available through the FTC's Business Center website, which averages one million unique visitors each month.[50] The Commission also hosts a Business Center blog,[51] which frequently features consumer privacy and data security topics; presently, approximately 3,500 attorneys and business executives

---

[47] *See Protecting Personal Information: A Guide For Business*, *available at* www.ftc.gov/infosecurity.

[48] *See Peer-to-Peer File Sharing: A Guide for Business*, *available at* http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm.

[49] *See* http://business.ftc.gov/documents/bus43-copier-data-security.

[50] *See generally* http://business.ftc.gov/. The Privacy and Data Security portal is the most popular destination for visitors to the Business Center.

[51] *See generally* http://business.ftc.gov/blog.

subscribe to these email blog updates.

VI. Conclusion

These policy, enforcement, and education efforts demonstrate the Commission's commitment to protecting consumers' privacy and security – both online and offline. As noted above, the Commission encourages Congress to develop general privacy legislation and to adopt targeted legislation addressing data brokers. We appreciate the leadership of this Committee on these issues and look forward to continuing to work with Congress, the Administration, industry and other critical stakeholders on these issues in the future.

Mrs. BONO MACK. Thank you very much for your testimony, gentlemen.

I would like to begin with recognizing myself for 5 minutes for questions, and I will start with you, Mr. Strickling. Who will be the final arbiter in the stakeholder process? And will the NTIA merely chair the discussions, or will it have a more substantial role?

Mr. STRICKLING. Our role is to facilitate the discussions and to serve as a convener. The outcome will be determined entirely by the participants in the process. It will be up to them to decide if and when they have reached consensus around a code to complete their work. We will not substitute our judgment for what they are doing. Other role will simply be to keep the parties talking and help guide them through the process to reaching a conclusion that they themselves will reach.

Mrs. BONO MACK. Do you have an idea how long this multi-stakeholder process should take or is going to take?

Mr. STRICKLING. Well, it is an ongoing process. We don't see this as just one set of discussions to create one code. In fact, starting out, we intentionally are going to try to choose a fairly discrete topic, perhaps one of our seven principles and perhaps one slice of industry, not because we are singling out any industry, but because we feel starting this process, we need to start with a discrete topic and a limited number of participants as we work through the process of having folks work together and reaching consensus. So we envision the potential that multiple codes will be created out of the process. It largely will be driven by the interests of industry responding to these concerns as they arise.

We will have the facility in place to help facilitate and convene these discussions, but we won't be dictating the number of codes or how frequently people meet or the rest of it. That is really up to the participants.

Mrs. BONO MACK. The blueprint recognizes that targeted ads are generally more valuable and the revenue derived therefrom supports an array of services and content as well as funds research and innovation. However, the blueprint calls on companies to, quote, provide consumers with meaningful opportunities to prevent disclosures to third parties. How do you foresee the balance between funding free services and the ability to innovate if consumers can prevent disclosure of information and thereby cutting off the critical stream of revenue?

Mr. STRICKLING. Well, let me go back to what I said before; I am not the regulator, and I am not the party that is going to make these judgments. What we want to do is run a process that will allow all interested stakeholders to carry out the discussions around questions just like the one you have just asked and try to reach a consensus view as to how best to approach it.

Again, to the extent that we at NTIA dictate what that outcome should be, that would put us in the role of tipping the balance that we are trying to achieve here as we allow industry and consumer groups to work on these issues together.

Mrs. BONO MACK. Thank you.

Mr. Leibowitz, what role did the commission play in the development of the administration's blueprint? Did you make any of the

recommendations that are included in the commission's report? And if so, why and why not?

Mr. LEIBOWITZ. I couldn't quite hear the last part of the question. Do we support the recommendations?

Mrs. BONO MACK. Did you make any of the recommendations? How involved in the process of formulating the blueprint were you?

Mr. LEIBOWITZ. So, working on your questions, from the last to first, we were involved in consulting with the Department of Commerce. We are very supportive of their approach. We will be involved, I believe, as sort of one of the ex officio stakeholders. And should codes of conduct be embraced by industry or accepted by industry, we will use the FTC act as a backstop for enforcing them. But, again, these codes of conduct are voluntary. And we are looking to forward to working with the Commerce Department.

Mrs. BONO MACK. Everybody is concerned about the unintended consequences. This question sort of falls on that. Are you concerned that some benefits of large anonymous data sets may be lost if many people sign up for Do Not Track? For example, predictions of flu patterns and epidemics by sharpened by recording information about searches relating to flu or other infectious diseases. If lots of people opt for no tracking, could these benefits be lost or at least undercut?

Mr. LEIBOWITZ. You know, I don't think so, Madam Chairman.

You know, one of the great things about this Do Not Track initiative is that the most supportive entities of it have been the business community. I think companies, you know, want more—I think the best companies and I think 90 percent of all companies involved in behavioral advertising or 90 percent of the advertising are supportive of the Digital Advertising Alliance, which is the business community's attempt to come up with a Do Not Track initiative. They have made great strides, and I don't believe that there will be any sort of informational harms to consumers. You will still be able to advertise to consumers, but consumers will have the right to opt out. Again, we think that is a deeply conservative right. It is a right to say no to people putting things in your computer.

Mrs. BONO MACK. Thank you.

My time has expired.

I recognize Mr. Butterfield for 5 minutes.

Mr. BUTTERFIELD. Thank you, Madam Chairman.

Before getting started, I am just told by my staff that Congressman Sarbanes from Maryland has been re-appointed to the committee.

Is that right, John?

Welcome back, thank you. Very much we look forward to your work.

All right. In its privacy report, the administration advances the framework that ideally includes the development and implementation of industry codes of conduct in parallel with Congress passing baseline privacy legislation. To the extent that the FTC intends to participate in the development of these codes of conduct and has also endorsed the idea of Congress passing baseline legislation, it also seems to endorse the idea that these things should happen in parallel or concurrently.

However, some are already arguing that these two pieces should be delinked from each other. That is the development and implementation of codes of conduct should completely play out before Congress takes any action on baseline privacy legislation. For example, one of today's witnesses argues, "If Congress is ever to grant the FTC new authority in this area, it should at least wait to learn from the self-regulatory process. Congress should assess the failure or success of the overall self regulatory scheme."

Let me ask both of you, I assume that you both disagree with the view that one should come after the other; instead, you agree that Congress should act sooner rather than later on comprehensive baseline privacy legislation. Can you please discuss why, ideally, development of codes of conduct should be accompanied by passage of a privacy law?

Mr. STRICKLING. So we absolutely support the passage of legislation to codify the baseline, the principles. Again, we don't envision this as being a complicated piece of legislation. We have given our—as we thought about it, we think 10- to 15-page bill ought to be adequate to capture what it is we are looking to do.

We do think and intend to proceed to work with industry and civil society on these voluntary codes of conduct, even as the legislative process continues. But clearly, I think industry would find greater certainty in the overall regime if legislation were passed as part of this process. But we will work with industry; we will work with civil society to develop these codes as we move forward.

Mr. LEIBOWITZ. I would say, too, you have to hit the sweet spot with legislation. And we are very supportive of what the Commerce Department is trying to accomplish. But what you get, I think, with legislation is greater certainty for businesses, and you tend to avoid the uneven playing field in which the best companies are willing to give very good privacy practices, but they feel like they are at a competitive disadvantage. So the answer is, yes, we are very supportive of moving forward on legislation.

Mr. BUTTERFIELD. Thank you.

Earlier this year, Google announced that it was consolidating most of its privacy policies for its various services into one plain English privacy policy. Google also made clear that it had long been sharing information across its services and had disclosed this and that it was now expanding the practice to include platform-wide cross-sharing of information obtain through its search and video services. Regardless of what Google did was right or wrong and regardless of how it told the public, there are some, including myself, who believe that the way in which Google openly and repeatedly told its customers its plan was the right way to do it.

For me, the key take away here seems to have been missed; that is that Google and any other company like it is mostly bound only by its own public promises to its customers. There is no baseline legal standard for what these companies can and cannot do. In this country, consumers' privacy rights are for the most part limited to what any one company chooses to grant its customers.

Chairman and Administrator, both the FTC and the administration are now calling for baseline legislation. Can you please speak to this in the 45 seconds we have?

Mr. LEIBOWITZ. Very quickly we are supportive of baseline legislation. It can clarify rules of the road going forward. We can bring actions ex post, after the fact, as we did against Google for what we believe to be a breach of its privacy promise to keep information private. They then made it public as part of their first attempt to start up a social network; that was Google Buzz. But yes, I think there are advantages to having clear rules of the road in advance. We can't mandate privacy policies, for example.

Mr. BUTTERFIELD. Thank you.

I yield back.

Mrs. BONO MACK. Thank you, Mr. Butterfield.

The chair recognizes Ms. Blackburn for 5 minutes.

Mrs. BLACKBURN. Thank you, Madam Chairman.

First, I would like to enter a statement from a Consumer Electronics Association for the record.

[The information follows:]

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

Hearing on "Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?"

Statement of the
Consumer Electronics Association (CEA)
March 29, 2011

Subcommittee Chairwoman Bono Mack, Vice Chair Blackburn, Ranking Member Butterfield and Members of the Subcommittee, on behalf of the Consumer Electronics Association (CEA), thank you for the opportunity to submit written testimony for today's hearing on the Administration's recently released white paper, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" ("Privacy Framework").

CEA is the preeminent trade association representing American innovators and entrepreneurs, both large and small, who are consumer technology companies. CEA's over 2,000 corporate members include manufacturers, internet providers and retailers. Our members design, produce and sell products and provide services that enable millions upon millions of consumers every day to access the often-times free wonders of the Internet.

CEA members believe that any policy proposals concerning privacy and electronic data collection should be based on a set of core principles as follows:

> The primary goal of any legislation or regulation concerning online privacy issues should be to enhance individuals' continued use of and trust in technology and technology products;
>
> Privacy legislation and regulations must be technology-neutral; that is, no one particular solution should be mandated nor should technology products be burdened with providing the sole resolution;

The definition of harm resulting from the use of consumer data collected electronically should be agreed to, including its standard of proof, before any overarching privacy legislation and/or regulations are adopted;

International agreements, such as the US-EU Safe Harbor framework, must be maintained so that U.S. companies have a streamlined means to comply with the EU's "adequacy" standard for privacy protection;

Innovations in technology and resulting consumer benefits made possible through electronic data collection should be protected and promoted. Efforts should be made to increase consumer knowledge about existing privacy protections, as well as the benefits to consumers made possible through electronic data collection; and

Self-regulatory approaches to privacy protection should be encouraged and embraced.

CEA agrees with the Adminstration's acknowledgment of the need to maintain consumers' trust in the technologies that drive the digital economy. But we note that the Privacy Framework is based upon the idea that consumer online trust or confidence is somehow lacking and that increased government protections, through perplexing state-enforced self-regulation and overarching and vague legislation, are critical to sustaining and augmenting this trust. Such a conclusion is contrary to evidence of ever-increasing Internet use by the America public. Every day, more consumers are operating CEA member companies' products and services to freely engage, share and make purchases online. Economic data about the booming digital economy clearly supports this finding.

CEA consistently calls for targeted government action if and when the data clearly indicates need for a public policy solution. We support established privacy laws and regulations in the identity theft, health care and child safety areas because of the evident harm to consumers if their information is misused or without their consent. But we find the evidence lacking regarding the alleged harm to consumers that the Administration now seeks to mitigate. Much text in the Privacy Framework is devoted to a description of the methods, be it through the multi-stakeholder process or proposed legislation, but a discussion of the assumed problem to be addressed is notably absent.

Before any solution is adopted, we must collectively first come to a definitive, clear and data-based conclusion and consensus about what issue, if any, we seek to solve. CEA takes the

position, as noted in our fifth privacy principle, that data collected electronically provides enormous consumer benefits and services. As such, we believe that any discussion of the supposed harm must also be measured alongside the advantages afforded by the rich and often-times free innovations available online.

CEA member companies deeply understand that respect for consumer privacy is an important and necessary business practice. Our member companies are committed to being responsible data custodians. They have and continue to develop, implement and enforce robust industry self-regulation and apply best business practices in a variety of areas related to consumer privacy. As CEA remarks in its final privacy principle, such self-regulatory approaches should be encouraged and embraced. We also must allow such approaches to be developed and implemented by companies that know their markets and their customers best.

CEA is heartened that the Privacy Framework specifically recommends that Congress avoid "prescribing technology-specific means of complying with the law's obligations," and it is our hope that the multi-stakeholder process embraces this charge as well. CEA also welcomes the framework's call for engaging with its international partners to increase interoperability across borders, which is also consistent with our principles.

CEA, on behalf of its over 2,000 member companies, appreciates the thoughtful and deliberate process that this subcommittee has taken over the course of the 112th Congress concerning the issue of privacy and electronic data collection. We stand ready to serve Congress and the Administration as a participant and resource on these important topics.

Thank you.

Mrs. BONO MACK. Without objection.

Mrs. BLACKBURN. Thank you.

Mr. Leibowitz, I want to talk with you about Commissioner Rosch's dissent from the FTC report. I am going to quote from that. He said, privacy may be used as a weapon by firms having monopoly or near monopoly power, and also large enterprises in highly concentrated industries may be tempted to raise the privacy bar so high that it will disadvantage rivals.

So my question to you is, are you concerned about the bigger players in this space using privacy to try to wedge out their competition?

Mr. LEIBOWITZ. Well, I have great respect for Commissioner Rosch. He agreed with some of our recommendations; for example, the legislation involving data brokers. He didn't agree with others. You know, on the antitrust side of what we do, we are always concerned about the larger players squeezing out new invasion, but our experience with self regulation—and again, our report best practices for companies; it is not regulatory, it is not—it doesn't impose obligations.

Mrs. BLACKBURN. Best practices, no rules, no force of law.

Mr. LEIBOWITZ. No rules, no, force of law. That is exactly right. And our experience with the advertising industry CARU, which has a self-regulatory mechanism that actually ensures in a lot of causes don't come to the FTC, has been that we haven't had that problem. But of course, we will keep an eye on it.

Mrs. BLACKBURN. All right.

Mr. Strickling, any comment on the that?

Mr. STRICKLING. Well, with respect to the—I am sorry, could you repeat the question?

Mrs. BLACKBURN. That is OK. Let's go ahead and move on because time is tight, and we are going to go have votes in a little bit.

Also Mr. Rosch said in his report, if implemented as written, many of the report's recommendations would instead apply to almost all firms and to most information collection practices. It would result—it would install Big Brother as the watchdog over these practices, not only in the online world but in the offline world. This is not only paternalistic, but it goes well beyond what Congress permitted the commission to do under Section 5(n).

Now the reason this is of concern to me and as we discuss privacy, in Tennessee, we not only have a lot of your entertainment platforms; we also have health care informatics, defense informatics. So we have your financial service sector that is very involved there. And we have got a lot of innovators that are trying to wedge into this space. So how do you respond to that portion of his critique?

Mr. LEIBOWITZ. I would say Commissioner Rosch is not only a brilliant litigator, but he has a very good turn of a phrase from time to time. But again, this is voluntary guidance; it is best practices for companies and really thoughts for lawmakers if you move forward with the privacy legislation. And so while I have great respect for him, I disagree; I don't think it is in any way going to undermine innovation. If it did, we wouldn't be releasing this report.

Mrs. BLACKBURN. Thank you.

Let me ask you one more thing in the minute that is left. Your opening, you referred to Do Not Track as a conservative proposition.

Mr. LEIBOWITZ. I do.

Mrs. BLACKBURN. I would take issue with you on that, and we will drink a cup of coffee and have a robust discussion one day. When you talk about Do Not Track, why don't you ever talk about it in terms of the Federal Government not tracking, instead of just telling businesses how to operate?

Mr. LEIBOWITZ. Because we don't support a Federal Government-run Do Not Track option. We support the private sector voluntarily coming together as they have, under the Digital Advertising Alliance, to come up with its own Do Not Track proposal and we think—they think it is the right thing to do I believe, you will have——

Mrs. BLACKBURN. In your opinion, then, how would the Do Not Track work? Would it be opt in for everything every time you log on to the computer?

Mr. LEIBOWITZ. That is a good question. So it would be opt out, so it is very modest in that sense, and it would only apply to third-party tracking. So when you have a direct interface with a company, Amazon, Netflicks, whatever, then there is a bargain—consumers understand they are going be tracked. When you go on a different—when you are on that site and someone else is trying to put a cookie in your computer, you would have the right to opt out. It is pretty modest, and our sense, based on some work that TRUSTe, which a privacy company based in San Francisco, has done is that the opt out numbers would actually be kind of small. But at least it is a choice and a right not to put property on your computer. And your computer is your property. So we will have that cup of coffee.

Mrs. BLACKBURN. Sounds like a winner.

I yield back.

Mrs. BONO MACK. Thank you.

The chair now recognizes Mr. Gonzalez for 5 minutes.

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

Welcome to the witnesses.

I guess I share some of the concerns of my colleagues but maybe not to the degree or the extent. I don't see that this Congress or any previous Congress has ever been paralyzed by changing technology. We don't worship at any particular altar of technology and sacrifice generally accepted principles that have been part of our law and which our citizens expect, and one is the right to privacy. We can adapt our laws as technologies changes. It seems we are just so fearful that somehow we can't because this technology is different; it is moving quickly.

Let me read to you something, this is way back December 12th, 2010, New York Times, an article by Natasha Singer. And she is citing from a Harvard Law Review: Solitude and privacy have become more essential to the individual, but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress.

The privacy experts wrote this in the Harvard Law Review, and I will give you the date in a minute, going on citing the article: In

this, as in other branches of commerce, supply creates demand, they added. And that demand, they noted, ends up broadcasting our private matters in public spheres.

Now the article was written by Samuel D. Warren and Louis D. Brandeis. It was in the Harvard Review in 1890, and it was referring to this viral technology of snapshot photography.

We have been able to adapt, haven't we? And we continue to do it. And the basis for it, and I want to see if you agree with this, it is the right to privacy. Do both of you agree? I have learned this from Mr. Dingell, but no one does it like Mr. Dingell. Just a yes or no. Do you agree that consumers have a protectable right as to who has access to their information and how it is used?

Mr. STRICKLING. We are asking you to enact those principles in——

Mr. GONZALEZ. Yes or no.

Mr. STRICKLING. Yes.

Mr. LEIBOWITZ. Yes.

Mr. GONZALEZ. And that that right is not contingent on any particular technology or the manner or the means in which it is accessed or which it is disseminated?

Mr. STRICKLING. Correct.

Mr. LEIBOWITZ. Correct.

Mr. GONZALEZ. Do you also agree that that individual citizen has a right to opt out of having access to his or her information and the dissemination of that information?

Mr. STRICKLING. Again, we are asking that that be a baseline, that it be enacted in the legislation we are recommending be passed to Congress.

Mr. GONZALEZ. Mr. Chairman.

Mr. LEIBOWITZ. Yes. And Justice Brandeis, as you know, was one of the architects of the Federal Trade Commission, along with President Wilson and President Roosevelt. And wrote about in Olmstead, the right to be let alone, which he called the most comprehensive of rights and the right most valued by civilized men in 1928.

Mr. GONZALEZ. I don't think anybody on either side of the aisle really wants to change that basic principle, because you may not have an outcry at this point, but I assure you it will be developing if in fact we don't adopt some sort of model out there for the behavior of the more responsible players in this particular technological sphere. So that is my concern. And that is going to be the voluntary nature of what you guys are proposing.

Now my understanding and my experience at this stage in my life has been that self regulation of any profession or business enterprise is contingent on basically mandatory enrollment, partnership in that particular endeavor. So I can see that we are going have this code, so everybody that adopts it, then may be enforceable through the FTC, even though it is not law, as you are saying, but you are saying we have authority to enforce. But then you probably have most of responsible players, and what do you do about everyone else that is not going to adopt this voluntary code and will not be subjected to any kind of enforcement procedure?

Mr. STRICKLING. Well, again, that is one of bases on which we are asking for legislation, because you are correct; the vast major-

ity of people who want to do the right thing will participate in these processes and adopt appropriate privacy policies, but then you have the question about the folks that don't do that. And our recommendation is pass the set of baseline principles, give the Federal Trade Commission the authority to enforce those against companies that don't adopt the codes of conduct so that you can deal with the very problem you are talking about.

Mr. GONZALEZ. Mr. Chairman, that is what you say you are playing out?

Mr. LEIBOWITZ. I agree with Mr. Strickling.

And I was talking yesterday to a very senior executive at a major technology company, and we were talking about the merits of Do Not Track. And he was saying to me, his company would like to do Do Not Collect, and that is where they want to be. In other words, which is what we say about Do Not Track; you shouldn't be able to collect information. It shouldn't just be do not advertise back to consumers, with a few exceptions for operational purposes and antifraud purposes. And he said one of the problems we have with this, John, is that we will be at a—we might be at a competitive disadvantage. What we want is an even playing field so that the best privacy protections are across the board. That is the argument for legislation.

Mr. GONZALEZ. Thank you.

Thank you, Madam Chair.

Mrs. BONO MACK. I thank the gentleman.

And the chair recognizes Mr. Olson for 5 minutes.

Mr. OLSON. I thank the chair and want to welcome the witnesses for coming here today. Thank you for your time and your expertise. And I apologize for all the bells and whistles that will happen pretty soon here. We have some votes coming up on the floor. Just so you guys know where I am coming from on these issues as a general position, I don't have a closed mind about anything, but I don't have an empty mind either. What I am very concerned about as a general rule, I am very skeptical about Federal Government interaction in a free market economy. I mean, we tend to have a one-size-fits-all mentality, and the private sector has an incentive that no government agency has; if they don't do what their consumers want, protect their customer's privacy, guess what, they are using some online service to get their resume up to date because they have lost their jobs.

And I just want to talk about, the private sector has made many tremendous advancements, and I want, Mr. Strickling, your thoughts on a couple of questions here. Do you think that the self-regulatory effort on the part of industry in developing new privacy tools is showing true signs of progress? So are they moving the ball down the field, so to speak? I ask this because I am familiar with the Ad Choices icon, and I am sure you are familiar with that as well. It is a project tool that gives consumers choices about online behavioral advertising. It was developed both very quickly and successfully—that the government can't do—with wide adoption by the industry. Now, this morning, a major Internet company, Yahoo, has announced that they will be implementing a global support for a Do Not Track mechanism that will recognize and implement a user's request to stop receiving Internet-based ads through a

browser-based signal. Say that 10 times quickly. It seems to me that these companies are on the right track, so I would like to hear your thoughts on that as well.

Mr. STRICKLING. Well, there is no question but that the self-regulatory efforts up until now have led to a certain level of protection for consumers for those companies that have participated in that and have adopted those approaches. But this problem isn't just a United States problem; it is a global issue. And our businesses want to do business in Europe; they want to do business in Asia. And what our overall framework helps enable is improved interoperability between what we have in this company versus the regimes in these other parts of the world, so that our businesses will have an opportunity to continue to expand and grow outside of the confines of the United States.

And there we see, particularly from Europe, they are looking to see how closely our regime fits with what they are doing. And there, for example, the—if Congress were able to enact these basic set of principles and legislation, that would very much help American businesses as they try to operate throughout Europe. It would help them in other parts of the world.

So our overall regime certainly would continue what has worked well up to now in terms of the self regulation from business but would allow us to take what is working here and serve as a beacon for countries in other parts of the world that are still deciding what sort of privacy regime they want to enact, as well as being interoperable with parts of the world, like Europe, that have very precise and detailed views about how they want companies to behave in this sphere.

Mr. OLSON. We are all concerned about opening up markets overseas to our companies. But again, we should do what is right for America. And if it is right for America, do what is right for America, and not worry about what Europe does, because again they are not a good business model, in my opinion, on many of these issues.

Secretary Leibowitz, can you give your comments on those questions I asked?

Mr. LEIBOWITZ. Yes. Although I don't think I deserve a promotion to Secretary, but thank you.

Mr. OLSON. It says "assistant secretary." I just chopped off the "assistant." In the military——

Mr. LEIBOWITZ. You are very indulgent and——

Mr. OLSON [continuing]. You don't call a rear admiral "Rear Admiral," you say, "Admiral," so "Secretary."

Mr. LEIBOWITZ. Going back to the Ad Choices Network, which I think is a marvelous example of self regulation moving forward. They served I think 2 months ago, 900 billion ads with the Ad Choices icon. I think they are up to a trillion in the last month I am told. So that is a great example of the Do Not Track notion moving forward in a self-regulatory way.

They have acknowledged that they have a little more work to do. They are going to be honoring what is known as the browser header, and the browser companies like Microsoft, and Mozilla, and Apple have really been out front in their support for Do Not Track. And they hope to have that finished by the end of the year. And I think that would be a great thing for Americans and for con-

sumers in terms of striking the right balance between innovation and privacy.

Mr. OLSON. One quick yes-or-no question because I am running out of time. But the President's privacy proposals calls for multi-stakeholder process to establish voluntary codes of conduct. If, at the end of this process, the companies choose not to adopt voluntary codes of conduct, what is your position? Do you have a plan B?

Mr. STRICKLING. Well, in the absence of legislation, that is the end of it. If legislation is passed, we are asking that the FTC be given the authority to enforce the basic seven principles that we have laid out, but that would only come if and when legislation is passed.

Mr. OLSON. Thank you.

Yield back.

Mrs. BONO MACK. I thank the gentleman.

And I am happy to welcome to our subcommittee, Mr. Sarbanes.

Welcome, we are happy to have you, and I recognize you for 5 minutes.

Mr. SARBANES. Thanks very much, Madam Chair, thank you all.

Chairman Leibowitz, you were talking a minute ago about someone you were talking with who said they would love to get to do not collect. Can you explain that a little bit more to me? And tell me why they would want to get to that?

Mr. LEIBOWITZ. Why we would like to see——

Mr. SARBANES. Why did that industry player say, I would like to get to do not collect? What is in his head?

Mr. LEIBOWITZ. Well, what he is thinking is this, he wants to do the right thing for consumers, his company. He knows also that as a general matter, the more private—the more consumers—the more privacy consumers have, the happier they have, the more trust they have in the Internet, and the more commerce they do on the Internet. You take a really good company that wants to do the right thing, and sometimes they have to compete against companies that don't have such a high privacy baseline or that actually are sort of bottom feeders. I mean, that is what we do with our enforcement side of the our agency, right, is we go after companies that violate and try to rip off consumers, basically. So what he is thinking and I believe what many companies are thinking is the right thing to do is to give consumers the ability to opt out of tracking, that is Do Not Track. And what he wants to know is that if he does that or if his company does that, that he will be among the many. I think we are moving towards a Do Not Track option for consumers that is easy to use; it is effective, and it is persistent.

Mr. SARBANES. Does the industry think that the public is actually not going to engage in as much sort of commerce or interaction online with their products and services if there isn't a Do Not Track opportunity or ultimately say do not collect, or they will be just in a better mood?

Mr. LEIBOWITZ. Well, I think study after study shows that consumers are very concerned about privacy and that the more trust they have in the Internet and in cyberspace, the more commerce—I don't have the surveys with me, but I will provide them to you after the hearing.

Mr. SARBANES. Anecdotally, we are all aware of that perspective. I think it is absolutely correct.

And I gather, also, what you are saying is industry by and large supports codifying the kind of principles that have been articulated here in both reports, right?

Mr. LEIBOWITZ. I can't speak for the Commerce Department, but I think that is right. I think, on Do Not Track, we have a sort of somewhat motley coalition, but everyone is pulling together to get to an endpoint. Maybe let me strike the word "motley." We have an interesting coalition.

Mr. SARBANES. They are all sitting behind you.

Mr. LEIBOWITZ. I know that.

Mr. SARBANES. Which one is the mot and which one is the ly?

Mr. LEIBOWITZ. I know and we have great respect for the people who are doing this. I think at the end of the day, by the end of year, I am optimistic that there will be no daylight, and we will have an effective Do Not Track option for consumers. And it will be done voluntarily by companies, which is very, very meaningful I think.

Mr. SARBANES. You say here—you don't say, but the standards that are articulated in the FTC's report you talk about, instead of setting forth a list now of commonly accepted practices for which companies do not need to provide consumers with choice, the idea is to say that as long as collection and use practices are consistent with the context of the interaction, but of course, that judgment is going to get made by the industry.

Mr. LEIBOWITZ. Sure.

Mr. SARBANES. So talk about the slope there, does that get slippery? And how do you sort of periodically go in and determine whether their idea of what the context of an interaction is, is the public's idea of the context of an interaction?

Mr. LEIBOWITZ. That is a great question. So the context of the interaction, you know, we put out our draft report in 2010. We got 453 comments, many of them very, very good. Most of them from business. So we sort of refined our thinking here. And context of the transaction means this—and again, these are all best practices. They are not rules. They are not regulations. But companies shouldn't have to give choice when the consumer understands that choice is necessary. So if you go to Amazon and order a book, and they are using someone to deliver that book other than Amazon or an online retailer, you expect that Amazon will give your information, your address, your name to the company that is doing the fulfillment and doing the delivery. So, in those circumstances, you shouldn't have to give consumers choice.

In other circumstances, we think the better approach is choice. And what do we do if companies don't engage in best practices? Well, if they don't engage in best practices, they are not liable under the FTC act. They are liable under the FTC act which prohibits unfair or deceptive acts or practices if they engage in unfair acts or practices. Again, these are, to some extent, aspirational for all companies; they are practices that the best companies engage in already. And then we go after the bad companies or the companies that sometimes are good companies but have engaged in unfair or deceptive practices by saying, you know, we are protecting

your privacy information but ultimately not doing that and making it somewhat public.

Mr. SARBANES. Thank you.

Mrs. BONO MACK. Thank you. And I would ask the witnesses to make sure you pull the microphones closer to your mouth. The people in the back row are having a hard time hearing you.

The chair now recognizes Mr. Kinzinger for 5 minutes.

Mr. KINZINGER. Thank you, Madam Chair.

Thank you, Secretary and Commissioner, for coming in to talk to us today. Very much appreciated. The committee has worked diligently over the past year to promote better consumer protections for consumers.

We want to maintain a marketplace of innovation and give consumers the tools to protect their personal information. I will be the first to say that the government needs to put an end to needless regulations that do little to protect consumers or protect jobs, but I do have some serious concerns that without privacy protections, consumers could lose confidence in the online free market. And in fact, that could be very counterproductive.

This committee has a very challenging task before it, how to provide regulation with the necessary flexibility to ensure government agencies don't stifle growth. I appreciate both of your efforts in this space and hope that your work is moving in the right direction.

Mr. Leibowitz, in your testimony you state that to the extent these best practices won't serve as a template for law enforcement or regulations under current law. What portion of the best practices do you believe falls under the current law or Section 5 authority of the FTC?

Mr. LEIBOWITZ. I don't think any. I would say best practices would never be in violation of the FTC Act. Even if you don't reach those best practices, you may still not be in violation of the FTC Act. It prohibits unfair or deceptive acts or practices. So we wanted to make it very clear that this isn't a regulatory document or an enforcement document. We go after companies when they engage in unfair or deceptive acts or practices, not when they don't meet the goals of the report.

Mr. KINZINGER. Understood. And do you believe the commission has the authority to enforce any privacy rules under Section 5?

Mr. LEIBOWITZ. We do. I mean, we have the authority to go after companies that engage in unfair or deceptive acts or practices. We just announced a case today involving a company that is very well known called RockYou. And RockYou is a popular social media gaming company. They failed to have—we believe they failed—we allege they failed to have adequate security measures. It resulted in personal information of more than 32 million consumers being captured by hackers; fortunately, not Social Security numbers, and fortunately, not credit card numbers. And we investigated them, and we put them under order this week.

Mr. KINZINGER. Excellent. This is for both of you, and you can keep it short because I know we have some things upcoming up here. Do you believe the lack of data security and notification legislation is a significant threat to consumers? And is it more of a threat than not passing a privacy framework in your opinion, sir?

Mr. STRICKLING. Well, they are both important. And certainly the administration supports the passage of data breach legislation to provide a national standard for the entire country.

Mr. LEIBOWITZ. I think they are both important, and data broker legislation—again, data broker—we support data security legislation. We worked with this committee on both sides of the aisle to try to make that go forward on data broker legislation. So data brokers are sort of third parties that collect information, monetize it, sell it. So there is some value to the economy for it. But there is also no interaction with consumers. We think that there should be limits on their ability to do that, sort of commensurate with the kind of information they are collecting and the use to which they are putting it. And actually, when we released the report, one of the senior executives at Acxiom, which is the largest data broker, acknowledged that it is not—quoting her from the New York Times, "It is not an unreasonable request to have more transparency among data brokers." And in fact, that is one of the areas where we had unanimity on the commission.

Mr. KINZINGER. Well, thank you. And again, thank you for your time.

Madam Chair, thank you for recognizing me. And I will go ahead and yield back.

Mrs. BONO MACK. All right.

And the chair now recognizes Mr. Waxman for 5 minutes.

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

Chairman Leibowitz, in your report from the FTC, you once again call on Congress to pass legislation to give consumers access to information about them held by data brokers. The FTC also calls on data brokers to create a Web site where they can identify themselves to consumers, tell consumers about their collection and use practices, and tell consumers about any rights and choices regarding information about them kept by data brokers. I appreciate the FTC has used its report to once again bring attention to offline data collection. Much of the discussion around privacy has focused on online data collection, pushing further into the dark a piece of the tracking industry that consumers know little to nothing about.

Yet I understand these two pieces, online and offline data collection, are beginning to converge so that the information from both sources gets mixed up into one super profile about a consumer. The FTC report also highlights something else interesting in connection with this. The report points out that following some scrutiny in the 1990s, some data brokers created a self-regulatory organization, but that group was subsequently terminated.

Then, in 2005, it was revealed that ChoicePoint, a large data broker, experienced a data breach, and these firms were once again in the spotlight. But as the report points out, there have been no meaningful broad-based efforts to implement self-regulation in this area in recent years.

Chairman Leibowitz, I would like you to address two things. First, what lessons can we draw from the failed efforts at self-regulation by data brokers? And second, can you please discuss why it is important that we pay attention to offline data collection and move legislation to grant consumers access rights to this information?

Mr. LEIBOWITZ. Well, let me take the second question first.

As you point out, there is a massive sort of collection of information by these companies. And they provide value. I don't want to say that the companies are inherently bad. And they combine online and offline. They monetize this information. They sell it, and consumers have no idea whether the information is—what information is being collected about them and where in cyberspace it is going.

So, even industry, I don't know if you heard my back and forth with Mr. Kinzinger, but even industry, some of the largest companies have acknowledged there is a need for more transparency here. So that is a good thing. And going back to your first point, I think the conclusion—a conclusion you might draw is that the notion of a centralized Web site is one that perhaps this industry may be willing to engage in. And we have called for you to explore it in legislation, and we are going to explore this issue going forward with the industry, because we want to work cooperatively with them.

Mr. WAXMAN. Administrator Strickling, do you have any thoughts to add about the self-regulatory experience with offline data brokers and the importance of improving access and transparency with respect to this part of the data collection industry?

Mr. STRICKLING. Well, in general, we see this as an area that could work with some improvement. And we do believe our multistakeholder process that we proposed would provide a good opportunity to do just that.

Mr. WAXMAN. Chairman Leibowitz, in your testimony, you discuss a final settlement the FTC entered into with Google late last year for a case in which the agency charged that Google deceived consumers in connection with how it rolled out Google Buzz. The FTC is also in the process of settling a case with Facebook in which you charge the company with several deceptive and unfair practices. The settlements are similar in that going forward, you require Google and Facebook to follow and implement a number of protective privacy practices.

However, neither of these companies has had to pay a penalty for what they did, not one penny. The fact that neither Google nor Facebook will have to pay a fine left some outside observers puzzled. So I would like you to discuss something else you bring up in your testimony, the need to grant the FTC civil penalty authority as part of any privacy bill that may come out of Congress. Is it correct that, as it stands now, even the FTC, had it wanted to, could not on its own seek civil penalties against Google, Facebook, or anyone else for unfair or deceptive privacy practices?

Mr. LEIBOWITZ. That is correct.

Mr. WAXMAN. And is it correct that you were not able to seek civil penalties from Google and Facebook because Congress has not granted you the authority to seek these penalties under these circumstances?

Mr. LEIBOWITZ. That is correct.

Mr. WAXMAN. And the FTC report calls on Congress, as part of any privacy bill, to provide the authority to seek civil penalties. Can you tell us why civil penalties should be seen as a key component of any privacy law?

Mr. LEIBOWITZ. Because I think it just makes much more effective deterrent. I think 46 attorneys general who have baby FTC Acts have this authority. You have to use it judiciously. And civil penalty authority for violations of the FTC Act, as you know, is unanimously supported by the commission, all four commissioners, Republicans and Democrats. And really the notion goes back to when Caspar Weinberger was the chairman of the FTC in the early 1970s, because he was a very big advocate for civil fining authority.

Mr. WAXMAN. Thank you, Madam Chair.

Mrs. BONO MACK. Thank you, Mr. Waxman.

It is my intention to roll through this one vote on the floor and have Vice Chair Blackburn take over momentarily.

But in the meantime, I am going to recognize Mr. Stearns for 5 minutes.

Mr. STEARNS. Thank you, Madam Chair.

Just to point out what Mr. Waxman said, wasn't it true with Google, you put in place a 20-year audit on them?

Mr. LEIBOWITZ. We did. Twenty years is our standard——

Mr. STEARNS. And in the possibility that they are in violation of that audit, then you could fine them, right?

Mr. LEIBOWITZ. Yes. If you are under order and you violate an order, then you are subject to fines. That is exactly right.

Mr. STEARNS. So you do have the ability to fine.

Mr. LEIBOWITZ. Yes, for the second violation.

Mr. STEARNS. Yes. OK. I just want to clarify that.

This question is a little self-serving. I have a bill dealing with privacy. It is H.R. 1528, the Consumer Privacy Protection Act of 2011. And in my opinion, this bill calls for a clear and easy-to-understand privacy policy statement, and provides the FTC to approve a 5-year self-regulatory program. I guess the question for Mr. Strickling and Mr. Leibowitz, Chairman, is would you support advancing this type of bill through Congress as an attempt for a Federal baseline?

Mr. STRICKLING. We have not yet taken a position as an administration on any particular piece of privacy legislation up here. But again, we absolutely support the enactment of a straightforward baseline set of privacy protections, subject to the multi-stakeholder process and codes of conduct which would then flesh them out. But in terms of what would go in legislation, yes, we support a very straightforward, simple piece of legislation to codify the basic principles.

Mr. STEARNS. If you can, just look it over. When I was chairman of this subcommittee for 6 years, I had seven hearings on privacy. And that was developed. And it was developed in consensus. We got it out of the subcommittee. Jan Schakowsky was the ranking member. So you might look at it.

Mr. LEIBOWITZ. We also have endorsed general privacy legislation, but nothing specifically. But we want to work with you, because I know you are trying to accomplish the same goals that I think we share.

Mr. STEARNS. Yes. And so when a person says Federal baseline, just give me one sentence, what does that mean to you?

Mr. LEIBOWITZ. A baseline?

Mr. STEARNS. Yes, Federal baseline.

Mr. LEIBOWITZ. On privacy?

Mr. STEARNS. Yes.

Mr. LEIBOWITZ. It means setting a standard that protects consumer privacy in a way that doesn't in any way undermine innovation.

Mr. STEARNS. And you, Mr. Strickling?

Mr. STRICKLING. Quite straightforward. I think it is taking our seven principles and putting them in a 10- to 15-page piece of legislation and enacting them.

Mr. STEARNS. I think some stakeholders have come out and made some positions known during this comment period that you are having here. How long is this comment period?

Mr. STRICKLING. It will close on Monday.

Mr. STEARNS. OK. Do you think that is long enough?

Mr. STRICKLING. I believe so. It has been open for nearly a month. Plus we, in our process to develop the blueprint, have had numerous conversations with industry and civil society groups for the last year and a half. So we feel we have a pretty good handle on where industry and the not-for-profits are at on these issues. But we still wanted to give them an opportunity to provide direct input on how we could craft the multi-stakeholder process that we are going to start later this spring.

Mr. STEARNS. How many comments have you gotten?

Mr. STRICKLING. Oh, we usually don't get them until the due date. So we extended the due date at the request of some commenters. I think we have gotten a handful so far.

Mr. STEARNS. You have got three or four comments is all you have got?

Mr. STRICKLING. I don't know the exact number, sir. But not a lot.

Mr. STEARNS. OK.

Mr. STRICKLING. I am told 15.

Mr. STEARNS. All right. That is what staff is for.

Mr. STRICKLING. Yes.

Mr. STEARNS. Would it make sense, as a first order of business, for the NTIA to formally acknowledge as acceptable those existing voluntary codes of conduct it has concluded are models of effective self-regulation?

Mr. STRICKLING. Well, we are not going to recognize any codes officially that come out of our process. So there is nothing about any work that has happened before now that is any way jeopardized or threatened by what we are going to put in place. It will build on the work that has already been done by industry and consumer groups up until now.

Mr. STEARNS. This is just a comment, Chairman Leibowitz. I think you said in an FTC privacy report that if a customer books a weekend vacation, they would be unlikely to be interested in continuing to see hotel advertisements after the trip is complete. What research or surveys did the FTC conduct to reach this conclusion, which seems to be a little subjective, depending upon who you are, because you might, after you get to your particular hotel, you might be interested in continuing seeing hotel advertisements and maybe make some calls if you want to extend your vacation?

Mr. LEIBOWITZ. You know, my anecdotal and personal opinion is that sometimes you do. And so I will go back and I will check on the research we have done in order to incorporate that, again, that prose. Again, what our report is about, and I know you have read through parts of it, is voluntary codes of conduct. So it doesn't impose any mandate on anyone, and it doesn't—if you don't delete—if a company doesn't delete those ads, of course, it is not an unfair or deceptive act or practice. It is a fair point.

Mr. STEARNS. So your research is anecdotal?

Mr. LEIBOWITZ. I will come back and I will research it with respect to central Florida.

Mr. STEARNS. All right.

Thank you, Madam Chair.

Mrs. BLACKBURN [presiding]. The gentleman yields back. I know we have Mr. Markey and Mr. Pompeo, who are en route.

And as they are returning, Mr. Leibowitz, I want to come back to you on this authority and the enforcement, what the FTC would do. It sounds like the White House and the Commerce Department feel like that we can get by more with self-regulation. So I want to know where there is a gap in authority when it comes to enforcing privacy violations. Tell me where you would see this.

You say, the FTC says it already possesses sufficient authority to enforce the privacy violations. And then you hear some things that Mr. Strickling says and some of the White House, and it looks as if they are looking more at self-regulation or would bend more to self-regulation. So, you know, tell me where you think there is a gap.

Mr. LEIBOWITZ. So this is a really good question. And we can go after unfair and deceptive acts or practices, and we do. That is our bread and butter. We are an enforcement agency. What we can't do—I mean, what we do as an enforcement agency, though, is we look back at violations; we don't look forward. So companies don't necessarily have the certainty that they want. And again, I was talking earlier today about a conversation I had with a very senior technology company executive who wants to do the right thing. But what he worries about, and it is a totally legitimate worry, is if I give the best privacy practices to customers, am I going to be at a competitive disadvantage? So the notion of privacy legislation and the codes of conduct that the Commerce Department and the White House are talking about is one that would give more certainty and create an even playing field. But again, you know, we——

Mrs. BLACKBURN. So if I were to define the differences between the way that you two gentlemen approach this, you would say, be more proscriptive; and you would say, depend more on the guidelines.

Mr. STRICKLING. Well, it is a four-part program. First is the baseline legislation, which could be directly enforceable by the Federal Trade Commission against those rogue companies that choose not to adopt any protections for their customers. But you are right, we then would have the detailed practices and processes developed through these voluntary codes involving industry and other stakeholders. We do think that those codes, if adopted voluntarily by a

company, would then be enforceable by the Federal Trade Commission just as they enforce those sorts of policies today.

Mr. LEIBOWITZ. So I wouldn't call our—I would say our efforts are complementary. Theirs looks a little bit more at sort of procedural aspects, how do you get companies in a room to come up with guidance. We look at sort of aspirational—best practices for companies today, and sort of aspirational practices for the companies that don't have the best privacy policies. And I think they are very, very complementary. But I don't think anything that we have talked about is proscriptive. Really we have sort of two functions, neither proscriptive. One is a policy function that goes back to when the agency was created in 1914, and the other is enforcement for violators. A lot of companies—so we go after the bottom feeders or the good companies that, you know, make a mistake once, hopefully only once. And then we try to encourage companies—again, we had a multi-stakeholder process as well. They only had 15 comments; we had 450—more than 450 comments. Most of them from companies. We held multiple workshops. And so this is a sort of a guide for really best practices. It is not proscriptive.

Mrs. BLACKBURN. Thank you.

At this time, I will recognize Dr. Cassidy for 5 minutes.

Mr. CASSIDY. Hello, gentlemen. Thank you for working on this. We have had several hearings on this. I met privately with some folks. And you guys have really worked hard at this. And it seems like we are coming to something that we can be comfortable with. So if you will, I want to move to something that we are not comfortable with, which frankly I don't know answers to, but because you are experts I explore with you.

We are all familiar with the tragedy of the gentleman Trayvon Martin who was shot in Florida. And some of us are familiar with the fact that Spike Lee retweeted the address of someone named George Zimmerman, not the George Zimmerman, but another. Now, this is counter to Twitter's stated user rules, but apparently, it took them 3 days to take that down so I have been told. And in the meantime, we have seen terrible tweets, until finally someone named Megan says anyone who retweets this is guilty of the same crime. Now, she was a sensible person.

Now, I am exploring this with you because this is privacy, but it is not technically consumer privacy on the other hand, and there was a policy on Twitter, but you see where I am going with this. And so to explore, I ask you your opinions. Aside from the fact that Spike Lee should not have done it, and it is reprehensible. I will say that.

Mr. LEIBOWITZ. So Spike Lee is a great filmmaker, but, you know, it is a bad practice, right? And the right to privacy is a very complicated right, but it is a bedrock right, you know, in our Constitution from government. And it is a critically important right for consumers with respect to sort of information that is aggregated. You know, but at bottom line, I would say people have to exercise good judgment. Right?

And one of the reasons why we focus a lot on children's privacy is because children and teens are incredibly lucid with technologies, but they act very impulsively, and they don't always exercise good judgment.

So it is, you know, it is a great example that you raise. There are no easy answers to it. I don't know that it is a violation of anything but good judgment and common sense.

Mr. CASSIDY. Now, I understand that there is the you cannot yell "fire" in the crowded movie theater kind of test as a limit of free speech. And Spike has 250,000 followers. And the elderly couple, the elderly couple, who is law-abiding, has had to move into a hotel because of death threats. And again, I am not doing anything but kind of posing the question, at what point does it come to the standing of yelling "fire" in a crowded theater?

Mr. LEIBOWITZ. Well, I don't know the answer to that because it is not subject to an easy—it is not subject to an easy answer. Obviously, we only have jurisdiction over commercial privacy issues. But I think it is important for people like you. And I was reading the transcript from the last hearing, and I saw your questions. I think it is important for people like you who care about privacy, and also care about justice to sort of speak out when you can.

Mr. CASSIDY. OK. So, at this point, it is still moral suasion, but it isn't necessarily anything that even though Twitter didn't take it down for 3 days, that there is anything you would consider would be appropriate in a regulatory realm?

Mr. LEIBOWITZ. You know, we will go back and think about that. I don't know what the circumstances are. I don't see it as an unfair or deceptive act or practice. Perhaps they should have taken it down sooner. But by the way, once someone puts a tweet up with 250,000 followers, you know, it is immediately retweeted and retweeted again. And Twitter, by the way, who we have under order for a data security breach, you know, Twitter has provided enormous value to consumers. And you know, you don't want to use the heavy hand of government I think when these companies are providing value and being innovative. But I hear your point.

Mr. CASSIDY. That is fair. Thank you.

And again, I was not challenging; I was trying to broach.

Next regarding children, as I read your testimony everybody understands children are a special case. But I keep on thinking that my savvy little 10-year-old is going to put down she is 19 when she wants to get on a Web site that she knows Daddy may not approve of. So unless I walk by and bust here, she is going to be someplace she wouldn't. Knowing you have thought about that, how do we address that?

Mr. LEIBOWITZ. Well, you know, you have tasked us, you the Congress, with enforcing the Children's Online Privacy Protection Act, which applies to sites targeted at 12 and under, and also applies to companies when they know that there is an underage user. You don't always know that, of course. What we have done in our proposal for updating COPPA, because the technology is massive—we actually accelerated as part of our regulatory reform efforts our COPPA update because the technology has changed massively in the last 10 years since COPPA was enacted—12 years since COPPA was enacted—is in proposal, we are taking comments, is to try to make it more difficult for the smartest children or the most tech-savvy children to elide around the COPPA protections. So that is something we are looking at. Happy to give you an offline briefing on what we are doing.

Mr. CASSIDY. Sounds good. Thank you.

I yield back.

Mrs. BLACKBURN. The gentleman's time has expired.

At this time, I recognize Mr. Butterfield in round two.

Mr. BUTTERFIELD. Thank you.

Chairman Leibowitz, in your testimony, you state that the World Wide Web Consortium, the Internet standards group known as W3C, is working with a broad range of stakeholders to create an international industry-wide standard for Do Not Track.

Overall, you seem to have a positive view about this process and the progress being made there. Can you please discuss the efforts of W3C so far and what its work can mean for consumers who want not only to not to be targeted, but who also want not to be tracked online?

Mr. LEIBOWITZ. All right. So there are sort of three different streams that are coming together. One is the Digital Advertising Alliance that is working on its Do Not Track option. And it serves close to a trillion ads every month—trillion ads or the ad choices opt out.

Another is the sort of browser vendors, the big browser companies, like Microsoft, Mozilla, and Apple, who have wholeheartedly endorsed the notion of Do Not Track. And the DAA is in the process of implementing the browser header approach, that if a browser says "Do Not Track me" or "do not collect my information," they will not do that.

And the third is the Worldwide Web Consortium, W3C, which is working on setting a standard. All of these streams are heading in the same direction. We believe, and I am optimistic, that they will come together by the end of the year in a persistent, effective, easy-to-use Do Not Track option for consumers.

Mr. BUTTERFIELD. In your testimony, you also state that some issues remain, and the commission encourages all of the stakeholders to work within the group to resolve these issues. Can you tell me what some of those issues are and why it is important?

Mr. LEIBOWITZ. Well, I think that within—well, I will let others, and there will be someone on the next panel speak for the Digital Advertising Alliance. I think many members of the Digital Advertising Alliance want to have robust Do Not Collect, with exceptions for antifraud efforts and network management. I think some others would like it to be Do Not Advertise back. I am comfortable—I am not only comfortable, I am enthusiastic that in a world where we haven't seen a lot of voluntary self-regulation, and really this is almost a code of conduct of the type that——

Mr. BUTTERFIELD. Mr. Strickling, you want to jump in here?

Mr. LEIBOWITZ [continuing]. That we are moving forward, and we are going to have it done.

Mr. STRICKLING. I am not directly familiar with the remaining issues in these discussions except that we are very supportive of the processes that are underway in all of the cases the chairman described.

Mr. BUTTERFIELD. The administration highlights two concepts as key to the multi-stakeholder processes for the development of self-regulatory industry codes of conduct. They are, as you know, openness and transparency. Openness means that a broad group of

stakeholders, including consumer groups and privacy advocates, have the opportunity to participate. Transparency means that it will be apparent to stakeholders in the public how decisions coming out of the multi-stakeholder process were reached. Some witnesses on the second panel today question the value of these two concepts to the codes of conduct development process. In particular, they suggest that some aspects of these negotiations should be private.

Mr. Strickling, can you please explain why both open participation and transparency are important?

Mr. STRICKLING. Well, we think it is quite important that the results of this process have credibility, both with the companies and the consumer groups that participate in it, but also with the consumers that are going to benefit from that. And we don't think there is any substitute for openness and transparency in terms of being able to establish that sort of credibility. But again, these are voluntary discussions. The discussions that we convene will have the hallmarks of openness and transparency. There is nothing about our process that in any way would prevent or deter parties from talking amongst themselves outside of our room. So those sorts of discussions may well take place in the interstices between our sessions. But the sessions we conduct will be open and transparent.

Mr. LEIBOWITZ. And we are very supportive of the Commerce Department's open and transparent approach.

Mr. BUTTERFIELD. All right. Thank you.

I yield back.

Mrs. BONO MACK [presiding]. The chair recognizes Mr. Barton for 5 minutes.

Mr. BARTON. Thank you, Madam Chairwoman.

I apologize for being tardy. I live 7 miles from the Capitol, and it took me almost an hour to get here today. I used every trick I could. The point remains to get into Washington from Virginia, you have got to cross the Potomac. And that means you have got to go across a bridge, and they were all clogged.

In any event, I want to welcome our two administration witnesses today. I especially want to commend the Federal Trade Commission. You all have been doing excellent work on privacy. I also think the recently issued Consumer Bill of Rights, Consumer Protection Bill of Rights, Privacy Bill of Rights is excellent. I think that is great.

My question to the FTC commissioner would be, does the bill that Mr. Markey and I have introduced, the Children's Do Not Track Act of 2011, is that congruent and consistent with what the FTC has been attempting to do from a legislative standpoint?

Mr. LEIBOWITZ. Yes. I think it is very, very consistent. And we are very supportive of what you are trying to accomplish. As you know, children, teens are very technology savvy, and they are also prone to act impulsively and recklessly. So some of the notions in your—what is in your legislation I think is very important. One of the areas that we explored in our report is the notion of the right to be forgotten. I think particularly for children and for teens, there is a real value in doing that. And in our order involving—you noticed it, I am sure—but in our order involving Facebook, we included a provision that allows consumers or users, if they are leav-

ing Facebook, to report their information back. So it is a sort of notion of the right to be forgotten. We think it is very important. And we want to work with you on your legislation going forward.

And the other thing I would say is of course, as you know, in our COPPA rulemaking, one of the few areas we do rulemaking in is Children's Online Privacy Protection Act, it is very consistent with some of the provisions in your legislation.

Mr. BARTON. Thank you, sir.

I want to ask Mr. Strickling, the Consumer Privacy Bill of Rights, as I understand it, is not in legislative language. Is it the administration's intention to present it in legislative language and ask the Congress to act on it at any time in the near future?

Mr. STRICKLING. Our goal is to work with this committee and to work with the Senate to come up with legislation. If it would help advance the process for the administration to propose specific language, we will certainly consider that. But I think our goal here is to work the best way we can in a bipartisan way to come up with legislation working with both Houses.

Mr. BARTON. I am going to yield back, Madam Chairwoman. I want to thank you for your focus on privacy and the hearings that you have held.

I also want to commend my friend Mr. Markey. I have lost a bet this week. We decided to get new cosponsors for our children's online protection privacy bill, Do Not Track bill. I think I have two. And I think he has around a dozen. So, for this week, but this week alone, Mr. Markey, the trophy goes to you. I know my Republicans are going to rally to the flag, and we will catch up. Good job on the cosponsors this week.

With that, Madam Chairwoman, I yield back.

Mrs. BONO MACK. All right. The gentleman yields back.

And the chair recognizes Mr. Gonzalez for 5 minutes.

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

At this time, I would like to yield to my colleague, Mr. Markey.

Mr. MARKEY. I thank the gentleman so much.

For kids, the Internet is oxygen. They can't live without it. So what Mr. Barton and I have done is introduce a bill to protect kids 15 and under. Each kid who lobbies successfully, they are 12 to 13, they are 14, to get their iPad, to get their Kindle fire, they are now off into places that their bicycle can't take them. And so the question is, are we going to protect those kids? Now, we should also debate what we are going to do for 24-year-olds, and 34, and 54, and 74. But do we really have to debate what we are going to do for 15 and under? Do we really have to debate that?

So let me ask you this, because I will give you the core of our bill. And I will ask the two of you—first of all, thank you, Mr. Leibowitz, for all your great work, and Mr. Strickling.

Our bill requires consent from parents before companies collect information about children; ensures that kids and teens 15 and younger have an eraser button to delete their personal information online; and it prohibits targeted advertising to kids and teens 15 and under. So this would not be big government; this would be big mother and big father able to police what is going on with their kids as they are going online. And we are only talking about children here. That is it. No more, no less than that.

And overwhelmingly, these numbers, the numbers on this go over 90 percent in polling. There should be a law that protects children. OK? There can be a debate perhaps over adults. But on kids, you know, they have a right to be forgotten. What they put online when they are kids, it shouldn't come back to haunt them in their college application. They have a right to develop. Kids have a right to develop. Kids have a right to make mistakes. And they have the right to be forgotten so that they can flourish into adulthood and not have this material they put online when they were 13, 14, 15 haunting them for the rest of their lives. Can we all agree upon that?

You agree with that, Mr. Strickling, that there should be a law that gives parents the rights to be able to erase this information?

Mr. STRICKLING. We absolutely support the idea that we need special protections for kids. That is laid out in our Consumer Bill of Rights.

Mr. MARKEY. Would you support a separate piece of legislation just to give that higher level of protection to children?

Mr. STRICKLING. We absolutely would be willing to work with you to develop that legislation.

Mr. MARKEY. And do you agree that children are entitled to a higher degree of protection?

Mr. STRICKLING. Our Consumer Bill of Rights recognizes that. And indeed, we could see moving forward fairly quickly, under our framework, to develop codes of conduct with respect to the very specific issues you have laid out.

Mr. MARKEY. You are saying legally enforceable. You are saying legally enforceable rights that parents could take the companies to court.

Mr. STRICKLING. Under our framework, once the companies adopt those policies——

Mr. MARKEY. No, but even if they don't adopt them. Let's say there is an outlier, a pirate company exploiting children; would you give the right to parents to go against a pirate company that is exploiting a 13-year-old girl who went online just trying to find information about her weight, and now she is being bombarded with 100 companies who are pirate ships? Would you give the parents a right to go against those companies?

Mr. STRICKLING. Again, the basic principles——

Mr. MARKEY. No, would you give the right——

Mr. STRICKLING [continuing]. Absolutely are important, and need to be supported. And again, we have not taken an administration position on this. But we will work with you on it.

Mr. MARKEY. Would you give them the legal right to go against the pirate ship coming against a kid, trying to exploit her anxiety about her weight, and now she is being bombarded by hundreds of companies with weight loss information?

Mr. STRICKLING. It is well worth being considered.

Mr. MARKEY. Well, I think you should not just consider it. I think you should support it, Mr. Strickling. I think that should be illegal if the parents want to block that company. I just think you are wrong on that. I don't think just consider it; I think it has to be the law.

What do you think Mr. Leibowitz? Should there be a law?

Mr. LEIBOWITZ. Well, as you know, our proposal for our COPPA update involves the notion of you need parental consent before you track children. So it would put sort of—it would really put much of your legislation, that Do Not Track kids, into place. Now, we are still taking comments. We haven't decided what we are going to do. But we are very supportive of the notion.

And I just want to make a couple of just other observations, and I will turn it back to you. So one is one of the great things about your legislation, and it is a reminder, is that privacy is a totally bipartisan issue. And that goes back to COPPA, when you and Mr. Barton and Senator Hollings and Senator McCain were very involved in implementing it. It is a fundamentally conservative notion in a certain sense. And it is one that is very important.

And as you look at this committee, or this subcommittee, I think everyone cares about it. You come at it from slightly different perspectives sometimes, but it is very much a bipartisan notion. And the notion of children as vulnerable is one that you have already made that determination.

Mr. MARKEY. I do not believe that it is morally appropriate for us to not put protections on the books, legally enforceable protections for kids 15 and under. YouTube should not become YouTrack. We should not have profiles of children being made by adults and companies trying to exploit their vulnerability. They have a right to be—they have a right to develop. And if there is nothing we can't agree on, on privacy in general, and I can see where that could happen this year, let's not have a debate over kids and making it enforceable. They are a special category. And I just hope the administration will zero in on this and make sure that we provide those extra protections. I thank the gentlelady.

Mrs. BONO MACK. Thank the gentleman.

And the chair recognizes herself for 5 minutes.

And I yield to Dr. Cassidy for questions.

Mr. CASSIDY. Thank you.

Mr. Leibowitz, you had said you had read the previous questioning. So I just thought I would follow up on a couple things that I previously brought up. A voluntary kind of, OK, we are going to address privacy is fantastic. And again, I am just so impressed with how you all have worked through many of these issues. But I am struck that there is little ways that obstruct me, when I am on the Internet, from protecting my privacy. So, once I was on an Apple site, and I actually clicked "read here" before you check to make sure, and it was literally pages of often repetitious, irrelevant material that I had to dig through to find that which was important about my privacy. And you begin to wonder if it is not tucked away in this thick forest of obfuscation solely because I get discouraged and say what the heck, let me hit the button, number one.

Number two, I think it was YouPlus on Google, or some function on Google where I said, let me explore. I go over there, and I almost had to reboot my computer to get that screen down. Now, I just tried to log on to see if that was still the case, and I couldn't get back to where I was. They probably know I am in here. But that said, it was just remarkable how easy it would have been for me to agree to turn over my personal data and how I could not hit

a back button to get off that screen. I had to close the browser and reopen to get to my Gmail account.

So, that said, there are subtle or not so subtle ways in which we are herded into confessing our personal information, if you will. Your thoughts on that? And I asked that before, so since, again, you all are giving great testimony, I thought I would bring it up again.

Mr. LEIBOWITZ. So on the privacy policy length and the inability to read it, according to TRUSTe, which is sort of a technology-based research company in San Francisco, Declaration of Independence, about 1,300 words; I Had a Dream speech, about 1,600 words; and average privacy policy, over 2,000 words. I asked my staff to look at privacy policies on mobile, and I did say, find me the worst one. And they found a mobile privacy policy that was 102 clicks. So you certainly shouldn't read it while you are driving, but no one is going to read it at all, except for my staffer, who had to.

Part of the reason why we support Do Not Track, again, which is voluntary, and which I think companies are moving very close to implementing, is because it gives you the right to opt out of having someone collect your information; only for third parties, not for first parties. When you are on someone's Web site, they should be able to track you. You sort of understand that around the Web site. But people who are dropping cookies in your computer, which is your property, they should give you the right to opt out.

Mr. CASSIDY. So if I log on Apple iTunes, and I click, yes, you can track me, if you will, that is only for Apple iTunes; it would not be on Safari tracing me all across the Web?

Mr. LEIBOWITZ. Yes, that would be—under our voluntary proposal, you would be able to opt out. I would say this. When you talked about the difficulty you had of getting out of a particular site, when we were—when I first came to the commission, shortly after, we were very involved in nuisance adware cases. So spyware that is in your computer. You can't pull it out. It is the software you can't get out, because they want to hide, and it serves up ads. So maybe it serves 20 ads to you a day. But, you know, in the aggregate, one company admitted putting cookies in I think 100 million consumers' computers. You know, in the aggregate, an enormous amount of harm, right?

And so those cases, like the one you talked about, and maybe we will have an offline conversation if you know the company, those begin to get into an area of unfairness where we might be able to go after them. It sort of depends—you have to see the context of it. But when you are making it difficult for someone to just get off of a screen, and if they are sucking up information that you don't want them to, that may very well be an unfair or perhaps a deceptive act or practice under the FTC Act.

Mr. CASSIDY. OK. To an extent, it may be caveat emptor; and to an extent, it may be, yes, they are doing something deceptive.

Mr. LEIBOWITZ. Yes, I think that is right. And just going back to the reason we support privacy legislation, again, going back to Chairman Bono Mack's point that you have to hit the sweet spot—I know you are not endorsing the legislation, but I thought that was something that is important to note—is we can't require privacy policies in advance by companies. So one of the things that

the Commerce Department's voluntary codes of conduct might be able to come up with is standardized privacy policies that are short and readable and the companies will adopt. And that is a good thing. And that is something you could require, for example, in legislation.

Mr. CASSIDY. Or even an abstract of two sentences placed above that which the attorneys want you to include.

Mr. LEIBOWITZ. Yes. Because—yes. And you know, look. What we want, and again, this is a document about best practices for the most part, what we want is best practices with respect to consumers and protecting their information. But look, it is better to have a notice in two sentences that says, if you come on our site, we are going to take all the information we can and do many things with it, than not understanding that at all. And I think if you understand, you know, the value proposition, if consumers have real privacy protections, and surveys have shown this, they will engage—they will have more trust in the Internet. They will engage in more commerce, and it is a virtuous cycle. But again, there are best practices, and many companies engage in best practices, but not all companies do.

And so part of the reason why we support legislation is because self-regulation has been—or is because self-regulation has been erratic. And we all know that from the number of breaches that we read about, for example.

Mr. CASSIDY. OK. I yield back.

Thank you.

Mrs. BONO MACK. Thank you, Dr. Cassidy.

The chair recognizes Mr. Harper for 5 minutes.

Mr. HARPER. Thank you, Madam Chair. Thank you for holding this hearing.

Gentlemen, I thank you for being here. I know you were looking for something fun to do today, and we are glad to have you here with us.

Mr. LEIBOWITZ. Always delighted to be here.

Mr. HARPER. There you go.

I will start with Mr. Strickling, if I can. Before the stakeholders can address what should be permitted and what should be out of bounds for purposes of consumer information practices, they will have to define harm. Outside of a data breach, how do you personally, or as head of NTIA, define harm in this context? I think that is really a critical deal for us is, how do you truly define harm? So how do you define it personally or within these confines?

Mr. STRICKLING. Right. Let me state, though, at the outset that developing these codes of conduct are not going to require the parties to define harm, because there are many goals in place here, one of which, which is fundamental to our work and is, I believe, fundamental to this committee's work, has been to promote innovation on the Internet. We do believe the development of these codes of conduct will help promote innovation on the Internet by allowing companies to retain the flexibility they need to have to try new business practices. But within that, as we think about harm, it is harm to consumers, as we have already discussed, but it is this larger question of, how do we continue to grow and expand the Internet economy? How do we protect and promote innovation?

It would be a harm to our economy, it would be a harm to American business if something were to happen that the Internet stopped being the tool of economic growth it has become. And to that, we link this concept of trust. What has allowed the Internet to grow has been in large part the trust that all of the actors have, that their information and that their transactions are protected on the Internet. So, in the development of these codes of conduct, to the extent we can continue to grow that trust, we then think that helps promote innovation, promotes new businesses. And that is very much a goal of what we are trying to accomplish here.

Mr. HARPER. Do you see users of the Internet having a changing view of the expectations of privacy?

Mr. STRICKLING. Absolutely. And what we want to preserve is both the flexibility that comes from technological change as well as the flexibility that emerges as consumer expectations change. That is why we are most emphatically not proposing a regulatory solution here. We are proposing these basic principles, which are very, very similar to the same principles that were first enunciated over 30 years ago, nearly 40 years ago, in these fair information practice principles. That is what we want to see enshrined in legislation.

And to Congressman Gonzalez's point earlier today, these are principles that are not going to change that much over time. How you implement them, the processes that are used, those will definitely change as a result of technology. And that is the flexibility we want to preserve. Because these codes, once they are developed, can certainly come back and be reexamined and changed to deal with changing circumstances in the market.

Mr. HARPER. Are you anticipating perhaps for users of the Internet to receive future warnings as to expectations of privacy? Are you anticipating any type of warning system or change in those warnings?

Mr. STRICKLING. Well, it is in our basic baseline that consumers ought to be informed of those sorts of changes. But again, how that would be done, that we want to leave to the private sector to determine through these discussions.

Mr. HARPER. Mr. Leibowitz, for years, I know FTC has prosecuted under its Section 5 authority only when there was a tangible harm unless the action involved deception. In fact, the FTC specified this practice in previous statements to Congress. The essential question I think in the broader privacy debate is, what is the harm to consumers that we are trying to address with these proposals?

Mr. LEIBOWITZ. So that is a great question. And I would say this. A couple points. So it is easy to define harm. We brought dozens of cases in the last 3 years, since the recession, involving foreclosure rescue scams and debt consolidation scams where companies would say on the radio, or call up and say, if you give us $5,000, we will get your mortgage and arrears back in shape. And they take the money, and they do nothing. So we all understand that is tangible harm.

But now go back to Mr. Cassidy's question, which is, you know, involves things like pop-up ads or nuisance adware. All right, I would say that is harm as well. Now, it may not be much harm to an individual, but in the aggregate, it is harm. So part of the

reason that we wrote—part of the reason that we wrote this report, which is about best practices, is because with privacy, we have tried the harm-based model, we have tried the notice and choice-based model. Now we know privacy policies don't really give people as much notice because they are incredibly long and difficult to read as we would like. So both of those models are ones that we used for prosecution.

But we also thought that with respect to privacy, where these issues are, as you know, pretty thorny and pretty difficult, it is best to engage, it is best to have best practices. I think this also goes back to the Commerce Department's notion of voluntary codes of conduct, where companies will decide what works best.

Mr. HARPER. OK. Thank you.

I yield back.

Mrs. BONO MACK. Thank the gentleman.

And I would like to thank our panelists for being here today. I look forward to our continued work together to do all we can to protect the online privacy of American consumers. Again, thank you for your time. You have been very generous. At this point, we are going to take a very brief recess as we seat the second panel. So thank you again.

Mr. LEIBOWITZ. Thank you, Madam Chair.

Mrs. BONO MACK. Hopefully, we can do this change in 1 minute or less for the second panel.

[recess.]

Mrs. BONO MACK. All right. We are going to continue with our second panel. So joining us today are Berin Szoka, president of TechFreedom; Pam Horan, president of Online Publishers Association; Jonathan Zuck, president, Association for Competitive Technology; Mike Zaneis, senior vice president and general counsel for the Interactive Advertising Bureau; and Justin Brookman, director of consumer privacy, Center for Democracy and Technology.

Good morning to our distinguished panel. Thank you all for coming. You will each be recognized for 5 minutes. To keep track of the time, please note when your light turns yellow, you will have 1 minute left. Again, we ask that you pull your microphones close to your mouths so everybody can in fact hear you.

And at this point in time, Mr. Szoka, welcome, you are recognized for 5 minutes.

STATEMENTS OF BERIN SZOKA, PRESIDENT, TECHFREEDOM; JONATHAN ZUCK, PRESIDENT, ASSOCIATION FOR COMPETITIVE TECHNOLOGY; PAM HORAN, PRESIDENT, ONLINE PUBLISHERS ASSOCIATION; MICHAEL ZANEIS, SENIOR VICE PRESIDENT AND GENERAL COUNSEL, INTERACTIVE ADVERTISING BUREAU; AND JUSTIN BROOKMAN, DIRECTOR, CONSUMER PRIVACY, CENTER FOR DEMOCRACY & TECHNOLOGY

STATEMENT OF BERIN SZOKA

Mr. SZOKA. Thank you, Chairman Bono Mack, Ranking Member Butterfield.

Let's try again. Chairman Bono Mack, Ranking Member Butterfield, Vice Chairman Blackburn, members of the sub-

committee, thank you for the opportunity to testify at this important hearing.

I commend you, in particular, for emphasizing the word "balance" in the title of today's hearing. As valuable as privacy can be, its value is not absolute. Privacy advocates and policymakers alike all too often overstate the value of privacy and understate its costs. We should approach privacy like any form of consumer protection, weigh harms against benefits, and empower consumers to make the right choices for themselves wherever possible.

The White House report gets the most important question right: Government lacks the flexibility, speed, and decentralization necessary to address Internet policy challenges. However laudable the report's principles, what matters is pragmatically transposing them into concrete rules that recognize real world trade-offs with innovation, convenience, and other competing values. Only a multi-stakeholder self-regulatory process can do this effectively.

But to avoid failure by design, that process must be voluntary, as the White House promises. Consumer advocates can play a vital role in offering constructive specific contributions in public fora. They can use public pressure to promote compromise within industry. But as with the DAA process itself, the difficult work of forging consensus must ultimately take place in private, and it must be industry that ultimately votes. There is much more to be praised in the White House report and the FTC report. But the White House's overall approach is both, well, unfair and deceptive.

First, while the White House report reminds us of the Fourth Amendment's essential protection against unlawful intrusion, it neglects to mention that the Fourth Amendment protects us against such intrusion by government. By using the term Consumer Bill of Rights just 2 months after a unanimous Supreme Court denounced excessive government surveillance in its Jones decision, this seems to me to be a constitutional sleight of hand, while the real Bill of Rights remains in peril.

Second, while the Fair Information Practice Principles play a useful role in conceptualizing consumer privacy protection, they are not enough. As law professor Fred Cate argues, the FIPPs have ultimately failed to serve consumers. Data protection laws should instead regulate data flows only when necessary to protect individuals from harm, while maximizing the flow of data. This is precisely why it is so important that both reports support proper re-identification of data as a way of balancing reasonable risks with the benefits of data-driven research and serendipitous innovation like Google's flu trends.

To quote Professor Cate, "Data protection is not an end in itself, but rather a tool for enhancing individual and societal welfare."

Indeed, as the FTC itself declared in its 1980 policy statement on unfairness, unjustified consumer injury is the primary focus of the FTC Act. The question policymakers should be asking is, what harms should the law remedy? Where the FTC's authority has proven inadequate, Congress has passed laws to remedy clear harms, such as the Fair Credit Reporting Act.

But before legislating further, Congress should ask whether the FTC can adequately address substantial harms through its unfairness and deception authority. The FTC must walk an exceedingly

fine line on unfairness. If used too seldom and if defined too narrowly, unfairness will fail to protect consumers from real harm, suggesting legislation is needed when in fact it is not. But if defined too broadly, unfairness will again make the FTC the national nanny, as the Washington Post dubbed the agency in the 1970s. Only this time the FTC will be micromanaging not children's advertising and funeral parlors but the very tools by which we communicate with each other. At worst, the Unfairness Doctrine would likely have banned the camera, that great invader of privacy, back in 1890. But at best, unfairness could supplement self-regulation if the FTC becomes more rigorous in its analysis.

Even as the FTC has lamented the inadequacy of its current authority, it has staked out a bold position on the scope of harm covered by unfairness. While unfairness certainly can cover nonmonetary harms, like reputation, the Unfairness Doctrine requires actual harm, not merely the risk of harm. While the Unfairness Doctrine should never coerce compliance with self-regulation, as Chairman Leibowitz suggested, it can validly punish laggards that persist in a practice disavowed by most of an industry. For example, standard industry practice recently helped the FTC establish that it was unfair for the Frostwire mobile android app to share every file on users' mobile phones without disclosing this when users did not expect this setting and could not change it easily. Unfairness is intended precisely to discourage such traps but not to punish innovative new paradigms for sharing information.

If the FTC dictates fair product design based on static user expectations, innovations that change our thinking about privacy, like the camera in 1890, will suffer. The problem with the Unfairness Doctrine is that the FTC has never had to defend its application to privacy in court, nor been forced to prove harm is substantial and outweighs benefits.

Given the strong reputational incentives by companies to settle out of court, only Congress can call the agency to account. Just as Congress once required the agency to produce its unfairness and deception statements, Congress should require the agency to explain how it has applied both doctrines to privacy.

And finally, Congress must ensure the FTC has the technical capacity for effective enforcement to balance its harms with benefits. The right measure is not how many lawsuits the agency brings, but whether it effectively deters the occasional abuses of data while enabling and even encouraging the overwhelming benefits created by the steady flow of information. Thank you again for inviting me to testify here today.

[The prepared statement of Mr. Szoka follows:]

Testimony of
Berin Szoka, President
TechFreedom[1]

on

Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?

Before the House Energy & Commerce Committee
Subcommittee on Commerce, Manufacturing, and Trade[2]
March 29, 2012

I. Introduction

The central challenge facing policymakers is three-fold:

- Defining what principles should govern privacy policy;
- Transposing those principles into concrete rules, whether through self-regulation or legislation, and updating them as technology changes; and
- Determining how to effectively enforce compliance.

Unfortunately, the privacy debate has until now focused mostly on the first part, crafting the right principles. Both President Obama's proposed "Consumer Data Privacy Framework"[3] and the FTC's Report[4] do wisely recognize not only the central importance of the second part (transposition from the abstract to the concrete), but also that the "flexibility, speed, and decentralization necessary to address Internet policy challenges"[5]—like balancing the dangers of data with its benefits—can come only from a self-regulatory process such as the Commerce Department has proposed to facilitate.[6]

---

1 Berin Szoka (@BerinSzoka) is President of TechFreedom, a non-profit, non-partisan technology policy think tank. He has written and commented extensively on consumer privacy. In particular, he testified on COPPA before the Senate Commerce Committee on April 29, 2010, available at http://tch.fm/syexUo, ("Szoka Testimony").

2 http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=9404

3 The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy ("White House Report"), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

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

5 White House Report at 23.

6 National Telecommunications and Information Administration, Request for Comments, *Multistakeholder Process to Develop Consumer Data Privacy Cades of Conduct* ("NTIA RFC"),

But both the White House and FTC propose principles that, while noble in their aspirations, may prove counter-productive for consumers if transposed without a careful consideration of the real world trade-offs inherent in regulating consumer data practices. Both documents present reformulations of the Fair Information Practice Principles. While the White House framework is perhaps the best articulation of the FIPPs thus far, the FIPPs alone cannot protect consumers effectively—at least not without imposing significant costs and burdens on consumers. The devil lies in effective transposition. As the Cato Institute's Jim Harper puts it so eloquently puts it:

> Appeals to the [FIPPs] are a ceremonial deism of sorts, boilerplate that advocates use when they don't know how to give consumers meaningful notice of information policies, when they don't know when or how consumers should exercise choice about information sharing and use, when they don't know what circumstances justify giving consumers access to data about them, and when they don't know how to describe which circumstances—much less which systems or what levels of spending—make personal data sufficiently "secure."[7]

Moreover, neither the White House nor the FTC adequately explores the legal authority and institutional capacity necessary to achieve effective enforcement, the real heat of the privacy problem. On capacity, Congress has a vital role to play in ensuring that the FTC has a clear plan to develop the in-house technical capacity it needs to keep pace with technological change and the resources needed to implement that plan.

Importantly in this regard, developing the capacity to understand and effectively regulate technology is as much about ensuring that regulators understand how innovative technology confers benefits on consumers as it is about ensuring that regulators understand how new technology *doesn't* impose imaginary costs. As technological advance brings about ever more effective means of collecting and analyzing information, there is a tendency to view this through the lense of harm—to see such advances as ever more intrusive and potentially harmful. Forty years ago, the great economist Ronald Coase warned us: "If an economist finds something—a business practice of one sort or another—that he does not understand, he looks for a monopoly explanation. And as in this field we are very ignorant, the number of understandable practices tends to be very large, and the reliance on a monopoly explanation, frequent."[8] The same risk arises here—that, finding a technology that they don't understand, regulators will look for a nefarious (or "unfair") explanation, overestimating harms to users (the more easily seen) and understating benefits (the more likely unseen).[9] Ensuring that regulators

---

https://www.federalregister.gov/articles/2012/03/05/2012-5220/multistakeholder-process-to-develop-consumer-data-privacy-codes-of-conduct.

[7] Jim Harper, *Reputation Under Regulation: The Fair Credit Reporting Act at 40 and Lessons for the Internet Privacy Debate*, Cato Policy Analysis No. 690 (Dec. 8, 2011), http://www.cato.org/pubs/pas/PA690.pdf.

[8] Ronald Coase, *Industrial Organization: A Proposal for Research*, in 3 Policy Issues and Research Opportunities in Industrial Organization, 59, 67 (Victor Fuchs ed. 1972).

[9] See Frederic Bastiat, *What Is Seen and What Is Not Seen*, http://www.econlib.org/library/Bastiat/basEss1.html

have the capacity to keep up with technological change is thus essential to facilitating both effective and appropriately restrained enforcement.

On authority, the FTC could do more with its existing unfairness authority to build a quasi-common law through enforcement actions and written guidelines on consumer data practices that cause greater consumer injury than benefit and which consumers themselves cannot reasonably avoid. The Unfairness Doctrine is a powerful tool by which the FTC can punish either practices not addressed by self-regulation or companies that simply choose not to abide by self-regulation. But it is precisely because this tool is so powerful that its use was carefully limited by the FTC in 1980—and should remain so.[10] If the Unfairness Doctrine proves too limited in the non-economic harms it recognizes, Congress should craft legislation narrowly tailored to those harms, rather than allowing the FTC to expand the scope of the Unfairness Doctrine in general. But even in legislating based on a somewhat broader conception of harm, Congress should heed the basic approach of the Unfairness Doctrine, which remains a sound basis for effective consumer protection: weigh consumer harm against consumer benefit and intervene only where consumers themselves cannot reasonably avoid the harm, such as through their own use of more effective privacy controls.

If Congress is ever to grant the FTC new authority in this area, it should at least wait to learn from the self-regulatory process. Congress should assess the failure or success of the overall self-regulatory system in three ways:

1. **Enforcement**: Can compliance with self-regulatory codes of conduct be policed effectively? If not, how can industry self-enforcement of self-regulation be strengthened? And how can FTC enforcement based on deception be enhanced?
2. **Outside Self-Regulation**: Can companies that remain outside self-regulation be policed effectively? If not, to what extent is the problem that the FTC lacks institutional capacity to use its unfairness authority effectively or that its legal authority is too limited because the limits on the Unfairness Doctrine make successful litigation too difficult?
3. **Scope & Evolution**: Does self-regulation adequately address privacy practices that, on net, harm consumers and cannot be reasonably avoided by consumers themselves?

In the first two cases, policymakers would do well to heed the paraphrase of an old adage about malice:[11] never attribute to a lack of legal authority that which can be adequately explained by a lack of institutional capacity. Of course, institutional capacity only goes as far as the FTC's legal authority, but where capacity is lacking, how can we know whether authority is really inadequate?

---

[10] FTC Policy Statement on Unfairness ("Unfairness Policy Statement"), appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984). See 15 U.S.C. § 45(n).

[11] Hanlon's Razor is an eponymous adage that reads: "Never attribute to malice that which is adequately explained by stupidity." See, e.g., http://en.wikipedia.org/wiki/Hanlon's_razor.

II. A "Bill of Rights" for Consumer Privacy?

It was President Kennedy who first introduced a Consumer Bill of Rights in a speech to Congress in 1962.[12] So it is hardly unprecedented that President Obama should choose a similar label for his consumer privacy framework. No doubt this is a highly effective rhetorical framing that will drive action—whether by industry or Congress—on this complicated and often arcane topic. But the "Bill of Rights" term is problematic in two senses.

First, the Report begins and ends as constitutional sleight-of-hand. President Obama starts by reminding us of the Fourth Amendment's essential protection against "unlawful intrusion into our homes and our personal papers"—by government. But the Report recommends no reform whatsoever for outdated laws that have facilitated a dangerous expansion of electronic surveillance. In other words, while the White House embraces the "Consumer Bill of Rights" rhetoric, the *real* Bill of Rights is in peril. This was precisely the message sent by a unanimous Supreme Court two months ago in its *Jones* decision.[13] Indeed, five Justices called on Congress to remedy this situation by updating outdated laws intended to implement the Fourth Amendment's protections in digital technologies.[14] The gravest threat to our privacy comes from Congress's failure to enact such reforms—while instead focusing its limited attention on legislation mandating that private companies retain *more* information about how we use the Internet, which law enforcement could access without judicial scrutiny,[15] and cybersecurity legislation designed to facilitate the monitoring of user communications.[16] Unfortunately, the White House Report dismisses such concerns in the first footnote.[17]

Second, conceptualizing privacy in "rights" terms, while emotionally appealing, is deeply problematic. The rights contained in the *real* Bill of Rights stand between us and our government, whose proper purpose is to protect our negative rights to life, liberty and the pursuit of happiness. "Rights" are, in philosophical parlance, often conceived as "trumps" over mere "interests"—in other words, not subject to trade-offs or balancing, except perhaps with

---

[12] John F. Kennedy, 93 - Special Message to the Congress on Protecting the Consumer Interest, Mar. 15, 1962, *available at* http://www.presidency.ucsb.edu/ws/?pid=9108.

[13] U.S. v. Jones, 565 US __ (2012), http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf.

[14] Id.; Berin Szoka & Charlie Kennedy, *Supremes to Congress: Bring Privacy Law Into 21st Century*, CNET, Jan. 29, 2012, http://news.cnet.com/8301-13578_3-57368025-38/supremes-to-congress-bring-privacy-law-into-21st-centur/.

[15] Berin Szoka, *Leading Free Market Groups Urge Congress to Update Key U.S. Privacy Law*, TechFreedom, April 6, 2011, http://techfreedom.org/blog/2011/04/06/leading-free-market-groups-urge-congress-update-key-us-privacy-law.

[16] Cybersecurity Act of 2012, 112th Congress (2012), http://www.hsgac.senate.gov/download/the-cybersecurity-act-of-2012-s-2105; Jim Harper, *The Senate's SOPA Counterattack?: Cybersecurity the Undoing of Privacy*, Cato@Liberty, Feb. 9, 2012, http://www.cato-at-liberty.org/the-senates-sopa-counterattack-cybersecurity-the-undoing-of-privacy/.

[17] "This framework is concerned solely with how private-sector entities handle personal data in commercial se ttings. A separate set of constitutional and statutory protections apply to the government's access to data that is in the possession of private parties." White House Report at 5 n. 1.

other rights.[18] This is essentially the European conception of privacy as a "fundamental human right." It conceives of privacy as a positive right, rather than the sort of negative right recognized under U.S. law. It is also essentially a property right in personal information, a problematic concept when applied to personal information.[19]

III. The Power, Risks and Benefits of Data

The privacy debate rests on a recognition of the growing power of data to shape our lives. But largely because of the conceptualization of privacy as a positive (fundamental) right, or a strict property right in personal information, the privacy debate has been systematically biased by an over-statement of the risks and an under-statement of the benefits of data. A more realistic debate would begin by weighing real privacy harms (a subject discussed below in the context of the FTC's Unfairness Doctrine) with information benefits such as:

- Enhanced advertising revenues for publishers of content and services that might otherwise have difficulty funding their offerings by charging for data, especially in markets where marginal costs are lower or zero (and basic economic theory would suggest that competition will inevitably drive prices towards zero).
- More effective advertising, which in turn means
    - More relevant, and potentially less annoying/interruptive advertising for consumers;
    - Better correlation between the production of content and services, and consumer
    - preferences;
    - Lower prices for consumers and greater innovation throughout the economy;
    - Better non-commercial messaging, too; and
    - More vibrant media and improved political discourse and communities[20]
- Serendipitous innovation based on the discovery of unexpected uses of data.

As discussed below, the FTC's existing Unfairness Doctrine provides a sound vehicle for weighing harms with benefits, and regulating only where users cannot reasonably avoid a harmful practice. But more generally, balancing risks realistic assessment of the degree to which a particular data set is likely to be tied back to a particular user at all.

---

[18] Leif Wenar, "Rights", The Stanford Encyclopedia of Philosophy (Fall 2011 Edition), Edward N. Zalta (ed.), http://plato.stanford.edu/archives/fall2011/entries/rights/#5.1.

[19] *See generally* Larry Downes, *The Laws of Disruption: Harnessing the New Forces that Govern Life and Business in the Digital Age* 70-71 (2009).

[20] *See generally* Berin Szoka, *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech,* Comments the FTC Privacy Roundtables (Dec. 7, 2009), *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00035.pdf

IV. PII, Anonymization & Re-Identification

The FTC's 2010 Preliminary Staff Report hinted that the agency might abandon the traditional distinction between PII and non-PII on the grounds that relevance of this distinction is decreasing as it becomes possible to identify anonymous datasets, or to re-identify de-identified data.[21] But in the face of criticism, the final FTC Report changed course and clarified that "data is not 'reasonably linkable' to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data." This is an eminently sensible compromise.

While the White House Report does not explicitly address the debate that has raged behind this reversal of positions, nor does it emphasize the importance of de-identification in general, it does specifically call for de-identification as a core element of its "Transparency"[22] and "Focused Collection"[23] principles.[24]

Ensuring proper de-identification should be a core goal of self-regulation—and legislation, if that proves necessary. Balancing realistic risks of re-identification with a realistic assessment of harms likely to flow from re-identification is essential to ensuring that privacy regulation (and self-regulation) benefits consumers. As Brooklyn Law School professor Jane Yakowitz explains in her seminal 2011 law review article, Tragedy of the Data Commons:

> Accurate data is vital to enlightened research and policymaking, particularly publicly available data that are redacted to protect the identity of individuals. Legal academics, however, are campaigning against data anonymization as a means to protect privacy, contending that wealth of information available on the Internet enables malfeasors to reverse-engineer the data and identify individuals within them. Privacy scholars advocate for new legal restrictions on the collection and dissemination of research data. This Article challenges the dominant wisdom, arguing that properly de-identified data is not only safe, but of extraordinary social utility. It makes three core claims. First, legal scholars have misinterpreted the relevant literature from computer science and statistics, and thus have significantly overstated the futility of anonymizing data. Second, the available evidence demonstrates that the risks from anonymized data are theoretical - they rarely, if ever, materialize. Finally, anonymized data is crucial to

---

[21] FTC 2010 Report at 39.

[22] "[C]ompanies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or *de-identify it from consumers*, and whether and for what purposes they may share personal data with third parties." White House Report at 14 (emphasis added).

[23] "Companies should securely dispose of or *de-identify personal data once they no longer need it*, unless they are under a legal obligation to do otherwise." White House Report at 21 (emphasis added).

[24] The Report also notes that the Department of Health and Human Services "plans to issue additional guidance on the HIPAA Privacy Rule's "minimum necessary" standard and on de-identification of health information under the HIPAA Privacy Rule. White House Report at 43.

> beneficial social research, and constitutes a public resource - a commons - under threat of depletion. The Article concludes with a radical proposal: since current privacy policies overtax valuable research without reducing any realistic risks, law should provide a safe harbor for the dissemination of research data.[25]

V. Individual Control

The White House's first principle is that "Consumers have a right to exercise control over what personal data companies collect from them and how they use it." This is probably the most viscerally compelling principle[26] but is deeply problematic if understood as a "right" to be strictly enforced rather than an aspirational principle to be transposed pragmatically, depending on the trade-offs inherent in the real world. Hence, the vital importance of the word "appropriate."

The concept has its roots in the original 1890 law review article by Warren and Brandeis that gave birth to modern privacy law, where they declared that:

> Recent inventions & business methods call attention to... the right "to be let alone." Instantaneous photographs & newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops.'"[27]

By contrast, the Supreme Court ruled in 1967 that:

> Exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and of press.[28]

In other words, much as we might want a right to keep people from speaking about us, we do not have, as the White House Report suggests if read literally, "a right to exercise [*absolute*] control over what personal data companies collect from [us] and how they use it."[29] UCLA Law professor Eugene Volokh explained this best in his seminal 2000 law review article, "Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You.":

---

[25] Jane Yakowitz, *Tragedy of the Data Commons*, 25 Harv. J. of Law & Tech 1 (Fall 2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1789749.

[26] "Properly defined, privacy is the subjective condition people experience when they have power to control information about themselves." Jim Harper, Cato Institute, Understanding Privacy – and the Real Threats to It, Cato Institute Policy Analysis No. 520, Aug. 4, 2004, http://www.cato.org/pub_display.php?pub_id=1652.

[27] Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (Dec. 15, 1890), *available at* http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

[28] Time, Inc. v. Hill, 385 U.S. 374, 388 (1967).

[29] White House Report at 1.

> Government attempts to let us "control ... information about ourselves" sound equally good: Who wouldn't want extra control, especially of things that are by hypothesis personal? And what fair-minded person could oppose requirements of "fair information practices"?
>
> The difficulty is that the right to information privacy—the right to control other people's communication of personally identifiable information about you—is a right to have the government stop people from speaking about you. We already have a code of "fair information practices," and it is the First Amendment, which generally bars the government from "control[ling the communication] of information" (either by direct regulation or through the authorization of private lawsuits, whether the communication is "fair" or not. While privacy protection secured by contract turns out to be constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law.[30]

There are also real costs to choice, and benefits of having no choice, as Indiana University Law professor Fred Cate argues in his essay, "The Failure of Fair Information Practice Principles":

> In some cases, consent may be undesirable, as well as impractical. This is true of press coverage of public figures and events, medical research, and of the many valuable uses of personal information where the benefit is derived from the fact that the consumer has not had control over the information. This is certainly true of credit information: its value derives from the fact that the information is obtained routinely, over time, from sources other than the consumer. Allowing the consumer to block use of unfavorable information would make the credit report useless.[31]

These practical and constitutional realities are already recognized by U.S. privacy law. The Fair Credit Reporting Act, for example, does not allow us to control what others say about our credit history, but instead gives us access and correction rights to make sure the information on which they base what they say about us is accurate.[32] This is premised not on our ownership of "our" information, but on the clear harms that can follow from inaccurate speech about us. While the FCRA is far from perfect,[33] it is at least an example of how a harms-based approach can serve as the basis for preventing harmful uses of information about us. And this example illustrates that even a principle as appealing as individual control cannot be treated as a "right" but must be transposed carefully to apply to a particular privacy problem.

---

[30] Eugene Volokh, *Freedom of Speech, Informotion Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, 1999, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=200469.

[31] Fred H. Cate, *The Failure of Fair Information Practice Principles*, 2006, *available at* http://ssrn.com/abstract=1156972.

[32] Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq., *available at* http://www.ftc.gov/os/statutes/031224fcra.pdf.

[33] Harper, *Reputotion Under Regulation, supra* note 7.

VI. Transparency

In some ways, the transparency principle is perhaps universally embraced in the White House Report. While many questions remain over whether we can rely on notice of a company's privacy practices, and some, like Fred Cate note the costs and failures of notice,[34] it does remain a sound aspirational principle that must be transposed effectively.

The main shortcoming of this principle is that it contemplates that the work of notice will be done primarily, if not entirely, by "plain language statements about personal data collection, use, disclosure, and retention." While such statements *are* important and should be made more readable and conspicuous where feasible, as the FTC Report also proposes,[35] they should be supplemented in two key ways.

First, companies should be encouraged to educate consumers through more accessible forms of notice that explain privacy policies and practices, as the FTC Report contemplates. This could include short videos such as on Google's Privacy Channel on YouTube,[36] FAQs, just-in-time notices about how mobile apps collect data, and so on. The FTC should be commended for making this general inquiry the focus of its upcoming May Workshop.[37]

Second, the White House missed an opportunity to promote the concept of "Smart Disclosure" developed by Cass Sunstein, director of the Office of Information and Regulatory Affairs, a close advisor to the President, and a widely respected thinker in law, policy and technology. In an OIRA memo to agency heads issued last fall, Sunstein defined "smart disclosure" as:

> the timely release of complex information and data in standardized, machine readable formats in ways that enable consumers to make informed decisions. Smart disclosure will typically take the form of providing individual consumers of goods and services with direct access to relevant information and data sets. Such information might involve, for example, the range of costs associated with various products and services, including costs that might not otherwise be transparent. ... In many cases, smart disclosure enables third parties to analyze, repackage, and reuse information to build tools that help individual consumers to make more informed choices in the marketplace.

This provides a powerful vision for reconceiving transparency as something that can be technologically intermediated—meaning that a company's disclosure of its privacy practices (among other things) need no longer be limited to the simplified form of its plain language

---

[34] "Businesses and other data users are burdened with legal obligations while individuals endure an onslaught of notices and opportunities for often limited choice. Notices are frequently meaningless because individuals do not see them or choose to ignore them, they are written in either vague or overly technical language, or they present no meaningful opportunity for individual choice." Cate, *supra* note 31, at 1.

[35] FTC Report at 61.

[36] The Google Privacy Channel, YouTube, http://www.youtube.com/googleprivacy

[37] Press Release, Federal Trade Commission, FTC Will Host Public Workshop to Explore Advertising Disclosures in Online and Mobile Media on May 30, 2012, Feb. 29, 2012, http://www.ftc.gov/opa/2012/02/dotcom.shtm.

disclosure (though, as discussed below, they should be consistent, or punished under the FTC's deception authority). Meaningful smart disclosure on privacy could bypass much of the current debate about the failure of effective notice to empower consumers by making "notice" technologically actionable: Users could subscribe to the privacy recommendations of, say, Consumer Reports, or any privacy advocacy group, which in turn could set their phone to warn them if they install an app that does not meet the privacy practices those trusted third parties deem adequate. Or, more simply, such a system could work for communicating whether a site, service or app acedes to a particular self-regulatory code of conduct—and phone privacy controls could be set by default to provide special notices when users attempt to install apps that do not certify compliance with self-regulatory codes of conduct..

Further, as the FTC Report notes, "Machine-readable policies, icons, and other alternative forms of providing notice also show promise as tools to give consumers the ability to compare privacy practices among different companies."[38] Again, the example of an app store might illustrate how such comparisons could work, allowing users trying to choose between several competing apps to compare their privacy practices side by side.

The FTC Report contemplates a particular application that as Commissioner Brill put it in a public response to my question at a Direct Marketing Association event on the day the FTC Report was released, "... is the first step towards structured disclosure more generally."[39] Specifically, the FTC Report proposes that:

> the data broker industry explore the idea of creating a centralized website where data brokers that compile and sell data for marketing could identify themselves to consumers and describe how they collect consumer data and disclose the types of companies to which they sell the information. Additionally, data brokers could use the website to explain the access rights and other choices they offer consumers, and could offer links to their own sites where consumers could exercise such options. This website will improve transparency and give consumers control over the data practices of companies that maintain and share data about them for marketing purposes.[40]

This concept merits exploration as a way of remedying the lack of transparency regarding companies that currently lack a direct way of offering transparency to those whose data they collect—provided the term "data broker" is defined appropriately. This could be an excellent test case for encouraging smart disclosure through self-regulation—but only if it can be implemented in a way that actually improves transparency for consumers and proves feasible for companies.

---

[38] FTC Report at 62.

[39] Keynote Address by FTC Commissioner Julie Brill at DMA in DC 2012, March 26, 2012, http://newdma.org/dma-in-dc

[40] FTC Report at 69.

VII. Transposition of Principles

Setting aside the first question raised at the outset (choosing the right principles), the core problem remains a practical one: How to translate a set of principles (or "rights") into workable guidelines and, where appropriate, binding rules that inform how data flows across the Internet through countless interactions every minute and through technologies yet to be conceived.

The Report aptly summarizes the virtues of "open, transparent multistakeholder processes": "when appropriately structured, they can provide the flexibility, speed, and decentralization necessary to address Internet policy challenges."[41] American reliance on multistakeholder processes has, as the Report notes, allowed the U.S. Internet policy to avoid "fragmented, prescriptive, and unpredictable rules that frustrate innovation and undermine consumer trust."[42] (This essentially affirms what the FTC said in its 1999 report on privacy: "[S]elf-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology."[43])

But just as the value of privacy principles depends on their transposition into real-world guidelines, that process of transposition depends on whether it is "appropriately structured."[44] In both cases, what matters is not the intention, but the process, for the process is what determines the outcome. If we wish to avoid "failure by design," we must take care to answer the following critical questions carefully.

First, what role will government play? The White House Report says, "The Federal Government will work with stakeholders to establish operating procedures for an open, transparent process. Ultimately, however, the stakeholders themselves will control the process and its results."[45] Fulfilling this promise requires that, if government officials actually serve as facilitators for the process, they must remain neutral conveners, and the principles contained in the White House Report must be clearly understood as one set of hortatory principles, rather than criteria by which the success of the self-regulatory process *must* be judged.

This is the most important factor separating the kind of self-regulation praised by the White House and what the Europeans call "co-regulation." In self-regulation, government may suggest aspirational principles (as the White House has done) and play a convening role, but in co-regulation, government "steers while industry rows," steering the process to determine its outcome. Co-regulation is, in fact, just another vehicle for governmental regulation; and while it might seem comfortably familiar to European privacy regulators, it cannot be relied on to deliver the workable policy framework that can only be forged in a true self-regulatory process as a voluntarily agreed upon compromise among many stakeholders with conflicting interests.

---

[41] *Id.* at 23.

[42] *Id.* at 24.

[43] 1999 FTC Report at 6.

[44] White House Report at 24.

[45] *Id.* at 24.

While the experience of the Digital Advertising Alliance,[46] for example, is a great example of how a multi-stakeholder process can achieve industry consensus on a difficult set of issues, it verges on co-regulation in one key respect: This process is not a high-level framework such as that proposed by the White House Report, but a sector-specific set of principles for online behavioral advertising developed by the FTC.[47] However admirable the end result, the more specifically government sets the basic contours of the self-regulatory process, the more likely that process is to produce outcomes that prove unworkable to some in industry.

Indeed, the less the multistakeholder process verges on co-regulation, the lower the risk of another failure point in the self-regulatory process: a legal challenge by a company that the process constituted government action that should have been subject to normal rulemaking requirements, or that it exceeded the jurisdiction of whichever agency might run the process.

Second, just how "open" and "transparent" must the process be? Requiring all discussions to take place in public would chill the very open dialogue among companies about their technologies and business practices necessary to allow self-regulation to distill widely dispersed expertise into workable compromises. This reality demands that at least some negotiations be conducted in private, without government or privacy advocates in the room—because both could use information derived from these negotiations in litigation against (or at least public criticism of) particular companies, something that would chill candid participation by those companies.

Third, how will civil society groups participate in the process? If they may exercise a "heckler's veto," they could derail the process. On the other hand, they may prove invaluable to the success of the process so long as their criticism is constructive, offering concrete suggestions on how to better protect privacy. And to the extent they can support the codes of conduct that result from the process, or at least the legitimacy of the process that produced them, the evolving U.S. privacy regime will benefit from greater acceptance by the public and our International partners. Of course, they need not accept these codes as the final word on the matter, and remain free to produce their own "minority report" or lobby for legislation in a particular area.

The model of the Digital Advertising Alliance is thus further instructive: Industry responded to the problem identified by the FTC's 2009 "Self-Regulatory Principles For Online Behavioral Advertising" by convening their own multi-stakeholder process behind closed doors, resulting in a set of principles unanimously approved by the participating companies.[48] The DAA published a draft report, solicited feedback from privacy advocates and the FTC, and reconvened their process to produce a final code of conduct, to which they unanimously certified.

---

[46] Digital Advertising Alliance, *Self-Regulatory Principles for Multi-Site Data* (2011), http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

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

[48] Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioral Advertising* (2009), http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf.

Fourth, by whom will self-regulatory codes of conduct be subject to approval? The White House Report merely says "the stakeholders themselves will control the process and its results"[49] but does not clarify what that means. Outrageous as it will surely seem to some, it must be industry itself that determines whether to approve a code of conduct. Otherwise, the process will fail because companies simply will not abide by the codes of conduct it produces. This is likely to be the most controversial aspect of designing the multi-stakeholder process because the expectations of privacy advocates are simply unrealistic. For example, in testimony before this Subcommittee last October, Pam Dixon of the World Privacy Forum demanded "Consumer, public interest and other independent representatives must be fully represented (if possible, up to 75 percent or more) on the governing bodies of self-regulatory schemes."[50]

Given such expectations, not getting to vote *at all* on approval will be a difficult pill for many well-meaning privacy advocates to swallow. But they can still meaningfully shape the outcome of these self-regulatory processes even without voting on the final product, not only through their official input in the process, but through their ability to channel public pressure on the companies that participate. The widespread public opposition to SOPA and PIPA earlier this year demonstrated just how powerful public pressure can be. There is no reason why civil society groups cannot attempt to use such grassroots pressure to influence the self-regulatory process.

Fifth, regardless of *who* votes, what will be the mechanism for voting? How high will the threshold be for approval, and how will voting power be determined? These are questions best answered by professionals with expertise in designing choice mechanisms for multi-stakeholder processes. As a number of economists have shown, the outcomes of a voting system are highly contingent on its structure.[51] Commissioner Rosch's concern about the danger of capture by industry leaders is worth noting.[52] But it nonetheless seems inevitable that voting power will have to be related in some fashion to market share. Otherwise, the outcome will be determined by who can get more seats at the table—much as the Soviet Union once tried to increase its representation in the United Nations by insisting that Soviet Republics like Byelorussia and Ukraine deserved their own seats.[53]

---

[49] White House Report at 24.

[50] 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, Oct. 13, 2011, at 11, http://republicans.energycommerce.house.gov/Media/file/Hearings/CMT/101311/Dixon.pdf.

[51] James Buchanan & Gordon Tullock, *The Calculus of Consent: Logical Foundations of Constitutional Democracy*, http://www.econlib.org/library/Buchanan/buchCv3.html.

[52] "[T]he self-regulation that is championed in this area may constitute a way for a powerful, well-entrenched competitor to raise the bar so as to create an entry barrier to a rival that may constrain the exercise of undue power. That possibility may be blunted by insuring that smaller rivals participate in the adoption of self-regulatory rules, but that may not be practical." Rosch statement, 2010 Draft Privacy Report at E-3.

[53] *See* N.S. Timasheff, *Legal Aspects of the Grant of Three Seats to Russia in the United Nations Charter*, 14 Fordham L. Rev. 180 (1945), http://ir.lawnet.fordham.edu/flr/vol14/iss2/4.

Sixth, will there be a shot clock for the process? If so, how will it work? If not, how can we ensure that each self-regulatory process work expeditiously and that those companies that prove resistant to compromise will not unduly drag out the process as a negotiating tactic? As with the voting mechanism, reasonable time limitations that are made clearly *ex ante* can help to avoid process failure—so long as they provide adequate time to resolve the issues specific to that process.

Seventh, how will the initial selection of issues work? The White House Report proposes only that "Stakeholder groups, with the assistance of NTIA, will identify markets and industry sectors that involve significant consumer data privacy issues and may be ripe for an enforceable code of conduct."[54] This conversation is probably one that can happen entirely in public, and would very much benefit from the active (and constructive) participation of civil society groups. The best way to approach this process may be to create a prioritized list of issues that make sense of the basis for a potential code of conduct, either specific to an industry or to a cluster of related practices.

For example, early topics to be considered might include transparency in the mobile ecosystem (a topic on which the FTC will hold a workshop in May[55]), cross-border transfers of cloud data, and transparency regarding "data brokers" whose operations are not directly visible to the public (a topic identified as critical by the FTC Report—but without any definition of the broad term "data broker"[56]). Other topics that may merit attention include the portability of user data, interoperability of privacy controls, and machine-readable disclosures (discussed above).

Finally, how exactly will self-regulatory codes of conduct be updated? By shaping expectations during initial negotiation, this question will play a large role in the success or failure of the initial process. The White House Report raises as many questions as it answers in this regard with its discussion of "evolution": "Stakeholders may decide at any time that a code of conduct no longer provides effective consumer data privacy protections, in light of technological or market changes."[57] How many? Much like the initial voting mechanism question, industry participants need to know *ex ante* what will be required to re-open negotiation of, and actually amend, a code of conduct. This is probably a question best resolved by industry itself in the initial negotiations. "NTIA might also ... seek to re-convene stakeholders. As with the initial development of a code of conduct, however, stakeholder participation in the process to revise a code of conduct would be voluntary."[58] So what will constitute an effective "quorum" for a revised process? Or will it be sufficient that some companies might accede to a version 2.0 of a code? What will happen if a code "forks" into multiple pieces (as sometimes happens with

---

[54] White House Report at 26.

[55] Press Release, Federal Trade Commission, FTC Will Host Public Workshop to Explore Advertising Disclosures in Online and Mobile Media on May 30, 2012, Feb. 29, 2012, http://www.ftc.gov/opa/2012/02/dotcom.shtm.

[56] FTC Staff Report at 68-70.

[57] White House Report at 27.

[58] *Id.*

open source standards)? If "Congress could prescribe a renewal period for codes of conduct," what would be required to renew and extend them?

VIII. Accountability: Effective Enforcement

Having discussed the first and second questions identified at the start of this testimony, let us now turn to the third: how the FTC can effectively enforce compliance. This has three component parts:

- Institutional enforcement capacity
- Deception authority
- Unfairness authority

The White House Report rightly emphasizes the need for "strong enforcement," but focuses on granting new legal authority to the FTC. Before reaching this point, the Report should have asked whether the FTC has the enforcement capacity necessary to use its existing authority—or to use any new authority it might be given—and whether that existing legal authority is being fully realized.

A. Enforcement by the Reputation Market

But before turning to turning enforcement by government, it is worth considering the way the Internet itself facilitates pressure on companies through the "reputation market" to abide by their privacy promises and improve their privacy practices. The social media revolution has made it possible for anyone concerned about online privacy to blow the whistle on true privacy violations. That whistle may not always be loud enough to be heard, but it's more likely to in this sector than any other. Traditional media sources like the Wall Street Journal have played a critical role in attracting attention to corporate privacy policies through its "What They Know" series,[59] which has been popularized using social media tools.

Social media tools were recently used to great effect to express grassroots concern about proposed copyright legislation. While some Internet companies certainly helped to promote these messages, even without their involvement, this experience demonstrates how effective social media activism can be. There is no reason why such techniques cannot be used effectively against major Internet companies themselves, just as Facebook users have used Facebook itself to rally opposition to Facebook on privacy concerns such as its Beacon ad targeting system.[60] Among the most important factors driving companies to participate

[59] *What They Know,* Wall St. J., 2012, http://blogs.wsj.com/wtk/.

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

constructively in the multi-stakeholder process, to forge meaningful privacy protections, and to abide by them will be the fear of a Wall Street Journal article, a social media frenzy, or organized campaign demanding action on a particular privacy problem.

B. Enhancing the FTC's Institutional Technical Capacity

Effective FTC enforcement requires the technical knowledge of the industry. Chairman Leibowitz deserves credit for appointing the agency's first Chief Technologist.[61] But even with someone as talented as Ed Felten in that position, the FTC is still way behind the curve: Ed's title is not Chief Technology *Officer* because there is no office behind him. Just over five years ago, Peter Swire called on the agency to "consider a new office of information technology to assist the Commission in making effective decisions about how to protect consumers in Internet activities. This office would parallel the FTC's in-house capability in economics, and would permit the FTC to act strategically to protect consumers from emerging online threats."[62]

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

These suggestions in no way diminish the important enforcement work done by the FTC's hardworking staff. To the contrary, it is unfair and unrealistic to expect the FTC to fulfill its consumer protection mission in the face of massive technological change without the expertise required to stay ahead of that change. If, in the last five years, policymakers had spent a fraction as much time on improving the FTC's institutional capacity as inventing new authority, the U.S. privacy regime would be far more effective in protecting consumers and ensuring their trust, and less easily dismissed as inadequate by foreign privacy regulators.

C. Enhancing the FTC's Deception Authority through Smart Disclosure

Punishing deception is the bedrock of the FTC's current privacy regime[63]—and it will the the ultimate tool for ensuring accountability by companies to the self-regulatory codes of conduct to which they subject themselves. Yet both the White House Report and the FTC Report miss

---

[61] Federal Trade Commission, *FTC Names Edward W. Felten as Agency's Chief Technologist; Eileen Harrington as Executive Director*, Nov. 4, 2010, http://www.ftc.gov/opa/2010/11/cted.shtm.

[62] Peter Swire, *Funding the FTC: Globalization and New Information Technologies Necessitate on Appropriotions Boost*, February 26, 2007, http://www.americanprogress.org/issues/2007/02/ftc.html

[63] "[T]he Commission will find deception if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment." FTC Policy Statement on Deception, 1983, http://www.ftc.gov/bcp/policystmt/ad-decept.htm (appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984)).

an important opportunity to enhance the FTC's deception authority through the enforcement of structured, machine-readable disclosures.

At a minimum, such disclosures could be used to indicate which self-regulatory codes of conduct the site or service complies with. This, in turn, should facilitate FTC enforcement by allowing the agency to easily determine the universe of companies acceding to the code.

In a more robust form, machine-readable disclosures could also be used by companies that want to accede to most of a code of conduct but not to particular components of its rules—or all of a code, *plus* additional protections. This might create a practicable way of managing enforcement of a multiplicity of codes of conduct without requiring binary all-or-nothing compliance. That, in turn, might help to facilitate both successful resolution of the multistakeholder process and continuing competition on privacy. In other words, companies are more likely to treat codes of conduct as a floor for their practices, rather than a ceiling, if they can be rewarded for exceeding the basic requirement of a code.

But to succeed in promoting the White House's Accountability principle, smart disclosures must be as legally enforceable as the plain language versions to which they correspond. The Deception Doctrine requires that a misrepresentation or omission be both likely to mislead a consumer and "material."[64] Thus, for example, a machine-readable statement about corporate privacy practices that was implemented as an industry standard but never adopted in any way that consumers actually relied upon might not be subject to a deception action, no matter how misleading a disclosure in that format might be. On the other hand, once relied upon by even a relatively small group of consumers, such a disclosure system *should* be legally enforceable under the Deception Policy Statement, which specifically notes that, "If the representation or practice affects or is directed primarily to a particular group, the Commission examines reasonableness from the perspective of that group."[65] In other words, even if only a relatively niche group of "power users" used a setting in their app store to limit installations to apps that complied with certain privacy practices, or acceded to particular codes, these representations should be enforceable by the FTC.

Unfortunately, such case of widespread deception has persisted for many years without an FTC enforcement action. In 2002, W3C published P3P: The Platform for Privacy Preferences,[66] which allows websites to describe their privacy practices in a compact privacy policy. Internet Explorer, starting with version 6 (released in 2001), will, by default, not load third party cookies from sites that do not have a compact privacy policy.[67] It was widely known for many years that many companies created compact privacy policies that did not correspond to their human-readable privacy policy (or their actual privacy practices), but in 2008 Lorrie Faith Cranor

---

[64] *Id.*

[65] *Id.*

[66] Platform for Privacy Preferences (P3P) Project, Enabling Smarter Privacy Tools for the Web (2007), http://www.w3.org/P3P/.

[67] Privacy in Microsoft Internet Explorer 6, MSDN, http://msdn.microsoft.com/en-us/library/ms537343.aspx

published a research paper documenting widespread mis-statements in P3P policies.[68] In December, a federal court dismissed a suit against Amazon on similar grounds for lack of standing,[69] making it clear that if P3P policies are to be enforced, the task must fall to the FTC.

While the FTC has never, to my knowledge, explained why it has not brought an enforcement case based on P3P misrepresentations, one possible explanation is that they have concluded that the IE6 implementation is inadequate to demonstrate that the representations within the compact privacy actually mislead consumers, as the Deception Policy Statement requires, because IE6 requires only that a site have a policy, not that the policy say anything in particular.

If so, the lesson is that any self-regulatory effort geared toward using machine-readable disclosures should be conducted in conjunction with those who might develop tools based on such disclosures, particularly browser-makers, to ensure that the useful disclosures are implemented by useful tools.

D. Using the FTC's Unfairness Authority

The FTC's unfairness jurisdiction is often mentioned only as an afterthought, but in fact, as the Commission has held, "unfairness is the set of general principles of which deception is a particularly well-established and streamlined subset."[70] As so often happens in policy discussions, the Report pays scant attention to the FTC's unfairness jurisdiction, merely noting, in a footnote, that it "will remain an important source of consumer data privacy protection."[71] In fact, this jurisdiction is the key to how the FTC could effectively police online privacy outside of self-regulation—punishing companies that do not participate in self-regulation as well as practices that are not prohibited by self-regulation.

This jurisdiction is a powerful tool against privacy abuses because it allows the FTC to build a quasi-common law limiting harmful trade practices as technology evolves. But unfairness can

---

[68] Lorrie Faith Cranor, Serge Egelman, Steve Sheng, Aleecia M. McDonald & Abdur Chowdhury, *P3P Deployment on Websites*, 7 Electronic Commerce Research and Applications 3, 274-293 (Autumn 2008), *pre-print available at* http://lorrie.cranor.org/pubs/p3p-deployment.html (In a study comparing the actual P3P policies of 21 popular websites to the corresponding natural language policies, the researchers found that only two P3P policies correctly specified the types of data that were being collected. As a result, "users reading only a P3P policy might be surprised to find a site collecting more data than what was advertised." p. 40. All of the sites has discrepancies regarding the ways in which collected data may be used. p. 40-41. And "[o]nly six of the websites examined either accurately report their data sharing policies ... or their P3P policies are overly inclusive ... in their reporting of data sharing." p. 41.).

[69] Del Vecchio v. Amazon, C11-366-RSL (W.D. Wash.; Dec. 1, 2011), available at http://docs.justia.com/cases/federal/district-courts/washington/wawdce/2:2011cv00366/174037/58/0.pdf?ts=1322842930; *see also* Venkat Balasubramani, *The Cookie Crumbles for Amazon Privacy Plaintiffs – Del Vecchio v. Amazon*, Technology & Marketing L. Blog, Dec. 2, 2011, http://blog.ericgoldman.org/archives/2011/12/the_cookie_crum.htm.

[70] International Harvester, 104 F.T.C. 949, 1060 (1984) *(cited in* J. Howard Beales, III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, § III, http://www.ftc.gov/speeches/beales/unfair0603.shtm [hereinafter *Beales Paper*]).

[71] Report at 27 note 32.

be a dangerous legal weapon if unleashed from its current limitations. Understanding the checkered history of the Unfairness Doctrine is essential to understanding the evolution of the FTC and U.S. consumer protection law more generally. In brief, until 1964, the agency generally did not distinguish between unfair acts and deceptive ones. In 1964, the agency defined "unfairness" in highly subjective terms, without weighing the benefits of a practice or how easily consumers could avoid it.[72] This led the FTC on an unfairness rule-making spree, trying to regulate everything from funeral home practices to advertising to children—to the point that it was dubbed the "National Nanny" by the Washington Post—hardly a Thatcherite bastion.[73] In fact, the Democratic Congress responded by briefly shutting down the agency and slashing its budget to make it clear that it had not dubbed the agency a regulatory knight errant, free to tilt its steely lance at imagined windmills of "unfairness" or "deception."[74] While this experience did serious harm to the FTC's institutional capacity,[75] it also led to the formulation of clear policy statements on unfairness (in 1980) and deception (in 1983), both at the request of Congress. These today provide the basis for the FTC's enforcement actions, and also reasonably clear legal standards by which companies may predict their legal liability. In 1994, Congress enshrined the Unfairness Policy Statement in the FTC Act itself.[76]

Under the Statement and the 1994 amendment, the Commission applies a two part test. First, it asks whether an "unjustified consumer injury" has occurred:

> To justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided.[77]

Second, the FTC will consider:

> whether the conduct violates public policy as it has been established by statute, common law, industry practice, or otherwise. This criterion may be applied in two different ways. It may be used to test the validity and strength of the

---

[72] See generally, Beales Paper, *supra* note 70.

[73] *Id.* (*citing* Wash. Post, March 1, 1978).

[74] *Id.*

[75] The agency in 2010 had 34% fewer full time equivalent employees as it did in 1980 (even without adjusting to for the growth in U.S. population)—and that number has grown significantly since the original slashing. *See* FTC Full-Time Equivalent History, http://www.ftc.gov/ftc/oed/fmo/fte2.shtm.

[76] 15 U.S.C. § 45(n) ("The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

[77] 1980 FTC Unfairness Policy Statement.

> evidence of consumer injury, or, less often, it may be cited for a dispositive legislative or judicial determination that such injury is present.[78]

But, by statute, "[s]uch public policy considerations may not serve as a primary basis for such determination."[79] Howard Beales has summarized the Unfairness Doctrine as follows:

> the modern unfairness test reflects several common sense principles about the appropriate role for the Commission in the marketplace. First, the Commission's role is to promote consumer choices, not second-guess those choices. That's the point of the reasonable avoidance test. Second, the Commission should not be in the business of trying to second guess market outcomes when the benefits and costs of a policy are very closely balanced or when the existence of consumer injury is itself disputed. That's the point of the substantial injury test. And the Commission should not be in the business of making essentially political choices about which public policies it wants to pursue. That is the point of codifying the limited role of public policy.[80]

The FTC has used its unfairness authority to protect privacy in several lines of cases. First, as noted in the FTC's 2010 Preliminary Staff Report, the Commission brought a number of unfairness cases requiring adequate security practices.[81] But as Commissioner Rosch noted in his concurring statement, "there was financial harm threatened in those cases."[82] Second, the FTC has brought unfairness actions to punish retroactive application of a revised privacy policy.[83] Third, late last year, the FTC brought, and successfully settled (but did not fully litigate) an unfairness case against Frostwire, the maker of a mobile peer-to-peer file-sharing program for its unfair product design. This case is groundbreaking both because it applies unfairness in the context of how product design can cause users to share more information than they expect and because it rests on non-monetary harms.

E. Unfairness and the Harm Debate

As noted above, the extent of the Unfairness Doctrine's applicability rests primarily on how broadly harm is defined—as is implied by the FTC's declaration that "Unjustified consumer injury is the primary focus of the FTC Act.""[84]

---

[78] *Id.*

[79] 15 U.S.C. § 45(n).

[80] Beales Paper, *supra* note 70.

[81] 2010 FTC Report at 10.

[82] 2010 FTC Report at E-2 n. 3.

[83] See, e.g., Gateway Learning Corp., No. C-4120, 2004 WL 2618647 (F.T.C. Sept. 10, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/0423047.shtm; Federal Trade Commission, *Self-Regulatory Principles for Online Behavioral Advertising supra* note 47, at 19; *see also* In re Orkin Exterminating Co., 108 F.T.C. 263 (1986), aff'd, 849 F.2d 1354 (11th Cir.).

[84] 1983 FTC Unfairness Policy Statement.

Even critics of the Unfairness Doctrine have been careful not to rule out its proper application in privacy cases. For example, in 2000, the Commission settled an enforcement action against ReverseAuction, which had violated eBay's terms of service by "using the e-mail addresses, eBay user IDs, and feedback ratings of eBay registered users for the purposes of sending unsolicited commercial e-mail to such registered eBay users."[85] Commissioners Swindell & Leary dissented, in part, on the grounds that this should have been a pure deception case and that violating user privacy by sending such unsolicited email "did not cause substantial enough injury to meet the statutory standard" but emphasized that "[w]e do not say that privacy concerns can never support an unfairness claim." Instead, they simply argued that: "This standard for substantial injury overstates the appropriate level of government-enforced privacy protection on the Internet, and provides no rationale for when unsolicited commercial e-mail is unfair and when it is not. We are troubled by the possibility of an expansive and unwarranted use of the Unfairness Doctrine."[86]

Howard Beales, former Director of the FTC's Bureau of Competition, argues that "Subjective value, as opposed to emotional distress, can be a form of real injury. For example, falsely claiming that a product is kosher would cause real harm to anyone on a kosher diet."[87] More importantly, he argues that reputational harm can be "substantial injury" under the Unfairness Doctrine. In a 2003 case brought by the Bureau of Competition under Beales, the FTC successfully settled a spoofing case:

> "Spoofing" is the practice of making it appear that bulk, unsolicited commercial e-mail ("spam") comes from a third party to the transaction by placing that person or entity's e-mail address in the "from" line of the spam. As a result... spoofing portrays these innocent bystanders as duplicitous spammers, often resulting in their receiving hundreds of angry e-mails from those who had been spammed.
>
> The Commission alleged that this practice was unfair in a federal district court complaint against Brian Westby, who used spam to direct traffic to an adult website. The spam also contained deception in the subject line, tricking consumers, including children, into opening the e-mail and being subjected, in some cases, to graphic adult images. The Commission alleged that this was deceptive. The deception theory, however, does not provide any relief to those consumers who were "spoofed," because they have not relied in any way upon Westby's deception. Unfairness, however, easily reaches the problem. The harm to those consumers - both economic injury caused by damage to their computing

---

[85] Complaint, FTC v. ReverseAuction.com, Inc. File No. 0023046, (Jan. 6, 2000), available at http://www.ftc.gov/os/2000/01/reversecmp.htm.

[86] Statement of Commissioners Orson Swindle & Thomas B. Leary, FTC v. ReverseAuction.com, Inc., File No. 0023046, (Jan. 6, 2000), *available at* http://www.ftc.gov/os/2000/01/reversesl.htm.

[87] Beales Paper, *supra* note 70 (citing Timothy J. Muris, *Cost of Completion or Diminution in Market Value: The Relevance of Subjective Value*, 12 J. Legal Stud. 379 (1983)).

> systems by the huge, unexpected influx of mail, the time spent deleting thousands of e-mails, and *the injury to reputation of hoving their name associated with deceptive adult spam - is substantial.* Hiding the real spammer's identity has no benefit to consumers or competition, so the amount of injury, though substantial, need not be high. Finally, there is no way consumers can anticipate and protect themselves from such an invasion. Anyone with an e-mail account is vulnerable.[88]

In the *Frostwire* case, the FTC alleged a number of non-monetary harms:

> Public exposure of the types of user-originated files that FrostWire for Android shared following a default installation and set-up could increase consumers' vulnerability to identity theft; *reduce their ability to control the dissemination of personal or proprietary information* (e.g., voice recordings or intimate photographs); and increase their risk of legal liability based on prohibitions against, or limitations on, making any such files publicly available for download.[89]

In short, the FTC has staked out a bolder position on the scope of harm covered by unfairness than many realize. This is not, to be sure, the end of the debate. Since these cases have not been litigated, but rather settled before full litigation, it is not certain that this position would survive completely in court. And, on the other hand, FTC Commissioner Julie Brill has raised some difficult questions about the need to recognize harms that are probably more amorphous than ought properly to be recognized under the Unfairness Doctrine.[90]

But as noted at the outset, harms not covered by the Unfairness Doctrine should be addressed by Congress, if at all, under the basic analysis of the Unfairness Doctrine: weigh consumer harm against consumer benefit and intervene only where consumers themselves cannot reasonably avoid the harm, such as through more effective privacy controls. Congress might eventually choose to deem certain practices injurious so that the FTC will need to apply only the other elements of the test. The Unfairness Doctrine contemplates such action through its second prong, clearly established public policy.

The FTC can, however, help to clarify this uncertainty by convening a public workshop on its unfairness authority, with a special emphasis on what it considers the proper definition of harm. Ideally, such a workshop would produce guidelines building on the 1980 Unfairness Policy Statement adequate to help companies predict how to build new and innovative services without running afoul of the unfairness authority. If the FTC pushes the boundaries of harm

---

[88] Beales Paper, *supra* note 70; *See also* FTC v. Westby, No. 03-C-2540 (N.D. Ill. 2003), http://www.ftc.gov/os/2003/09/marriedcomp.pdf.

[89] F.T.C. v. Frostwire L.L.C., No. 11-23643-CV-GRAHAM (S.D. Fla. 2011), at 17. The last claim appears to refer to, *inter alia*, legal restrictions on, for example, making photographs of others publicly available without their consent.

[90] FTC Commissioner Julie Brill, *Big Data, Big Issues*, Remarks at Fordham University School of Law (Mar. 2, 2012), http://www.ftc.gov/speeches/brill/120228fordhamlawschool.pdf.

too far, Congress should intervene, as it did when it ordered the FTC to prepare its policy statements on unfairness and deception in the early 1980s.

F. The Use of Unfairness Authority to Supplement Self-Regulation

While self-regulation does not constitute established public policy adequate to justify an unfairness action on its own (if violated by a company that never acceded to a voluntary code of conduct, therefore making a deception action impossible), self-regulation may *indirectly* bolster an unfairness action—as the *Frostwire* case implies. This nuanced distinction is important to fulfilling the White House Report's promise that "There is no Federal regulation at the end of the process, and codes will not bind any companies unless they choose to adopt them."[91]

Prior to 1983, the Commission considered industry practice as well as statutes and the common law in determining whether a practice violated public policy. But the 1983 Unfairness Policy Statement implies that industry practice may play only a limited role in determining whether a practice violates public policy.[92] The 1994 amendment to the FTC Act goes a step further and declares that "public policy considerations may not serve as a primary basis for [an unfairness] determination."[93] Thus, the precise significance of industry practice remains somewhat unclear—a question that merits clarification by the FTC.

This means that industry practice, such as might be established through self-regulation, will primarily influence the consumer injury prong of unfairness, which the FTC has called "the primary focus of the FTC Act," and which can, "by itself it can be sufficient to warrant a finding of unfairness."[94]

Specifically, in the *Frostwire* case settled late last year, the FTC's unfairness argument relied, in significant part, on the fact that it was not standard industry practice to "allow the public disclosure of private files by default"[95] in establishing two of the three prongs required by the FTC's 1980 Unfairness Policy Statement. Under the third prong, the FTC argued that "a significant number of consumers using Frostwire for Android could not reasonably avoid the unwitting public sharing of their private files. These consumers would not have understood that FrostWire for Android operated in the manner described above from either the Defendants' disclosures or from prior experience with other software."[96] Under the second prong, the FTC argued that "the design and default settings [of Frostwire for Android] provided

---

[91] *Id.* at 24.

[92] 1983 FTC Unfairness Policy Statement ("To the extent that the Commission relies heavily on public policy to support a finding of unfairness, the policy should be clear and well-established. In other words, the policy should be declared or embodied in formal sources such as statutes, judicial decisions, or the Constitution as interpreted by the courts, rather than being ascertained from the general sense of the national values.").

[93] 15 U.S.C. § 45(n)

[94] 1983 FTC Unfairness Policy Statement.

[95] *Frostwire Complaint* at 17.

[96] *Id.* at 16.

few or no countervailing benefits to consumers or competition. Configuring software applications to allow the public disclosure of private files by default runs counter to standard software development guidance, and counter to established practices in the development of file-sharing applications."[97]

It would, of course, have been better—from the perspective of crafting predictable legal standards—if a court had weighed such arguments in an adversarial proceeding and provided guidance on where, exactly, to draw the line on both counts. But both arguments would likely have prevailed in court, had the FTC not settled the case. In this sense, such settled complaints form the basis of a quasi-common law of unfairness (or deception) that is at least adequate to allow companies wrestling with technological change to predict with reasonable confidence what the FTC is likely to consider a violation of Section V of the FTC Act.

The FTC's first argument hinges on their claim that "Nothing in the FrostWire for Android installation and set-up process, or the application's user interface, adequately informed consumers that the application operated in this manner."[98] In this context, the inconsistency of a practice (in this case, public disclosure of private files by default from a peer-to-peer mobile application) with standard industry practice speaks to whether it would have occurred to the reasonable consumer to investigate (a) which files the software made publicly available and (b) how to change the default setting. Simply put, the failure of transparency makes industry standards more dispositive of whether consumers would rightly expect a harmful practice.

The FTC's second argument—that industry standard for software design bear on the analysis of countervailing benefits to consumers or competition—seems somewhat more tenuous but still convincing in this case. While the FTC did not elaborate on this point (as it would have had to do before a judge had the case not been settled), it seems reasonable to argue that compliance with industry standards can benefit consumers both by lowering product design costs and also by lowering the non-monetary costs to users of learning and using a particular product interface. This is not to say that non-compliance with such standards is itself a harm, but it certainly is not a benefit if the non-compliant user interface shares sensitive information by default and makes it extremely difficult for consumers to realize this and change the necessary setting. Of course, more important than this lack of benefit is that the default sharing setting in this case did not seem to provide users a "countervailing" benefit sufficient to outweigh the potential harm flowing from the inadvertent disclosure of all the files on a user's Android device.

In summary, the *Frostwire* case does *not* stand for the proposition that industry self-regulation necessarily binds non-participating companies in its prohibitions on specific practices, but rather for the proposition that, if a company engages in a practice that diverges from industry practice *and* meets the other required elements of unfairness (causing a "substantial injury" that is "not be outweighed by any countervailing benefits to consumers or competition"), its

---

[97] *Id.* at 17.

[98] *Id.* at 16.

burden of empowering consumers to avoid that practice grows as the degree of divergence of industry practice increases.[99] Thus, the Unfairness Doctrine already offers the FTC a tool for implementing the second prong of the new framework it proposes in the FTC [Draft] Report: "For data practices that are not 'commonly accepted,' consumers should be able to make informed and meaningful choices."[100]

Concretely, then, *Frostwire* means that at least some companies that choose not to accede to the standards established by the self-regulatory process envisioned by the White House Report may have to engage in a heightened degree of "Privacy by Design" planning to analyze their non-compliant privacy practices under an unfairness analysis. Depending on their analysis of consumer harms and benefits, they may feel obliged to build accordingly more robust, and more usable, user interfaces that inform the consumer as to privacy defaults and how to change them.

This is precisely as it should be: Using its unfairness authority, the FTC can thus build on self-regulation *without* forcing compliance with self-regulation—in which case self-regulation, no matter how "voluntary" at its outset, would become co-regulation: just another vehicle for imposing top-down solutions on a complex ecosystem that requires, as the Report notes, the "flexibility, speed, and decentralization" that only true self-regulation can provide.

Yet the self-regulatory process is no less voluntary because companies that do not sign on to self-regulatory codes of conduct may be subject to somewhat elevated risks of unfairness enforcement actions for practices that diverge from industry practices established through self-regulation. But it *is* important that industry understand that the FTC's unfairness authority may play an increasingly important role as the U.S. privacy regime evolves towards more robust self-regulation. In this sense, it is that much more unfortunate that neither the White House Report nor the FTC Report does more to explain this seemingly esoteric and under-used, but extremely important, area of law. The FTC workshop and guidelines on unfairness proposed above should specifically consider how unfairness might apply to non-compliance with self-regulatory codes of conduct.

G. Self-Regulatory Policing

Robust self-regulation should involve industry enforcing the requirements on its own—in addition to FTC enforcement. The Digital Advertising Alliance has coordinated with the Better Business Bureau on just such a self-regulatory enforcement program.[101] If successful in demonstrating compliance and/or bringing enforcement actions against non-compliant companies, this enforcement program could be a model for other self-regulatory enforcement programs.

---

[99] This responsibility would, of course, also grow in proportion to the substantiality of the injury that could result from that practice, and in inverse proportion to the benefits from the practice.

[100] 2010 FTC Report at vi; *see alsa id.* at 40.

[101] Jack Marshall, DAA Steps Up Enforcement of Self-Regulatory Program, May 23, 2011, http://www.clickz.com/clickz/news/2073203/daa-steps-enforcement-self-regulatory-program

H. Private Ordering through Contract

Just as the White House Report acknowledges the importance of self-regulation, it also recognizes the critical importance of private ordering through contract to ensuring effective enforcement of privacy rules. Under the principle of Individual Control:

> When consumer-facing companies contract with third parties that gather personal data directly from consumers (as is the case with much online advertising), they should be diligent in inquiring about how those third parties use personal data and whether they provide consumers with appropriate choices about collection, use,and disclosure.[102]

And under the Accountability principle:

> Companies that disclose personal data to third parties should at a minimum ensure that the recipients are under enforceable contractual obligations to adhere to these principles, unless they are required by law to do otherwise. ... if a company transfers personal data to a third party, it remains accountable and thus should hold the recipient accountable—through contracts or other legally enforceable instruments—for using and disclosing the data in ways that are consistent with the Consumer Privacy Bill of Rights.[103]

Structured disclosures could help to promote compliance with such principles by making it more immediately evident (and potentially searchable) whether a company's partners abide by at least the same privacy protections. Or, structured disclosures could be used to identify who a company's partners are and directly link to their privacy policies.

IX. Privacy Regulation as International Trade Barrier

A final word about enforcement: selective enforcement may be a tool for invidious discrimination by national privacy regulators, most notably by European Data Protection Authorities against American companies. Yet neither the White House Report nor the FTC Report discuss the ways discriminatory enforcement of privacy laws against American companies burden international trade in data and the products and services enabled by data—or how to ensure that our own regulations do not do the same to foreign companies. In fact, the Administration has already recognized that privacy protections, however well-intentioned can, in fact, function as barriers to international trade. At last September's APEC meeting, U.S. Ambassador Phillip Verveer warned that privacy regulations that could slow adoption of cloud services:

> In these circumstances, we would expect every economy to welcome cloud services without regard to the national origin of their producers. But there are

[102] White House Report at 11

[103] *Id.* at 21.

> complications. One of the big ones is the limitations on trans-border data flows .... It is very important, however, that we not unnecessarily sacrifice the economic advantages inherent in cloud computing in our arrangements to protect personal privacy. Stated more directly, we should not let our quest for effective privacy mechanisms become a barrier to international trade in cloud services.[104]

This concept requires further conceptual development but it certainly deserves more attention.[105] It could also be the subject of a very productive workshop, perhaps convened by the Commerce Department.

---

[104] Patrick Ryan, *Cloud Services and International Trade*, Google Enterprise Blog, (Oct. 13, 2011), http://googleenterprise.blogspot.com/2011/10/cloud-services-and-international-trade.html.

[105] *See generally*, Bob Boorstin, *Promoting Free Trade for the Internet Economy*, Google Pub. Pol'y Blog (Nov. 15, 2010), http://googlepublicpolicy.blogspot.com/2010/11/promoting-free-trade-for-internet.html.

Mrs. BONO MACK. Thank you, Mr. Szoka.

Mr. Zuck, you are recognized for 5 minutes.

STATEMENT OF JONATHAN ZUCK

Mr. ZUCK. Chairman Bono Mack, Ranking Member Butterfield, distinguished members of the committee, thank you for holding this hearing and allowing me to participate.

I have, as the app trade association, get asked to talk about the app industry over and over again. And what is amazing is that every time I talk about it, the new figures surrounding the app marketplace continue to go up. Before we even reached previous projections of $8.3 billion that were supposed to happen by 2013, we are already at a $20 billion industry that is now projected to be $76 billion by 2015.

So as was mentioned earlier, the employment statistics that are fueled by this incredible growth are clear for everyone to see. And it is a small business phenomenon. Eighty percent of its marketplace is made up of small businesses, companies like Zco in New Hampshire and companies like InterKnowlogy in California and Computer Ways in Florida. So there is this dispersed and small business element to this that I think has to always persistently be acknowledged when discussing the potential impact of regulation.

I have had the opportunity to participate in many multi-stakeholder processes around the world. And despite that fact I am still interested in participating in the one being convened by the Commerce Department. If anything, it should be better than the sort of de facto regulation that comes to enforcement. If we take the example of Google Buzz that Chairman Leibowitz raised, that is a clear case where an enforcement action was brought, but instead of punishment being the result, the result was the bare bones of a regulatory expectation that has survived until today with their Do Not Track proposals that would in fact create a regulatory framework for everyone else that would benefit Google over its competitors. So that can't be the best outcome, especially when no one else had a say in how the proceedings would take place. Certainly a multi-stakeholder approach is a superior one.

But I guess my one hesitation, if you will, with the multi-stakeholder discussion as they are being currently proposed is the suggestion that we should begin the discussion with mobile apps. And certainly as the mobile app trade association, it is predictable I would say that. But I would guess I would say this is the area of the industry that is the newest, and the area of the industry that is most dynamic, and the area of the industry that is least understood. So as a practical matter the idea of beginning there seems ludicrous because it is the thing we know the least about and the thing we are in the least position to make decisions about. So the only real conclusion that I can draw it seems like the easiest group to try to impose regulations on, and I think that is the wrong way to approach this process.

The real issue has always been about data and we need to make sure, as the FTC pointed out, that that data is online and offline data and that it has do with it no matter how it is collected, but instead has to do with the conditions under which data can be collected, the conditions under which it must be stored both from a

security and a privacy standpoint and also conditions under which it can be shared.

There is an old saying that the memo makes the meeting. And so even though everyone is talking about nonbinding voluntary things that we also want legislation to support, it is tough for me to keep track of all of that. Even in that context the very fact that I am raising this issue first means that I am suggesting that this is the issue most in need of addressing. And that will already have an impact on consumer understanding of that marketplace.

At best there is the suggestion that this is the most important area to address and at worst the suggestion can be made that it is the only area that needs to be addressed, when the reality is it is data that is the most important. If the memo makes the meeting, the we start off the meeting with everyone trying to figure out how they are not supposed to be the ones being discussed. GM will certainly suggest that OnStar is not mobile technology, even though I would suggest that it is. Instead if we decide something like location data is the place that should be discussed first, then it will apply across the board.

Secondly, the memo makes the news. So you have the same sort of situation that says that we have suggested that this is the most important way of proceeding when in reality I think that to the extent there is consumer concern about privacy, as Chairman Leibowitz brought up, it has been more driven by large data breach failures by a few large players and persistent disregard for privacy by a few large players and doesn't have to really do with the mobile apps that seem to be the focus of attention currently.

So while I support the multi-stakeholder approach andI look forward to participating in it, I think it is really imperative to remember that the only way that a multi-stakeholder approach will work is if everyone has a stake in the outcome. If you don't have—otherwise we in the mobile app community are going to feel like we are the steak and everyone else is carrying around A1 sauce. So I would like to make sure that we focus on the data and not the technology it is collected.

Thank you.

[The prepared statement of Mr. Zuck follows:]

Testimony

of Jonathan Zuck
President
The Association for Competitive Technology

before the
Committee on Energy and Commerce
The Subcommittee on Commerce, Manufacturing, and Trade

on
Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?

March 29, 2012

Chairman Bono Mack, Ranking Member Butterfield, and distinguished members of the Committee: My name is Jonathan Zuck, and I thank you for holding this important hearing examining the various proposals for government regulation of personal privacy.

I am the president of the Association for Competitive Technology (ACT). ACT is an international advocacy and education organization for people who write software programs--referred to as application developers. We represent over 4,000 small and mid-size IT firms throughout the world and advocate for public policies that help our members leverage their intellectual assets to raise capital, create jobs, and innovate.

My goal today is to explain the evolving nature of the mobile application industry and how the Administration's proposed new privacy framework and its multi-stakeholder process offers both promise and challenges to continued innovation in this marketplace.

Specifically, app developers have three key messages for the members of the Committee:

1. **The app marketplace is still in its earliest growth stage, rapidly continuing to evolve.**
2. **The best way to address consumer privacy concerns is through a multi-stakeholder process producing voluntary, but enforceable, codes of conduct. However, it should avoid regulating technology instead of**

behavior and promote conditions to encourage the free exchange of ideas.

3. **App developers and industry organizations are adopting measures to improve consumer privacy protections and increase awareness of the potential uses of personal information.**

Evolution of the App Marketplace

I am often invited to speak on the subject of mobile apps and each time I do it seems new figures emerge about the growth trajectory of our marketplace. Just two years ago, total industry revenues were $3.8 billion and expected to rise to $8.3 billion.[1] At the close of last year we had grown to $20 billion and are projected to reach $76 billion by 2015.[2] This is a meteoric rise for an app economy that didn't even exist four years ago.

This is also a small business phenomenon. Over 88 percent of the top 500 app makers are small businesses.[3] And as small business is the engine of economic growth in our country, app makers are contributing greatly to the job market with half a million jobs created in this new marketplace.[4] These jobs can be found anywhere. Thirty percent are in the state of California – but the rest are spread out all across the country.

As a brand new industry, we are experiencing rapid changes in the marketplace with new business models emerging every year. Recently freemium apps and in-

[1] http://www.eweek.com/c/a/Mobile-and-Wireless/Apple-Google-Lead-38B-Mobile-App-Charge-IHS-512817/
[2] http://www.slideshare.net/joelrubinson/an3-us-appeconomy20112015
[3] http://Republicans.EnergyCommerce.house.gov/Media/file/Hearings/CMT/100511/Reed.pdf
[4] http://www.technet.org/new-technet-sponsored-study-nearly-500000-app-economy-jobs-in-united-states-february-7-2012/

app purchasing have become the favored means to monetize new releases.[5] Not long ago, paid downloads ruled the day. Through it all, developers are still exploring whether the advertising model can generate enough income on its own.[6]

While business models continue to evolve, developers are also experimenting with different platforms. Currently Apple's iOS provides the most dependable platform, but RIM has been aggressively wooing developers to Blackberry as its userbase in Asia and the Middle East remains strong.[7] Android continues to gain marketshare, though the platform suffers from fragmentation; and with dramatic changes coming in the new Metro user interface of Windows Phone 8, many software developers are porting their programs to that new mobile platform.[8]

Some very successful developers who are creating innovative apps come from the states of Members on this Committee. Companies like Zco Corporation whose latest release is PolicePad, an iPad-based system that can replace PC and telemetry systems in police cruisers at a fraction of the cost. Zco Corporation employs 20 people in New Hampshire making custom applications for a wide-range of consumer devices as well as 3D animations. Or Interknowlogy in Carlsbad, California which makes custom applications for the healthcare industry, government and non-profits like the San Diego Zoo. Or Computer Ways, Inc., in

[5] http://www.nytimes.com/2012/03/19/technology/game-makers-give-away-freemium-products.html?_r=1&pagewanted=all
[6] http://tech.fortune.cnn.com/2011/11/21/piper-jaffray-android-app-revenue-is-7-of-iphones/
[7] http://www.engadget.com/2012/02/03/RIM-free-BlackBerry-Playbook-Android/
[8] http://www.reuters.com/article/2012/03/20/mobile-developers-idUSL1E8EJAGT20120320

Deerfield Beach, Florida, which developed an app bringing the beauty of Florida coast to the Windows 7 phone.

With such a dynamic mobile ecosystem it is difficult to predict where the market is headed next and what industry standards will be adopted. This makes it difficult to implement a regulatory regime for the app marketplace. The industry is far from mature and activities or practices that regulators seek to address may no longer exist in their current form by the time new rules can be implemented.

The Multi-stakeholder Process Offers Promise as Well as Concerns

While the app marketplace is experiencing dramatic growth and innovation, concerns for consumer privacy online have grown. While most of the headlines have been earned by big companies operating in traditional internet commerce, the app industry has not been immune from privacy missteps. Various federal agencies have considered proposals to protect consumers' personal information including apps among their areas of concern.

The Administration recently published its proposed privacy framework, *Consumer Data Privacy in a Networked World*,[9] featuring several principles that ACT emphasizes in its recommendations for developers. Specifically, the Administration has identified seven areas of focus around which it has crafted a Consumer Privacy Bill of Rights. ACT advised the Administration during the drafting of this document

[9] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

and has been invited to participate in the multi-stakeholder process that is intended to produce a consensus agreement on a voluntary industry code of conduct. ACT strongly supports the concept outlined by the multi-stakeholder process proposed by the Administration. Bringing together representatives from industry, government, academia, and advocacy to collaborate in the development of voluntary codes of conduct provides the best opportunity to reach an agreement that works for everyone.

While we believe strongly in the industry's ability to implement self-regulatory measures, it is clear that bad actors deserve swift enforcement response. When reckless companies get attention for violating consumers' privacy rights it's bad for everyone's business. Developers only enjoy success in the marketplace when consumers have confidence in the safety of their personal information online.

For this reason ACT applauded the FTC when it exercised its existing enforcement authority to punish app makers violating the Children's Online Privacy Protection Act (COPPA). Just this week the FTC took action against app maker RockYou for misleading customers about their privacy and failing to maintain adequate data protection practices.[10] The FTC has also taken enforcement action against Playdom – now a Disney subsidiary – for violating COPPA, fining them $3 million,[11] and against a small app company, W3 Innovations, fining them $50,000 for similar

[10] http://news.cnet.com/8301-1009_3-57405308-83/rockyou-settles-with-ftc-over-charges-of-exposing-user-info/
[11] http://news.cnet.com/8301-13506_3-20062566-17.html

infractions.[12] These actions showed that the FTC is prepared to go after companies both large and small if they violate children's privacy.

These enforcement measures also showed that the Commission has sufficient authority in consumer privacy cases under COPPA and Section Five of the FTC Act. In testimony before the Senate Commerce Committee last year,[13] and again in Chairman Liebowitz's press conference earlier this week,[14] the FTC has confirmed it needs no new regulations as it already possesses sufficient authority. Voluntary adoption of codes of conduct will provide the Commission with additional opportunities to exercise that authority should the need arise.

While we are thankful to be part of the multi-stakeholder proceedings and believe it is critical that app developers have a role in these discussions, we have a few concerns about the process initiated by the National Telecommunications and Information Administration (NTIA). First, a comprehensive approach is the only way to address the issue of consumer privacy and it appears the NTIA has deviated from this path. Secondly, it is crucial for participants in this process to feel unfettered in their participation, free to engage in wide-ranging discussion and propose bold solutions. We believe the free exchange of ideas is likely be sharply curtailed by the format of the discussions.

---

[12] http://9to5mac.com/2011/08/15/w3-innovations-pays-the-ftc-50000-for-collecting-childrens-info-in-ios-apps/
[13] http://www.c-spanvideo.org/program/MobileTechn
[14] http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html#March_26_12

Consumers have raised privacy concerns across the broad spectrum of online properties so it makes little sense to target one technology sector. In fact, to do so is the cardinal sin of regulation. Anyone who works in the technology regulatory or legislative fields has heard the admonition, "regulate bad behavior not technology." Sadly, we are concerned this is the sort of step NTIA appears to be taking. Through its Request for Comment, the NTIA suggests it's necessary to convene an "initial multi-stakeholder process to facilitate the implementation of the Transparency principle in the privacy notices for mobile device applications."[15] This is intended to occur outside the broader industry framework and to precede any efforts to address the issue of privacy in a comprehensive fashion.

Singling out the work of an industry of small business developers is unnecessary and counterproductive. It sends a chilling message to entrepreneurs and startups and will have a devastating impact on innovation. Moreover, it is difficult to fathom why regulators want to devote all their attention to a technology overwhelmingly comprised of small businesses while big companies are in the headlines every month stoking the privacy fears of Internet users across the globe. NTIA needs to return its focus to the big picture of online privacy and leave behind ill-advised efforts to target specific technologies.

It is also necessary to sound a note of caution on the suggestion of a fully transparent multi-stakeholder process. It is important to remember that industry

[15] http://www.ntia.doc.gov/files/ntia/publications/fr_privacy_rfc_notice_03052012_0.pdf

participants will be searching for a resolution that involves compromise – compromise that could negatively affect their companies' bottom lines and attract criticism. In order for the best solutions to emerge in a consensus fashion, stakeholders must have confidence that the dialogue provides wide latitude to offer a range of alternatives.

If this process takes the form of a public discussion, industry participants will be looking over their shoulders or sitting on their hands instead of offering bold ideas for workable solutions. Fully transparent proceeding will not produce the free exchange of ideas and consensus agreement that is the stated aim of the stakeholder process. For NTIA to get the best results from these efforts, they need to value positive outcomes more than an open process.

As President of ACT, I have spent a considerable portion of my time in hotel conference centers around the world working on one of the biggest multi-stakeholder efforts of all time, ICANN. Additionally I've done my multi-stakeholder time at W3C, the EU Data Directive Safe Harbor provisions for US eCommerce Companies, WIPO on Discussions on Patent Law Harmonization and the EC working group on European Software Strategies. If there's one lesson I've learned, it's that multi-stakeholder processes move slowly; while industry moves to respond to customers within hours.

App Developers and Industry Groups Taking the Lead on Privacy

While federal regulatory bodies and multi-stakeholder groups have been considering measures to address consumer privacy, app makers have been learning about the issue and developing their own self-regulatory responses. App makers are particularly concerned with consumer confidence in the safety of private information because in the absence of this assurance they face reluctant customers.

The biggest hurdle to implementing industry-wide privacy standards is developer education. There are over 200,000 app developers in the United States. App makers want to do the right thing on privacy, but often don't know whether their app creates privacy concerns or what they need to do to be rules compliant. As most small business app developers are making customer-facing software for the first time, they are also addressing privacy issues for the first time. Matters typically handled by a legal department or chief privacy officer in a larger company are now most often handled by a small business owner.

Recognizing the need to boost developer education, ACT has been particularly active on this issue during the past twelve months. In addition to frequent meetings with lawmakers and regulators here in Washington, we have traveled around the country to speak at developer conferences to raise awareness about consumer privacy.[16]

[16] http://vimeo.com/34560160

While warning developers about possible new regulations, we have also helped to map out proactive steps they can take.

First and foremost, we advise app developers to be open with consumers about the information they collect and how it is used. We strongly advocate the use of privacy policies – even if an app maker believes no information is being collected. It is also important that this information is presented to users in a meaningful way so that they may easily comprehend it. On mobile devices this means that the information provided must be simple and clear enough to fit on a small screen.

ACT also advises app developers to be mindful of the relationships they have with third parties such as ad networks. App makers must be aware that the SDKs (software development kits) supplied by platform providers or ad networks may contain code that uses consumer information in ways they hadn't considered. Even if the developer never sees the data which passes straight through to an advertiser, the responsibility still lies with the app maker to inform the user what information is shared and how it is being used. Additionally, developers should ensure that they collect only as much information as is needed. When this information is no longer required, it should be de-identified.

ACT is committed to identifying self-regulatory methods to address this problem and we work with developer groups dedicated to finding their own solutions. One such affiliate group is Moms with Apps, comprised of more than one thousand

children's app makers. These developers are parents who decided to make apps to educate their children. They are conscious of privacy concerns and the collection of data because the last thing any of them want is to expose their own children's private information.

Moms With Apps Privacy Icon

Because of this concern, independent developers in Moms with Apps took the initiative to design a parental notification system that identifies the privacy settings of an app in a simple, easy to identify graphical display. While this isn't a final solution, it's a great step initiated from within the industry to safeguard user privacy.

In addition to the initiative shown by these app-making parents, other efforts have also been undertaken by industry to provide improved consumer access to privacy information. To address the accessibility of privacy policies, groups like TRUSTe[17] and PrivacyChoice.org[18] have begun offering privacy policy generators. Developers simply fill out a survey explaining the functions of their app and a privacy policy is automatically generated. This is a useful option for startups that can't afford legal staff. The resulting privacy policy is generated in both the long form that we are

[17] http://www.truste.com/products-and-services/small_medium_business_privacy/privacy_policy_generator.php
[18] http://www.privacychoice.org/resources/policymaker

accustomed to seeing (and seldom reading) as well as a more easily digestible version composed of simplified language. The other benefit of these services is that they customize the end product to appear on a small screen.

Tip the Balance?

The question posed for this hearing is whether the Administration's consumer privacy efforts tip the balance at the expense of innovation. At this time, we are hopeful that the concerns we have expressed don't tip the balance against innovation. ACT is committed to the multi-stakeholder process as an effort to improve industry efforts to protect consumer privacy. We recognize that consumer confidence in the safety of their privacy is necessary for app makers to effectively market their products. We will continue to work through this process, and with the members of this Committee, to improve these efforts.

ACT does, however, find serious shortcomings in the process outlined by the Administration for the multi-stakeholder proceedings. Targeting apps – a single technology – outside the general framework of the process is troubling and a cardinal sin of technology regulation. Isolating the industry sector composed primarily of small businesses disproportionately favors the larger companies that have repeatedly given consumers the most reason to be worried about their privacy. Additionally, suggesting that negotiators conduct proceedings without any privacy

will discourage industry participants from fully engaging in the process making consensus an elusive goal.

We will continue to convey our position on these matters during the multi-stakeholder process and encourage the Administration to make the necessary adjustments to fix these provisions.

Thank you for the opportunity to appear before the Committee today and I look forward to addressing any questions you may have.

Mrs. BONO MACK. Thank you, Mr. Zuck, for the sound byte of the day. And Ms. Horan, you are recognized for 5 minutes.

STATEMENT OF PAM HORAN

Ms. HORAN. Chairman Bono Mack, Ranking Member Butterfield, and distinguished members of the subcommittee, thank you for the opportunity to speak with you today. My name is Pam Horan, and I am the President of the Online Publishers Association.

The OPA is a trade association that represents the online content community and its unique role in the future of media. Our members include some of the most respected online publishing brands from Gannett, the New York Times, CBS interactive to Washington Post, Time, Inc. and Disney Interactive media, to name a few. OPA members are the public face of the Internet with well established track records of integrity and quality. Many of our members serve a critical role in a functioning democracy to gathering and distribution of news and information.

OPA members have long understood the need to respect and protect consumer privacy. These trusted brands hold a direct first party relationship with their consumers. They must maintain confidence in their brands to attract the large audiences necessary to compete in the advertising marketplace.

With thousands of alternative Web sites just a click away, there are a multitude of places online for consumers to easily get their news, information and entertainment, especially if they don't trust a Web site's privacy practices.

Both the Department of Commerce's Consumer Privacy Bill of Rights and the FTC's privacy report that was released this past Monday recognizes that companies do not need to provide choice before collecting and using consumer data for practices that are consistent with context or consumer expectations.

A good example is if a user might visit CNET.com, a leading source of technology product reviews, to research 3–D TVs. As a user is reading a review of Sony's newest 3–D TV CNET might show a list of similar products viewed by others who also read that review. Consumers expect and want publishers to offer additional content that enhances their Web site experience.

Last year our members invested over three-quarters of a billion dollars in the production and creation of high quality online content. Given the infancy of the industry and the economic challenges facing the publishing businesses, it is important to continue to allow publishers to monetize their investment, especially when their efforts meet consumer expectations.

We are encouraged by several of the principles contained in the Consumer Privacy Bill of Rights. One is the respect for context. That principle supports that first party data collection practices fall within consumer expectations and consumers trust first parties to collect and use their data appropriately.

Second is the access and accuracy principle, which recognizes that a consumer's right to being assess the data a company holds could have First Amendment implication. OPA members play a critical role in gathering and distributing news and information, which is necessary for a vibrant democracy. We appreciate that the

administration notes that this principle should be interpreted to respect the freedom of the press.

There are several other aspects of Consumer Privacy Bill of Rights which are of concern. The report urges consumer facing companies such as publishers to disclose not only their own data collection and use practices but also those of their business partners. Publishers are actively working to monitor and track the data collection activities of third parties on their Web sites in order to protect their consumers. However, based on the complex and dynamic nature of the Internet and the sheer number of partners and service providers, this is a daunting task. The obligation to disclose practices of other parties implies that publishers would be responsible for violations by these other parties. We believe that, as in the case of the DAA self-regulatory program, each entity that collects and uses data is and should be accountable.

Also, the Bill of Rights urges companies to provide consumers with a reasonable way to access all data that a company holds about them while providing appropriate privacy protections. This presents significant technical challenges that could actually increase risk to consumers in the end.

The OPA has worked closely with our colleagues in the DAA to create a self-regulatory regime to provide transparency and choice for consumers. Online privacy is different for every individual and the DAA self-regulatory program accommodates those individual choices with ease.

Self-regulatory models such as the one developed by the DAA can more efficiently adapt to technological innovation and evolving consumer needs, thereby offering the most effective privacy protection. Ultimately we believe industry self-regulatory program can more quickly and effectively deliver privacy protections for consumers than a legislative or regulatory approach.

Thank you for the opportunity to share the perspective of first party publishers with you today. I look forward to answering any questions you may have.

[The prepared statement of Ms. Horan follows:]

Statement of Pam Horan
President,
Online Publishers Association

before the
House Energy and Commerce
Subcommittee on Commerce, Manufacturing and Trade

Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?

March 29, 2012

Madame Chairwoman, Ranking Member Butterfield and Distinguished Members of the Subcommittee, thank you for this opportunity to speak with you today.

The Online Publishers Association (OPA) is a trade association that represents the digital content business and its unique role in the future of media. Our members include many of the Internet's most respected online publishing brands reaching an unduplicated audience of 220.4 million unique visitors or 100% reach of the U.S. online population monthly (comScore Media Metrix, December 2011).

OPA members include many of the nation's leading online media companies such as The New York Times, Washington Post Digital, Time Inc., Disney Interactive Media Group, Forbes.com, CBS Interactive and Discovery Communications to name a few. OPA members are the public face of the Internet with well-established track records of integrity and quality. Many of our members serve a critical role in a functioning democracy – the gathering and distribution of news and information.

Consumer Trust

OPA members have long understood the need to respect and protect consumer privacy. These trusted brands hold a direct, first party relationship with their consumers and therefore, must maintain confidence in their brands to attract the large audiences necessary to be competitive. With millions of alternative websites just a click away, consumers have a multitude of options and can easily obtain their news, information and entertainment elsewhere if they don't trust a site's privacy practices.

The Federal Trade Commission (FTC) again recognized this unique first party relationship in the report it released this past Monday, March 26, 2012, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers." The report noted that consumers hold different expectations of privacy with respect to information collected in the context of a direct first-party relationship with a website publisher than they do with respect to information collected by third parties in the online ecosystem.

In turn, the FTC recognizes that, as first parties, publishers provide an enhanced consumer experience including site optimization and personalization and the delivery of more relevant content through the collection of data.

Self Regulatory Programs Underway

In an effort to further improve consumer trust online, the OPA has worked closely with our colleagues in the Digital Advertising Alliance (DAA) to create a self-regulatory regime to provide transparency and choice for consumers. Self-regulatory models, such as the one developed by the DAA, can quickly and

efficiently adapt to changing landscapes and new business practices thereby offering the most effective privacy protection for consumers.

Under the DAA program, consumers can opt-out of being served behaviorally-targeted advertisements. In addition, data that is collected cannot be used to determine a consumer's eligibility for employment, credit standing, healthcare treatment and insurance. Also, under the DAA program, all entities on the Internet are responsible for their own actions. This important provision ensures that everyone in the ecosystem that collects and uses data is accountable. This is the most effective way for us to regulate our industry.

The DAA program has shown promising results since it was officially launched in the fall of 2011. The opt-out program is easy to identify with the power "i" icon, easy to understand and easy to use. The power "i" icon appears in nearly 1 trillion ads per month. All of the top 15 ad networks are in compliance. As more and more consumers become aware of the power "i" icon and the choices available to them, we are confident that the self-regulatory model will prove to be highly effective in addressing the privacy concerns of consumers. Online privacy is different for every individual and the DAA's self-regulatory program accommodates those individual choices with ease.

White House Consumer Privacy Bill of Rights

On February 23, 2012, the White House released a report entitled "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy." Within the report, the Administration advocates seven core principles, collectively called the Consumer Privacy Bill of Rights. They are as follows:

- *Individuol Control*: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- *Transparency*: Consumers have a right to easily understandable and accessible information about privacy and security practices.
- *Respect for Context*: Consumers have a right to expect that companies will collect, use and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- *Security*: Consumers have a right to secure and responsible handling of personal data.
- *Access and Accuracy*: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
- *Focused Collection*: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- *Accountability*: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

The OPA would like to highlight two principles that are particularly encouraging to publishers.

The "Respect for Context" principle emphasizes the critical role that context plays in shaping consumer expectations and the need for companies collecting consumer data to honor those expectations: "*Generally speaking, companies should limit personal data uses to fulfilling purposes that are consistent with the context in which consumers disclose personal data*." This principle supports the OPA position

that first party data collection practices fall within consumer expectations and consumers trust first parties to collect and use their data appropriately. The report concludes that "companies may infer consent to use personal data to conduct marketing in the context of most first-party relationships, given the familiarity of this activity in digital and in-person commerce, the visibility of this kind of marketing, the presence of an easily identifiable party to contact to provide feedback, and consumers' opportunity to end their relationship with a company if they are dissatisfied with it." In addition, the report suggests that companies should be able to infer consumer consent to collect personal data for a range of purposes "that are common, even if they may not be well known," such as analytics, fraud prevention, compliance with legal obligations and the protection of intellectual property.

For example, a user might visit CNET.com, a leading source of tech product reviews, to research 3D televisions. As the user is reading a review of Sony's newest 3D television, CNET might show a list of similar products viewed by others who also read this review. Consumers expect and want publishers to offer additional content that may be valuable, ultimately enhancing their website experience.

In addition, consumers expect that first parties will collect and use information to optimize and subsidize online advertising. Last year, our members invested over $750 million in the production and creation of high-quality digital content. Ultimately, the future of the online publishing industry will depend on our ability to continue to compete successfully in the online advertising marketplace. To remain competitive, publishers must continue to have the flexibility to develop innovative and effective advertising services for advertisers while also continuing to attract large Web audiences to our digital properties. Given the infancy of the industry and the economic challenges facing the publishing business, it is important to continue to allow publishers to monetize their investment, especially when their efforts meet with consumer expectations.

The "Access and Accuracy" principle recognizes that a consumer's right to access the data a company holds could have First Amendment implications. As OPA pointed out in its comments to the Department of Commerce in January 2011, "any choice or consent requirement...should clearly exclude the collection of information for newsgathering, political commentary and other forms of editorial expression that are protected as core speech." OPA members play a critical role in gathering and distributing news and information, a role that is key to a functioning democracy. As such we are pleased the report notes that "individuals and members of the press exercising their free speech rights may well speak about other individuals and include personal information in their speech" and therefore concludes that "[t]he Access and Accuracy principle should . . . be interpreted with full respect for First Amendment values, especially for non-commercial speakers and individuals exercising freedom of the press."

Despite these positives, however, the OPA must note concerns with other portions of the Consumer Privacy Bill of Rights.

The report urges consumer-facing companies, such as publishers, to disclose not only their own data collection and use practices but also those of their business partners and service providers. Publishers are actively working to monitor, track and limit the data collection activities of third parties on their websites in order to protect their customers. However, based on the complex nature of the Internet today, the number of partners and service providers changes frequently and dynamically, making this a daunting task. The obligation to disclose practices of other parties implies that publishers would be responsible for violations by these other parties which would be an unworkable model. We believe that,

as in the case of the DAA's self-regulatory program, each entity should be held responsible for its own actions.

The Access and Accuracy principle "recognizes that the use of inaccurate personal data may lead to a range of harms." Accordingly, the report urges companies that collect consumer data to "provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation." The burden imposed by this obligation is amplified by the report also requiring that whatever mechanisms companies create to allow consumers to review and correct data "should not create additional privacy or security risks." Allowing all consumers to access whatever data companies have about them, while ensuring that those who access the data are the very consumers (and only the very consumers) to which the data pertain, presents significant technical challenges and could actually increase risk to consumers.

In summary, while we appreciate many elements of the Administration's proposal, as we have noted, there are aspects which are of concern. Ultimately, we believe industry's self-regulatory program can more quickly and effectively deliver privacy protections for consumers than a legislative or regulatory approach.

Conclusion

Thank you for the opportunity to present the perspective of online publishers. We appreciate the Committee's leadership role on consumer privacy issues and we look forward to continuing to work with you.

Mrs. BONO MACK. Thank you very much. Mr. Zaneis, you are recognized for 5 minutes.

STATEMENT OF MICHAEL ZANEIS

Mr. ZANEIS. Thank you very much, Chairman Bono Mack and Ranking Member Butterfield, for this opportunity to testify before you on these important issues today. My name is Mike Zaneis.

Mrs. BONO MACK. Please pull your microphone closer.

Mr. ZANEIS. My name is Mike Zaneis, and I am the Senior Vice President and General Counsel for the Interactive Advertising Bureau. IAB represents more than 500 leading new media companies. That includes the largest Internet portals and search engines, traditional newspapers and magazines, television broadcasters who are migrating their content to the digital world. And increasingly that includes the smallest players in this ecosystem, the mom and pop small publishers that constitute the long tail of Internet. But the thread that binds them all together is they depend upon digital advertising, the advertising revenue that allows them to invest in creative new content and innovative services, almost all of which are available freely to consumers.

So I would also like to take this opportunity to congratulate President Obama's administration and the Federal Trade Commission on the release of their respect of privacy reports recently. We are especially gratified when both reports recognize the tremendous success of industry self regulation in the consumer privacy arena.

Some 4 years ago IAB joined with our sister trade associations, the 4As, the ANA, DMA and in conjunction with the Council of Better Business Bureaus to create the most comprehensive, digital consumer privacy self-regulatory program. We were especially proud to be asked to participate, as you were, Chairman Bono Mack, on February 23rd when the White House held a press conference to release their privacy report. The DAA was held up as a model of success for what they call enforceable codes of conduct. Similarly, the FTC has recognized the great progress that we have made in self-regulation. And I think that all of this praise is with great merit.

I would like to share a couple of data points with you, metrics of success if you will. As Chairman Leibowitz testified to earlier today, the DAA program is transforming the way consumers receive information about how data is collected and used about them online. The ad choices icon, that little blue triangle with an "I" in it that you are seeing all over the Internet is being served within more than 1 trillion ads every month. Let me repeat that, more than 1 trillion ads every month contain this new notice provision. It is easy, it is easily discoverable for consumers. They can click on the icon and within 2 or 3 sentences they can understand how data is being collected about them. This is revolutionary.

Of equal importance is the fact that within that simple notice they can click through to the consumer choice page. And that is a simple, one-stop shop mechanism for consumers to opt out of having data collected about them. That is key. We have over 93 third-party entities participating in the DAA consumer choice page. It covers well over 90 percent of the ecosystem.

The last statistic I would like to share with you is through the Council of Better Business Bureaus' enforcement program we are covering 100 percent of the digital advertising ecosystem. That is because the BBB doesn't just enforce against IAB members or DAA members. No, they enforce against every party throughout the supply chain, and that is key because we know any self-regulatory program is only as strong as the enforcement mechanism behind it.

I think that this track record of success is what I would like to really focus on with the last minute I have here because there is a cautionary tale in each of these privacy reports as well. We want to ensure that any additional enforceable codes of conduct that are developed really build off track record of success self-regulation proven recently. Instead of displacing it we should build on that.

Secondly, I want to make sure before government entities call for new government burdens and requirements, that they have identified specific concerns and that they have well targeted legislative proposals to address those concerns.

Lastly, I would like to point out one provision that we have great concern with in the Federal Trade Commission's report, and that is this new call for data broker legislation.

I think we need to realize the FTC has given great praise to self-regulation with one hand and we want to make sure that they don't take that away by having an overly broad definition of data broker. In this day and age in the digital economy we have to realize that every publisher, every marketer, every ad agency, every advertising network and every analytics firm that is operating on the Internet transacts in data. We have to understand that in this information economy data is the new currency.

With that, I look forward to working with the subcommittee and the full committee, the Commission and the administration as we move forward on these issues. And I look forward to taking any questions you may have.

[The prepared statement of Mr. Zaneis follows:]

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE

OF THE

HOUSE COMMITTEE ON ENERGY AND COMMERCE

HEARING ON

"BALANCING PRIVACY AND INNOVATION:

DOES THE PRESIDENT'S PROPOSAL TIP THE SCALE?"

MARCH 29, 2012

TESTIMONY OF

MICHAEL ZANEIS

SENIOR VICE PRESIDENT AND GENERAL COUNSEL

INTERACTIVE ADVERTISING BUREAU

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 Michael Zaneis. I am Senior Vice President and General Counsel of the Interactive Advertising Bureau ("IAB"). Founded in 1996 and headquartered in New York City, IAB (www.iab.net) represents over 500 leading companies that engage in and support the sale of interactive advertising, including prominent search engines and online publishers. Collectively, our members are responsible for selling over 86% of online advertising in the United States. IAB educates policymakers, consumers, marketers, agencies, media companies and the wider business community about the value of interactive advertising. Working with its member companies, IAB evaluates and recommends standards and practices and fields critical research on interactive advertising. IAB has also led, with other prominent trade associations, the development and implementation of cross-industry self-regulatory privacy principles for online data collection, which is the program known as the Digital Advertising Alliance ("DAA").

The IAB appreciates the Subcommittee's interest in exploring how consumer privacy concerns should be balanced with consumers' desire for innovative products and services. We believe that industry self-regulation, coupled with consumer education, is the best way to strike this balance. Industry self-regulation is flexible and can adapt to rapid changes in technology and consumer expectations, whereas legislation and government regulation can stifle innovation.

I. Benefits of Online Advertising

The Internet is a tremendous engine of economic growth. It has become the focus and a symbol of the United States' famed innovation, ingenuity, inventiveness, and entrepreneurial spirit, as well as the venture funding that follows. Simply put: the Internet economy and the interactive advertising industry creates jobs. A 2009 IAB 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]

Advertising fuels the Internet economic engine. 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. Because of advertising support, consumers can access a wealth of online resources at low or no cost. These advertising-supported resources have transformed our daily lives. The support provided by online advertising is substantial and growing despite the difficult economic times. In the first half of 2011, Internet advertising revenues reached a new high of $14.9 billion, an impressive 23% higher than the same period the previous year.[3]

---

[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] 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 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. 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.

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

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. I will be updating the Subcommittee on the tremendous efforts of our industry 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.

II. Industry Self-Regulation of Online Data Practices

A. Implementation Update on Digital Advertising Alliance

Today, I would like to highlight for the Subcommittee the latest developments in the DAA Self-Regulatory Program for online data collection, which was recently recognized by the White House as "an example of the value of industry leadership as a critical part of privacy protection going forward"[4].

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

The DAA initiative was led by the IAB along with other leading trade associations: the American Association of Advertising Agencies ("4A's"), American Advertising Federation ("AAF"), Association of National Advertisers ("ANA"), and Direct Marketing Association ("DMA"). Our trade associations collectively represent more than 5,000 U.S. corporations across the full spectrum of businesses that have shaped and participate in today's media landscape. Our record amply demonstrates the merits of industry self-regulation.

As the Subcommittee has heard in prior testimony, the Self-Regulatory Principles for Online Behavioral Advertising ("OBA Principles") were released in July 2009, following a roadmap set forth by the Federal Trade Commission.[5] Following additional dialogue with the Commission, in November 2011, the DAA extended the OBA Principles with the release of the Self-Regulatory Principles for Multi-Site Data ("MSD Principles"). The MSD Principles establish comprehensive self-regulatory standards governing the collection and use of "multi-site data," defined as data collected from a particular computer or device regarding Web viewing over time and across non-affiliated Websites. The MSD Principles build on the DAA's existing implementation and accountability efforts, including the enforcement programs administered by the DMA and the Council of Better Business Bureaus ("CBBB").

The DAA's distinctive Advertising Option Icon is a key feature of the Self-Regulatory Program. Launched in 2010, the Advertising Option Icon is now a familiar sight across the Internet. Participating companies serve the Icon in or around advertisements as a uniform way to

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

provide consumers with transparency and choice in compliance with the Self-Regulatory Principles.

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

- The Icon is being served in nearly 1 Trillion ad impressions per month.
- We believe that the DAA program now covers over 90% of the online behavioral advertising being delivered, based on the participation of the top 15 U.S. ad networks.
- Today, the DAA program has more than two thousand companies licensed to use the Advertising Option Icon ("Icon") (including leading global advertisers like American Express, AT&T, Disney, General Motors and Kraft Foods). Not only is the DAA working directly with large publishers – it has also forged innovative partnerships to enable small business publishers to display the Icon on their web sites for free.
- The DAA's AboutAds website (www.aboutads.info) provides consumers with information about online advertising and provides an easy-to-use opt out mechanism. There have been over 5 million page views at AboutAds.info since its inception about a year ago.
- Shortly after the launch of AboutAds.info, in December 2010, there were about 4,300 page views per week, with 36% of visitors to Aboutads.info coming from the Icon. At

this time, there are approximately 520,000 page views per week, a dramatic increase that is tied directly to the broad adoption and proliferation of the Icon.

- In November 2011, the CBBB announced its first enforcement cases.
- In December 2011, the DAA began to offer tools that enable persistent consumer opt outs in Chrome and Firefox browsers. The DAA released a persistency tool for users of Internet Explorer in March 2012.
- In January 2012, the DAA launched an education campaign to inform consumers about interest-based advertising and how to take greater control of their online privacy. This multi-phase online campaign, designed by McCann Erickson Worldwide, includes banner advertising that directs consumers to the DAA's Icon and links to a new, informational website, www.youradchoices.com, which features three educational videos and a user-friendly consumer choice mechanism. The website has already had over 2.3 million page views since its launch. To continue driving traffic to this website, the DAA has secured nearly 2 Billion pro bono ad impressions from companies participating in the Program.

We expect that the DAA Self-Regulatory Program will continue to adapt over time to respond to changes in technology and consumer concerns. Currently, the DAA has convened a subcommittee of its Communications and Advisory Committee that is working to extend the Principles to the mobile ecosystem.

B. Benefits of Industry Self-Regulation

The IAB's commitment to self-regulation has put us at the forefront of new consumer protection initiatives. The IAB believes that self-regulation is the appropriate approach for addressing the interplay of online privacy and online advertising practices. This approach has been successful in addressing consumer concerns while ensuring that the U.S. Internet economy can continue to thrive. Self-regulation provides industry with a nimble way of responding to new challenges presented by the evolving Internet ecosystem. For our information-driven economy to thrive and continue as an engine of job creation, self-regulation led by industry codes of conduct is the ideal way to balance privacy and innovation.

Based on the IAB's commitment to advancing industry self-regulation, we are concerned about some of the proposals recently put forward by the Obama Administration and the Federal Trade Commission in their respective consumer data privacy frameworks. In particular, both the Administration and the Federal Trade Commission have called for comprehensive legislation in the area of consumer data privacy. The IAB does not believe that such new legislation is needed at this time. There has been no demonstration that legislation is needed or any evaluation of legislation's likely impact on this leading area of American job creation. IAB is concerned that laws and regulations are inflexible and can quickly become outdated in the face of evolving technologies. When this occurs, legislation thwarts innovation and hinders economic growth.

Formal rules can also serve as a disincentive to the marketplace to innovate in the area of privacy. Companies are increasingly offering consumers new privacy features and tools such as sophisticated preference managers, persistent opt outs, universal choice mechanisms, and

shortened data retention policies. These developments demonstrate that companies are responsive to consumers and that companies are focusing on privacy as a means to distinguish themselves in the marketplace. IAB believes that this impressive competition and innovation should be encouraged. New laws or rules could impede future developments or discourage companies from continuing to compete over privacy features.

III. Remarks on the Federal Trade Commission Framework

The IAB is similarly concerned that new proposals put forward this week by the Federal Trade Commission could impede economic growth and innovation. In particular, I would like to highlight for the Subcommittee the potential negative consequences of the Commission's call to single out "data brokers" for new restrictions.

The term "data broker" has no widely accepted definition, and the definition proposed in the Commission's framework is extremely broad. The Commission defines a "data broker" as a company that collects information from a variety of sources for the purpose of reselling such information to customers for purposes including marketing.[6] This definition is far broader than the definition contained in the prior legislation referenced in the Commission's report. In fact, virtually every publisher site, advertiser, ad network, or analytics firm collects or shares data with other parties in order to make the digital economy work, and would be at risk of falling within the category proposed by the Commission.

[6] FTC Report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers" (March 2012).

Data access legislation based on such an expansive definition could harm the most fundamental operations of the Internet. As the Commission itself recognizes in its report, "the costs of providing individualized access and correction rights [for data used solely for marketing purposes] would likely outweigh the benefits."[7] Online advertising data is not generally personally identifiable and is not generally maintained in a format that would be meaningful to consumers. Providing individual access and correction rights for such data, for most companies operating today, would be prohibitively costly and could require the collection of personally identifiable information that would not otherwise be collected. Thus, to avoid unintended and counterproductive outcomes, it would be essential to carefully and narrowly define the entities that would be covered by any new legislative or self-regulatory proposals aimed at "data brokers."

IV. Development of Industry Codes of Conduct

As the Administration considers the appropriate approach for facilitating stakeholders' development of privacy codes of conduct, the IAB believes that it is essential to build on – rather than undermining – effective self-regulatory initiatives that already exist.

A. Survey of Existing Self-Regulation

First, the Administration, through the National Telecommunications and Information Administration ("NTIA"), should target only those issues that are not subject to existing statutory regimes or self-regulatory programs. This would serve two main purposes. It would allow NTIA to identify and replicate the common attributes among initiatives that have resulted in

[7] *Id.* at 65.

successful standards and programs. In addition, this type of survey would help NTIA to ensure that the multistakeholder process is not revisiting areas that are already covered by existing codes.

The business community has invested significant resources to develop effective codes of conduct and accountability mechanisms to address specific privacy concerns. It is important that the Administration avoid disrupting these existing industry codes in order to avoid consumer confusion and duplicative or contradictory obligations for businesses. For instance, the IAB has established a Member Code of Conduct, to which all IAB members are required to adhere.[8] Our Code builds on the DAA's Self-Regulatory Program, which establishes principles for the collection and use of Web viewing data for purposes such as online behavioral advertising.[9] These are among many industry initiatives that have resulted in robust, voluntary programs that promote best practices designed to protect consumers while fostering economic growth and market innovation. The NTIA should not in any way interfere where there are already industry developed standards in place.

B. Room for Private Negotiations

Second, NTIA should take steps to foster industry participation in the proposed process, specifically by recognizing the important role of private negotiations. The Administration has proposed an open and transparent process to develop codes of conduct. This goal should be balanced with ample room for companies to engage in private discussions. In the IAB's

[8] IAB Website, "IAB Member Code of Conduct," available at http://www.iab.net/public_policy/codeofconduct.
[9] Digital Advertising Alliance Website, available at www.aboutads.info.

experience as a leader of self-regulatory initiatives, such private negotiations promote the frank exchange of ideas and can help participants to reach consensus despite divergent views.

Companies operate in competitive marketplaces. They have little incentive to share proprietary information in a public forum, especially when other participants have a history of using information against companies as a basis for litigation or media scrutiny. Thus, while some stages of the multistakeholder process may present periodic opportunities for transparency, such as to solicit feedback, the IAB encourages the Administration to structure a process that emphasizes private discussions among industry representatives.

C. Industry Leadership

The IAB's experience also shows that industry leadership in drafting codes is important to achieving a workable balance of privacy and innovation. The business community is in a unique position to understand both technological limitations and consumer expectations. These insights are critical to create effective but feasible standards that can be adopted and implemented broadly by industry.

The example of the DAA Self-Regulatory Program illustrates the merits of industry negotiation and leadership. Hundreds of companies, including IAB members, are now participating in this program. In line with the Administration's vision for codes of conduct, the underlying Self-Regulatory Principles were generated through a multistakeholder process involving 11 trade associations and 25 companies that met regularly to achieve consensus. Discussions were largely private with input provided at appropriate stages by government agencies and private advocacy groups. This effort, which has been universally applauded,

resulted in comprehensive principles and the unique Advertising Option Icon to foster consumer-friendly standards across the Internet data ecosystem. This model demonstrates the potential for codes of conduct to attract widespread voluntary participation. This was done without government funding or government-convened forums.

D. Government Role as Facilitator

NTIA should have a limited role in the multistakeholder process. The Administration has stated that "the stakeholders themselves will control the process and its results."[10] We urge the Administration to adhere to its commitment that the agency will not substitute its own judgment when stakeholders are developing codes of conduct.[11] As the White Paper states, "there is no Federal regulation at the end of the process."[12] Thus, to achieve the voluntary adherence sought by the Administration, the IAB believes that industry leadership will provide the best opportunity for success.

* * *

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

---

[10] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* 24 (February 2012) (hereinafter "White House Framework").
[11] *Id.* at 27.
[12] *Id.* at 24.

Mrs. BONO MACK. Thank you very much.

Mr. Brookman, welcome. And you are recognized for 5 minutes.

STATEMENT OF JUSTIN BROOKMAN

Mr. BROOKMAN. Thank you, Madam Chairman, Ranking Member Butterfield, members of the committee. Thank you very much for the opportunity to testify in today's hearing. I think you have chosen a really apt title for this hearing. Privacy and innovation are two issues that are very near and dear to CDT's heart. They are both vitally important and I think it is fair to say we probably failed so far in obtaining both of them for consumers.

However, I want to stress that privacy and innovation are not opposite ends of the spectrum. Innovation and privacy are not a zero sum game. To the contrary, invasion thrives in an environment of trust. And the assurance of privacy is integral to consumer trust and new technologies.

I think over the past couple of years we have started to reach a tipping point where consumers have developed considerable mistrust about how their information is being collected and used both online and off. I can refer you to my written testimony for just a handful of any number of recent studies demonstrating that modern consumers are very, very worried about privacy and in many cases are resisting adoption of technology such as location base services and mobile banking applications because of concerns about protection of their personal information.

In short, if consumers are unable to trust this increasingly complex network of innovative services, then innovation itself will suffer. For this reason we have seen a number of leading companies step forward and say the United States needs a flexible comprehensive privacy law.

Two years ago before this subcommittee was Intel and Microsoft, who testified in a hearing about their support for privacy legislation and the need for clear and consistent consumer protections to encourage the adopting of cloud computing technologies. But it is also increasingly emerging niche players in smaller and developing markets who stand to benefit from increased consumer trust of a result of consistent privacy standards. So recently the chief strategy officer of the Honda Group, which is a consulting firm for facial recognition and digital signage companies that evaluate consumer faces in public and try and decide what ads to show to them, argued that our industry needed a legislative solution on privacy, saying that whether through an expansion of the Electronic Communications Privacy Act or under entirely new privacy legislation I believe that clear and concise rules regarding what can and cannot be collected and/or communicated through digital media and integration will minimize unnecessary confusion, vulnerabilities and liabilities to consumers, network operators and deployers.

Now this is an industry at the bleeding edge of technology arguing for baseline rules to promote trust in their products. In fact CDT has worked really closely with members of this industry to develop voluntary codes of conduct to promote that trust. So far it is just the self-regulatory standards not everyone has to follow. And there is concern that leading actors will try to do the right thing to promote trust in the ecosystem but the smaller free riders who

are not as publicly known or don't have a consumer effacing side will fail to follow those same rules and will be able to coast on and consume that goodwill from self-regulation. That is from those who have agreed to protect consumers' privacy.

So for these reasons CDT has been really supportive of the idea of comprehensive privacy legislation both to protect consumers' rights, but also to foster confidence they can engage with and adopt new services and technologies without worrying that they have no idea and no way to find out what is happening with their personal information.

I think the goal that legislation is trying to achieve here, I hope not controversial, is to treat user information reasonably, to follow the basic principles of transparency about practices, but not requesting or retaining more information than you need, giving users some measure of control over what happens to their information. The hard question has always been how do you take these high level ideas and turn them into operational rules or reverse business practices and technologies and industries. And how do you give companies certainty that their practices will be deemed appropriate? You could have very prescriptive technology specific legislation which would have to be updated constantly like the Tax Code. At CDT we push against that approach because we don't think statutory law should mandate particular technological solutions and that law will have trouble keeping pace with the technological innovation.

The value of the voluntary code of conduct approach is that industry will have a key role in taking a hand at developing the specific rules that they will be following because they typically have the most knowledge about how the technology works and what will and will not be practical. We believe this is the best way to create certainty for companies and encourage privacy innovation over time and reward the adoption of accountable practices.

Another way to do it could be through FTC rulemaking and enforcement powers and useful backstops. But I think the preferable ideal approach is for stakeholders to come together to develop reasonable, rational flexible rules for industry players that they can rely upon as they develop new ad innovate consumer services.

Now we have some concerns about whether this multi-stakeholder process will work without substantive law in place, that you need to get soft safe harbor compliance, deemed compliance for. Ultimately I think it will be necessary for legislation to incentivize companies to come to the table to work on these industry wide codes of conduct. However, we understand the administration's desire to move forward giving consumer concern about privacy. And we are hopeful that there are some areas where there are sufficient incentives to get everyone to the table to agree to good strong reasonable privacy rules. If that happens we can make substantive progress on privacy now and we will have a model that should inform the shape of privacy legislation in the future.

Thank you very much again for holding this hearing. I look forward to discussing this issue with members of the committee.

[The prepared statement of Mr. Brookman follows:]

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of **Justin Brookman**
Director, Consumer Privacy
Center for Democracy & Technology

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

Hearing on
"Balancing Privacy and Innovation: Does the President's Proposal Tip the Scales?"

March 29, 2012

Chairman Bono Mack, Ranking Member Butterfield, and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today. We applaud the Chairman's continuing leadership in exploring privacy issues and potential solutions.

CDT is a non-profit public interest organization dedicated to keeping the Internet open, innovative and free. We believe that privacy and innovation — when properly balanced — are mutually beneficial. We view the Administration's proposal for transparent, multistakeholder collaborations to translate the Fair Information Practices (FIPPs) into voluntary, enforceable codes of conduct as a modest but important step forward toward protecting user rights and building the consumer trust necessary to encourage continued innovation. Ultimately, however, we agree with the Administration and the Federal Trade Commission that flexible, comprehensive legislation will be necessary to fully achieve these goals.

My testimony begins with a brief overview of the privacy threats faced by modern consumers, analyzes the relationship between privacy and innovation, and finally discusses the Administration's proposal and the need for a privacy framework to support the rapid innovation propelling our economy forward today.

1. Privacy in the information age

Privacy is an essential building block of trust in the digital age. However, in recent years, technological developments and market forces have created fundamental challenges to our assumptions about privacy. Massive increases in data storage and processing power have enabled diverse new business models predicated on the collection, analysis and retention of richly detailed data about consumers and their online — and offline — activities. While these new services and applications are often of great value to consumers, they also present new risks to consumer privacy. Americans turn to search engines to answer sensitive questions about their health. They use smart phone applications to pinpoint their location and obtain directions to a lawyer's or therapist's office. They shop, leaving digital traces of the book stores they browse, credit card numbers, and home and email addresses with "salesclerks" they never meet.

Loss of Control

A crucial first step to protecting privacy is empowering consumers to make meaningful decisions for themselves. Meaningful decisions presuppose both that choices are available and that consumers understand enough about the services they use (and, even more obscurely, the online data trade these services participate in).

It is well-established that consumers today simply aren't provided with enough insight to make informed choices, even when such choices are available. For example, a 2009 study conducted by researchers at UC Berkeley and the University of Pennsylvania's Annenberg School of Communication found that sixty-two percent of respondents incorrectly believe that "If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission."[1]

Given the considerable length and complexity of most privacy policies, it is no surprise that consumers do not understand their purpose. Researchers at Carnegie-Mellon University have shown that for a consumer to reach a basic understanding of how his or her information is being collected and used, he or she would have to spend between 181 and 304 hours each year reading Web site privacy policies. Nationally, this sums to between 39.9 and 67.1 billion hours per year spent reading privacy policies, for an estimated annual national economic cost of between 559 billion and 1.1 trillion dollars.[2]

This state of affairs is made worse still by the fact that the few controls we do have are often overcome. Over the past few years, we've seen "flash cookies" override choices made by users who choice to disable cookies to avoid tracking.[3] More recently, we read about Google's inadvertent tracking of users on Apple's Safari browser, despite privacy features in the browser that should be trusted to prevent such tracking.[4] Mobile applications routinely take more

---

[1] Turow, et. al, *Americans Reject Tailored Advertising and Three Activities that Enable It*, September 29, 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[2] Aleecia McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society* (2008 Privacy Year in Review issue), *available at* http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

[3] *See, e.g.*, Ayenson, et. al., *Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning*, July 29, 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390.

[4] Julia Angwin and Jennifer Valentino-Devries, *Google's iPhone Tracking, The Wall Street Journal*, February 17, 2012, http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html.

consumer data than they need,[5] including in many cases entire address books.[6] And major services have violated their own privacy policies, leaving users unsure of what to expect.[7]

This lack of meaningful understanding and choice is just the threshold problem. A lack of privacy assurances creates an array of undesirable results, from palpable physical and financial losses (in the cases of stalking[8] and identity theft[9]), to global distrust of American products and services.[10]

Why Privacy Matters

As the President wrote in his forward to the Department of Commerce's privacy report:

> *Americans have always cherished our privacy. From the birth of our republic, we assured ourselves protection against unlawful intrusion into our homes and our personal papers. At the same time, we set up a postal system to enable citizens all over the new nation to engage in commerce and political discourse. Soon after, Congress made it a crime to invade the privacy of the mails . . . . Citizens who feel protected from misuse of their personal information feel free to engage in commerce, to participate in the political process, or to seek needed health care.*[11]

The enjoyment of privacy enables the exercise of our right to liberty. The FTC recently endorsed the idea that privacy harms extend beyond literal physical and financial harms.[12]

---

[5] Scott Thurm and Yukari Iwatani Kane, *Your Apps are Watching You*, THE WALL STREET JOURNAL, December 17, 2010, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html

[6] Cesar Torres, *Path addresses privacy controversy, but social apps remain a risk to users*, ARSTECHNICA, February 12, 2012, http://arstechnica.com/gadgets/news/2012/02/path-addresses-privacy-controversy-but-social-apps-remain-a-risk-to-users.ars.

[7] *See, e.g., In re Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.; *In re Google Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order) *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzcompt.pdf.

[8] *See, e.g.*, Kate Ashford, *Online Privacy Predators*, Women's Health, December 20, 2010, http://www.womenshealthmag.com/life/cyber-crime.

[9] Identity theft and other scams cost Americans $1.52 billion last year. Ian Simpson, *ID theft, fraud cost Americans $1.52B last year*, MSNBC, February 28, 2012, http://www.msnbc.msn.com/id/46562746/ns/business-consumer_news/t/id-theft-fraud-cost-americans-b-last-year/.

[10] *See, e.g.*, Jennifer Baker, *European distrust of US data security creates market for local cloud service*, COMPUTERWORLD, December 2, 2011, http://www.computerworld.com/s/article/9222361/European_distrust_of_US_data_security_creates_market_for_local_cloud_service.

[11] *See generally Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, The White House, February, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (letter from President Obama).

[12] The recent *News of the World* hacking incident provides a useful case study about why an expansive definition of "harm" is necessary to evaluate privacy concerns. In this example, reporters from a British tabloid used readily-available technological means to obtain the private voicemails of dozens of high-profile celebrities. The tidbits gleaned from these voicemails became the basis for many of the paper's subsequent stories. Although the individuals whose privacy was breached cannot say they were "harmed" in a physical or economic sense, an ordinary person would certainly deem this unexpected access of their private communications to be improper, unwarranted, not consented to, and, hopefully, illegal. *See* Julia Day, August 6, 2006, *Phone Tap Investigation Widens*, http://www.guardian.co.uk/media/2006/aug/09/royalsandthemedia.themonarchy

These include "the unexpected revelation of previously private information, including both sensitive information (*e.g.*, health information, precise geolocation information) and less sensitive information (*e.g.*, purchase history, employment history) to unauthorized third parties."[13] The FTC's recent actions against Google Buzz and Facebook exemplify rectification of these harms.[14] These harms should resonate on both a personal and business level: unexpected uses of data damage our trust and impinge upon our desire to engage with innovation.

Increasingly, we live in a world where *everything we do is observable*. Pervasive closed-circuit television and drone surveillance, and the emergence of facial recognition, may soon allow companies to persistently track users across space and over time by their individual identities.[15] Indeed, even the privacy that we expect inside our house is threatened by technological developments. Researchers at the University of Washington have uncovered ways to determine what television shows are being watched inside a home by measuring the electromagnetic radiation emitted from the power lines publicly observable outside your house.[16]

There is an incredible amount that we as a society have to gain from innovative new technologies, but there is also an incredible amount that we have to lose. Without a framework in place to assure everyday consumers of the ability to limit the collection and retention of the minutiae of their lives by unknown third parties, any sense of a realm of personal privacy may completely evaporate. In short, we may lose:

- Our right to read newspapers unnoticed: to throw a quarter into the vending box and grab a copy, to privately choose which articles we read and which we don't, gradually slips away each time a local paper shutters its presses or halts print distribution.
- Our right not just go for a drive unnoticed, but to talk to friends unnoticed, to write letters unnoticed,[17] to read books unnoticed, to watch a TV show unnoticed, to buy a gift unnoticed — all of these rights are eroding as these activities move into the networked world and surveillance technologies become more sophisticated.
- Our right to walk down the street unnoticed, whether en route to a political rally or to a doctor's office, is eroding as facial recognition technology advances and becomes more widely deployed.[18]

---

[13] *Protecting Consumer Privacy in an Era of Rapid Change*, Federal Trade Commission Report, March 2012, http://www.ftc.gov/os/2012/03/120326privacyreport.pdf, 8.

[14] *Id.*

[15] *See* Harley Geiger, *The Drones are Coming*, CDT Blog, December 21, 2011, https://www.cdt.org/blogs/harley-geiger/2112drones-are-coming; Harley Geiger, *Facial Recognition and Privacy*, CDT Blog, December 6, 2011, https://www.cdt.org/blogs/harley-geiger/612facial-recognition-and-privacy/.

[16] Miro Enev, *et al*, Televisions, Video Privacy, and Powerline Electromagnetic Interference, *Working Paper*, http://abstract.cs.washington.edu/~miro/docs/ccs2011.pdf.

[17] USPS mail currently receives more privacy protections than does electronic mail. *See*, *Federal Statutes and Regulations Relation to the Privacy and Security of Mail*, http://about.usps.com/who-we-are/privacy-policy/intelligent-mail-privacy.htm#H7.

[18] *See* Harley Geiger, *Facial Recognition and Privacy*, CDT Blog, December 6, 2011, https://www.cdt.org/blogs/harley-geiger/612facial-recognition-and-privacy/.

But to "opt out" of the data collection, correlation, and/or use that takes place when we go about the activities described above would be analogous to "opting out" of electricity a mere thirty years ago. To disconnect from the services that collect such personal, sensitive data would be to disconnect from society. Cutting off all data collection is not viable, but finding a middle-ground compromise that forestalls persistent monitoring is absolutely necessary to ensure consumer trust in the digital ecosystem.

Crucially, neither the loss of privacy nor the assumption of these harms is an inevitable cost of technological innovation. Instead, both have been the natural outgrowth of a policy framework that has turned a blind eye to the foundational benefits that privacy offers us as citizens of a democracy and as consumers in a strong capitalist society. Smartphones, for example, would be no less magical if applications did not have such pervasive access to all of our phone's files and functionality. In some instances, consumers could lose functionality if they were unwilling to share some personal data with services, but increasingly, many consumers would prefer a more privacy-protective, and less personalized, user experience.[19]

Certainly, many companies that access user data in unexpected ways do not intend to publicize or even share the data with others. However, that fact alone does not nullify a consumer's reasonable privacy concerns. Even when data is collected merely for limited purposes, consumers could reasonably worry that their data could later be used for new, unexpected and unwanted purposes,[20] accessed by a rogue employee,[21] breached by hackers,[22] unwittingly exposed to the world,[23] or accessed by the government without robust legal process.[24] And the knowledge that their behavior is being monitored and retained (and potentially shared, accessed, or lost) can have a very real chilling effect on free expression, as well as the adoption of new technologies and services.[25]

2. Trust and innovation are inseparable ideals

Technology and market forces have unleashed a wave of innovation rolling at a pace we have never seen. Today, consumers regularly turn to the Internet to build their social networks,[26]

---

[19] John C. Dvorak, *Pew Finds Searchers Attitudes Toward Privacy Are Changing*, March 16, 2012, PCMAG, http://www.pcmag.com/article2/0,2817,2401717,00.asp (finding "73% of search users supported a statement that they would not be okay with a search engine keeping track of their searches and using that information to personalize future search results because they feel it is an invasion of privacy").

[20] *New York Accuses Gratis Internet of Largest Deliberate Privacy Breach Ever*, March 24, 2006, CONSUMERAFFAIRS, http://www.consumeraffairs.com/news04/2006/03/ny_gratis.html.

[21] Adrian Chen, *GCreep: Google Engineer Stalked Teens, Spied on Chats*, September 14, 2010, GAWKER, http://gawker.com/5637234/.

[22] Liana B. Baker and Jim Finkle, *Sony PlayStation suffers massive breach*, April 26, 2011, REUTERS, http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426.

[23] Declan McCullagh, *AOL's disturbing glimpse into users' lives*, August 7, 2006, CNET, http://news.cnet.com/2100-1030_3-6103098.html.

[24] David Kravets, *Yahoo, Feds Battle Over E-Mail Privacy*, April 14, 2010, WIRED, http://www.wired.com/threatlevel/2010/04/emailprivacy/.

[25] Emmett Higdon, *Privacy Concerns Threaten Emerging Interest in Banking on Social Sites*, Emmett Higdon's Blog, May 21, 2010, http://blogs.forrester.com/emmett_higdon/10-05-21-privacy_concerns_threaten_emerging_interest_banking_social_sites.

[26] For example, Facebook reported 845 million monthly active users as of December, 2011. Facebook Newsroom, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22 (*last visited* March 27, 2012).

keep in touch with loved ones,[27] engage in commerce,[28] and join political movements.[29] American companies play a leading role in this innovation, benefitting the economy and creating jobs,[30] and enriching our lives. This is innovation we should all embrace and encourage.

And the pace of this innovation is still accelerating. Exponential growth in data, computing power, and powerful analytic techniques are opening new markets and creating possibilities every day.[31]

While few consumers fully grasp the extent of this large and growing data trade, numerous independent studies show that practices such as deep packet inspection, online behavioral advertising, and the merger of online and offline consumer data into profiles undermine consumer trust, the fundamental building block of Internet use.[32] Privacy worries continue to inhibit some consumers from engaging in online shopping and banking, [33] and are a top reason consumers decline to adopt location-based services.[34] A poll conducted by Zogby International

---

[27] And find new ones: online dating has recently surged in popularity. *See, e.g.,* Abby Ellin, *The Recession. Isn't It Romantic?*, THE NEW YORK TIMES, February 11, 2009, http://www.nytimes.com/2009/02/12/fashion/12dating.html.

[28] Online retail sales in the United States total $145 billion annually. U.S. Census Bureau, *E-Stats*, May 26, 2011, http://www.census.gov/econ/estats/2009/2009reportfinal.pdf, at 1.

[29] Online political engagement is growing but stratified by income and education. *The Demographics of Online and Offline Political Participation*, Pew Internet, Sept. 1, 2009, www.pewinternet.org/Reports/2009/15--The-Internet-and-Civic-Engagement/3--The-Demographics-of-Online-and-Offline-Political-Participation/2--Online-Politics.aspx.

[30] *See, e.g.,* John Moore, *IT jobs thriving despite lackluster economy*, ABC NEWS, August 16, 2011, http://abcnews.go.com/Technology/jobs-thriving-lackluster-economy/story?id=14311664; John Furrier, *Big Data is Creating The Future — It's A $50 Billion Market*, FORBES, February 29, 2012, www.forbes.com/sites/siliconangle/2012/02/29/big-data-is-creating-the-future-its-a-50-billion-market/.

[31] For example, Apple reported that over 15 billion apps have been downloaded from its app store as of July 2011. Apple Press Release, *Apple's App Store Downloads Top 15 Billion*, July 7, 2011, http://www.apple.com/pr/library/2011/07/07Apples-App-Store-Downloads-Top-15-Billion.html

[32] *See e.g.,* Scott Cleland, Americans Want Online Privacy – Per New Zogby Poll, PUBLIUS' FORUM, June 9, 2010, http://www.publiusforum.com/2010/06/19/americans-want-online-privacy-per-new-zogby-poll; Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessey, Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It (Sept. 2009), http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf. See also Alan F. Westin, Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles: Level of Comfort Increases when Privacy Safeguards Introduced, HARRISINTERACTIVE, April 10, 2008, http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Majority-Uncomfortable-withWebsites-Customizing-C-2008-04.pdf (in which majority of respondents said they were not comfortable with online companies using their browsing behavior to tailor ads and content to their interests even when they were told that such advertising supports free services); John B. Horrigan, Use of Cloud Computing Services, PEW INTERNET & AMERICAN LIFE PROJECT, September 2, 2008, http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf (showing that 68% of users of cloud computing services say they would be very concerned if companies that provided these services analyzed their information and then displayed ads to them based on their actions).

[33] *See* John B. Horrigan, Online Shopping, PEW INTERNET & AMERICAN LIFE PROJECT, February 13, 2008, http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Online%20Shopping.pdf.pdf; Emmett Higdon, *Privacy Concerns Threaten Emerging Interest in Banking on Social Sites*, Emmett Higdon's Blog, May 21, 2010, http://blogs.forrester.com/emmett_higdon/10-05-21-privacy_concerns_threaten_emerging_interest_banking_social_sites..

[34] *See* Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, & Norman Sedeh, Location-Sharing Technologies: Privacy Risks and Controls, CYLAB USABLE PRIVACY & SECURITY LABORATORY 18 (2010), http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

in June 2010 found that 88% of Americans are concerned about the security and privacy of their personal information on the internet.

This trust is the difference between innovation that delights us and innovation that deeply discomforts us. In short, trust underpins and fuels this innovation. If consumers are unable to trust this increasingly complex network of innovative services, innovation suffers.

Privacy is about securing user rights. But it is also about building trust in the marketplace in hopes of protecting and accelerating the innovation we see today. In short, innovation and privacy are not incompatible paths, but intertwined paths.

Increasingly, for many companies, the growth of cloud computing is bringing new urgency to the call for comprehensive privacy legislation.[35] As American companies continue to innovate and expand their markets overseas, they are finding that America's weak privacy framework is bad for business. Without adequate privacy protections in place, individuals, companies, and governments in other countries do not feel comfortable — or in many cases are legally restricted from — taking advantage of U.S.-based cloud computing services. With our advanced technology and infrastructure, U.S. companies and the U.S. economy are poised to lead adoption of this hugely important new generation of cloud-based services.[36] However, the lack of a comprehensive privacy protection framework puts U.S.-based companies at a disadvantage to other providers.

3. The Administration's framework supports privacy and innovation

The proposal contained within the Administration's "Consumer Privacy Bill of Rights" is a modest step toward protecting consumer's expectation of privacy rights and building trust to support innovation. To understand why, it's important to situate the Administration's Proposal in a broader context and compare it to other self-regulatory and legislative efforts.

Modern privacy advocacy has centered squarely around the "Fair Information Practices,"[37] or FIPPs. These high-level principles are the fundamental building blocks of any modern privacy

---

[35] Sara Jerome, *Intel, Microsoft, eBay support Rush's privacy bill, while noting concerns*, Hillicon Valley Blog, October 7, 2010, http://thehill.com/blogs/hillicon-valley/technology/123197-intel-microsoft-ebay-support-rushs-privacy-bill-while-noting-concerns-.

[36] Article 25 of the EU Data Protection Directive states that the personal information of EU citizens may not be transmitted to nations outside of the EU unless those countries are deemed to have "adequate" data protection laws. The Article 29 Working Party does not consider U.S. law "adequate" (in part because the U.S. has no comprehensive data protection law), and thus in general personal information about EU data subjects may not be transferred to the U.S. for storage or other processing. While there are several compliance mechanisms, such as the U.S.-EU "Safe Harbor" agreement, that allow U.S. companies to process personal information from the EU, each comes with its own compliance challenges. For an in-depth discussion of these compliance challenges, see Comments of the Center for Democracy and Technology on Information Privacy and Innovation in the Internet Economy, CDT (2010), http://www.cdt.org/files/pdfs/20100613_doc_privacy_noi.pdf.

[37] FIPPs have been embodied to varying degrees in the Privacy Act, Fair Credit Reporting Act, and other sectoral federal privacy laws that govern commercial uses of information online and offline. A recent government formulation of the FIPPs offers a robust set of modernized principles that should serve as the foundation for any discussion of consumer privacy frameworks. These principles, as described by the Department of Homeland Security in 2008, include:

framework. They are found in the Administration's Consumer Bill of Rights,[38] strongly echoed in the FTC's Final Report on consumer privacy,[39] and have a long history throughout other federal privacy laws. The FIPPs include concepts like "transparency," control," and "purpose specification" — together, these concepts provide a roadmap for empowering individuals to both understand and impact how their data is collected and used. In simpler terms, FIPPs aim to offer consumers a sense of control, insights into the tradeoffs they're making with their data, and assurances of security. By nature and design, FIPPs are flexible and open to interpretation.

Theoretically, there are a number of ways we could translate the high-level principles contained in the FIPPs into actionable policy across a range of diverse technologies and industry business models:

• **Transparency**. Entities should be transparent and provide to the individual regarding their collection, use, dissemination, and maintenance of information.

• **Purpose Specification**. Entities should specifically articulate the purpose or purposes for which personal information is intended to be used.

• **Use Limitation**. Personal information should be used solely for the purpose(s) specified in the notice. Sharing of personal information should be for a purpose compatible with the purpose for which it was collected.

• **Data Minimization**. Only data directly relevant and necessary to accomplish a specified purpose should be collected, and data should only be retained for as long as is necessary to fulfill a specified purpose.

• **Data Quality and Integrity**. Entities should, to the extent practicable, ensure that data is accurate, relevant, timely, and complete.

• **Individual Participation**. Entities should involve the individual in the process of using personal information and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of this information. Entities should also provide mechanisms for appropriate access, correction, and redress regarding their use of personal information.

• **Security**. Entities should protect personal information through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

• **Accountability and Auditing**. Entities should be accountable for complying with these principles, providing training to all employees and contractors who use personal information, and auditing the actual use of personal information to demonstrate compliance with the principles and all applicable privacy protection requirements.

U.S. Department of Homeland Security, *Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (December 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. The Administration's Consumer Bill of Rights is based on a slightly reworded, but fundamentally comparable set of FIPPs. *See generally Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, The White House, February, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[38] *See id.*

[39] *See generally Protecting Consumer Privacy in an Era of Rapid Change*, Federal Trade Commission Report, March 2012, http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

- prescriptive, industry-specific legislation;
- flexible, principles-based legislation with detailed FTC rulemaking;
- flexible legislation with targeted FTC enforcement;
- flexible legislation with safe harbors for FTC-approved voluntary codes of conduct;
- self-regulation

As the FTC made clear in its Final Report on privacy earlier this week, and as documented above, we've already witnessed a general failure of self regulation to adequately inform consumers or give them control over their personal information.[40] On the other hand, a highly inflexible, prescriptive piece of legislation could lose relevance as technology develops and could deter innovation. CDT suggests that both of these solutions come at an unacceptable cost to either trust or innovation. The solution falls somewhere in between.

CDT has long supported a carefully-crafted framework that gives industry segments flexibility to develop tailored privacy solutions that benefit consumers. We believe that these codes would be best developed through multistakeholder discussions with civil society advocates and regulators, but in any event, the voluntary codes must be formally endorsed by the Federal Trade Commission to ensure they are sufficiently robust and to garner consumer confidence in them. We believe this is the best way to create certainty for companies, encourage privacy innovation over time, and reward the adoption of accountable practices. Traditionally, this support has come in the context of advocating for flexible baseline consumer privacy legislation that also protects innovation.[41] We continue to believe this is the best path forward. However, the Administration's interim process of voluntary convenings provides a path to make substantial progress on privacy through enforceable voluntary codes on emerging privacy problems as new technologies develop (on the spectrum above, the Administration's interim measure would fall somewhere between the fourth and fifth options).

The voluntary, multistakeholder approach offers an open, transparent forum for good faith negotiations among industry, advocates, and regulators. The codes will not be written in stone and will be open to innovation over time. The FTC is prepared to enforce the promises made in the negotiated codes, offering important assurance to consumers and certainty for those companies that step up to the negotiating table.[42] Our greatest concern is that absent a law to incentivize companies to negotiate interpreting rules for the treatment of personal data, not all companies will be interested in negotiating these codes, and others may eventually walk away and fail to adopt the codes, with limited consequences.[43]

CDT agrees with both the Administration and the FTC that a baseline privacy law will ultimately be needed, and we call on this Subcommittee to move forward toward that goal. But we cannot

---

[40] *Id.*

[41] *See, e.g.,* Statement of Leslie Harris Before the House Committee on Energy and Commerce, *The Best Practices Act of 2010 and Other Federal Privacy Legislation*, July 22, 2010, http://www.cdt.org/files/pdfs/CDT_privacy_bill_testimony.pdf.

[42] Justin Brookman, *Two Step Forward for Privacy*, CDT Blog, February 24, 2012, https://www.cdt.org/blogs/justin-brookman/2402two-steps-forward-privacy.

[43] *Id.*

wait to make progress; and we believe that in certain industries, the incentives may well be already aligned to develop strong, industry-wide codes of conduct, offering progress on privacy now and a model that should inform the shape of privacy legislation in the future.

4. Conclusion

CDT would like to thank the Subcommittee again for holding this important hearing. We believe that Congress has a critical role to play in ensuring encouraging the development of privacy frameworks that foster innovation. CDT looks forward to working with the Members of the Subcommittee as they pursue these issues further.

For more information, contact Justin Brookman, justin@cdt.org, (202)637-9800.

Mrs. BONO MACK. Thank you, Mr. Brookman. I am going to recognize myself for 5 minutes of questioning, and I would like to start with Mr. Szoka.

You criticize the White House's decision to use the phrase "Bill of Rights" in describing its privacy principles. Why do you think that term is problematic?

Mr. SZOKA. Well, for the very reason you heard today, the term is now being used as a shorthand for regulatory framework. We have a Bill of Rights in this country. I happen to consider it the basis of our Constitution, of our civil liberties. The White House essentially has appropriated that term for its own purposes. Now you might think that the White House report is a fairly good document. You might think we should do something on privacy, but I don't think it is appropriate to use that term. And I think if you look at the historical provenance of the way the term in general Consumer Bill of Rights has been used in this country, you go back to President Kennedy's 1962 Consumer Bill of Rights. I still wouldn't have used the term then, but even there the rights he was focused on were primarily rights against deception and harm. And in my opinion those are things already covered today by the FTC's act. They are things that should be the basis for legislation. That is a very fine concept for us to talk about. But for us to put the term "rights" into this conversation I think is counterproductive. It makes it difficult for us to recognize the complex tradeoffs that are at issue here.

Mrs. BONO MACK. Does anyone else care to comment on that? No.

OK, let me ask the second question, and I will start with Mr. Szoka again but open it to anybody who would like to answer. I think whenever we use anecdotal questions, as Mr. Markey did and talked about online privacy for children, I think that was very important. But the question came to me, he used an example of a 16-year-old searching weight loss products and suddenly began being bombarded with weight loss ads that were negative for a 16-year-old. But at the same time as somebody who cares very deeply about the problem of drug abuse in this country that 16-year-old was searching on the Web for OxyContin. Could not that same child be targeted with ads for rehab or recovery or drugfree.org? Couldn't there be the same opportunity for good in that example? Does anyone want to comment on that?

Mr. SZOKA. If I may, absolutely. I think it is important to remember here that when we talk about messaging we are not just talking about selling products, we are talking about that sort of expression. It could be for a health message, it could be for any sort of social message, health message or religious or political message. I also think it is important on that particular example on Mr. Markey's bill to recognize that any time we start talking about segmenting users by age we are very limited in what we can do. COPPA strikes a good balance. If you go beyond that you essentially wind up with an age verification mandate system, which the Supreme Court has declared unconstitutional.

Mrs. BONO MACK. Anyone else wish to weigh in on that?

Mr. ZANEIS. Sure, I would like to. What you are describing is exactly the power of the Internet, which is the ability to provide rel-

evant content. Sometimes that relevant content is also the advertising. We have to be very careful not to close the line into truly sensitive data categories. And the industry has really since 1999 had a self-regulatory program through the network advertising initiative, which cordons off certain practices in data categories we think should be off limits.

But I think the key thing is it is not just about what you specifically are looking for. One of the powers of the Internet is this discoverability and learning things new and being exposed to new ideas and new products. And I think because of the data then flows online, that is enriching in the consumer experience in exactly the way that you describe.

Mrs. BONO MACK. Thank you. Mr. Zuck.

Mr. ZUCK. Just briefly to follow on what Mr. Szoka said, I think it is not only a constitutional problem, but as a programmer I have to call it a technical problem to do age verification. In the absence of some kind of universal biometric verification across the country, which a lot of people would take issue with, I think the actual feasibility from a technical perspective of identifying people's age is something that really has to be taken into consideration as well.

Mrs. BONO MACK. I want to actually move to the next question to you quickly with 1 minute left. You are an international organization with firms throughout the world. How many U.S. firms versus non-U.S. firms do you have? And is there a reason the U.S. is leading innovation in the Internet space? And has the EU privacy directive hurt innovation?

Mr. ZUCK. Thank you, Chairman, it is an excellent question. As an organization we have about 4,000 members totally and 3,000 of them in the U.S. and perhaps about 1,000 outside the U.S., and many of those in Europe, and so have had a chance to hear the stories from both sides.

I think the reason the United States leads the world innovation is because of the level experimentation that is permitted in our economic system. So small businesses being able to try things, bring out new products that people wouldn't expect to succeed, and then quickly pull them off the market if they fail, et cetera. Experimentation both in terms of business model, experimentation in terms of the labor you are consuming as a business are all things that make it possible for entrepreneurship to thrive much better here than it does in Europe. And there have been plenty of studies that have affirmed the fact that undue regulation in Europe has stunted the growth of Internet based startups in the continent.

Mrs. BONO MACK. Thank you, Mr. Zuck. My time has expired. I am going to recognize Mr. Butterfield for 5 minutes, and we have 2 votes on the floor. We will take a brief recess for the votes.

Mr. BUTTERFIELD. Thank you. I will accelerate this. Consumer choice about when and whether to disclose information can often make an illusion. For example, it appears that consumers have a choice about whether to give up personal data in exchange for participation in a supermarket's frequent shopper card program, for example. But we all know in the current economy families are struggling to make ends meet. So when a constituent or citizen trying to keep food on the table and—let me try that again. So when constituents are trying to keep food on the table and the difference

between signing up and not signing up is somewhere between $3 and $5 for cereal, they don't have a choice. And for a family those differences can add up to many dollars. Imbalances in economic power and imbalances in the control of information needed for basic life functions such as doing most jobs in an information economy have made the choice over whether to give out personnel data and illusion.

Please help me, Mr. Brookman, I just want, given the point you raise in your testimony, do you have additional thoughts on these observations?

Mr. BROOKMAN. Yes. By and large I am actually generally OK with people paying with their privacy as opposed to paying higher dollars for goods and services as long as there is a robust market for the products. So if one wants to get and use their Safeway card and Safeway is going to give them cheaper prices in exchange for some privacy, I mean if they don't like that they can either not do it or go down the street to the Harris Teeter. I think as long as it is transparent, I think that is fine.

I think part of the problem with the online information sharing is that it is not really transparent. Right now if I want to evaluate New York Times versus Fox News for which one treats my privacy better, which one is sharing more information on me, I actually cannot make that determination. I can try to install add-ons, I can try to figure out what is going on but I need to be pretty technically sophisticated in order to do that.

I think there have been improvements with the Icon program, has made some progress in that direction. I think by and large there is not a lot of education to teach people what that means. I think whenever I talk outside of D.C. About the Icon program, I ask people do you guys know what it does, generally no one raises their hands. So I think more needs to be done for publishers and advertisers to make that value proposition clear to consumers, but as long as there is a value proposition I think that does offer people better alternatives to make decisions for themselves about what they want to do.

Mr. BUTTERFIELD. Thank you. I yield back.

Mrs. BONO MACK. I thank the gentleman. The chair recognizes Dr. Cassidy before we break for the floor vote.

Mr. CASSIDY. Mr. Szoka, I found all of your testimony provocative but let me start with you. You dispute, somehow disagree with the concept that my privacy would be considered as a property right. I think, I don't want to mischaracterize, you know so much more than me. I am trying to understand, I am the pupil here. But I get a sense the logical extension of your testimony is that minority report is quite OK, that I can walk into a store and there will be some facial recognition software that would say Bill Cassidy, 54-year-old fellow, who is a little overweight, he needs a tailor. Will you please go down the hall and you will meet the tailor?

One, that would be a troubling thing to be recognized as, but secondly, again is the logical extension of your testimony the minority report is OK?

Mr. SZOKA. So I do agree that the property metaphor is not a useful one for privacy. And the reason is that, for instance, we are all here in this room. We all might in some sense own our shared

experience, but it is a shared experience. If you go down the road of propertytising personal information and our interactions with each other you create what I think becomes an unworkable system of information control precisely because those interactions are shared. If you take an off-line example——

Mr. CASSIDY. But What is the limit? What would be your limit that you would establish what someone could do with my personal information?

Mr. SZOKA. As I said today and in my testimony, the clear limits are harm and deception.

Mr. CASSIDY. On the other hand, me walking into the mall and having facial recognition software directing me, that is Bill Cassidy, let's send them down here, would that be a limit that you think—would that be over the limit or on the good side of the limit?

Mr. SZOKA. Well, in principle I think that those systems can be done consistent with my conception of privacy. I think what we need to do is look at how they are actually likely to be done. And in this respect I would point you to the good work that my colleagues at CDT, Harley Geiger in particular, have done, describing the ways in which they think that self—that industry is likely to actually implement those systems in the privacy protection phase.

Mr. CASSIDY. But now I am actually asking for the specific question. Facial recognition software when I walk into Tysons Corner directing me to a store that they kind of figure out I need, is that an appropriate use, is that over the bounds or within the bounds of what we should be doing regarding privacy?

Mr. SZOKA. I think it certainly can be an appropriate use. And just the same way I think that we are seeing concern today about that it much resembles the concern about cameras and photography.

Mr. CASSIDY. I disagree with that and I saw your analogy, but I will also say that if there is a picture taken of me in a public event with folks who are not public figures, there is a request that they sign over or the paper says maybe it is with children I have noticed this, they get specific approval to use that.

Now, Mr. Brookman, would you agree that facial recognition software is an appropriate use, et cetera, et cetera?

Mr. BROOKMAN. I think you draw attention to a really important point and this kind of goes to the harm question we keep talking about. I think there is some sort of harm, the surreptitious pervasive collection of personal information about ourselves that we have no control over whatsoever. And I think you are absolutely right that it becomes scarier as technology becomes more and more sophisticated. It is not just online anymore, it is not just the fact that I can't be private online. It is increasingly going to be the fact that I can't walk down the street in public anymore without having cameras collect who I am and watch where I go and create bread crumb trails about my self over time.

And yes, to some extent increasingly everything we do about ourselves is observable. And I think there needs to be some sort of limitations on what companies can do about that.

Mr. CASSIDY. Where is the limitations?

Mr. BROOKMAN. I would say for private companies tracking what you do in public, I would say that this is the guidelines we have worked with some facial recognition companies on, is they should not remember who you are over time and correlate over time or identify you without your permission.

Mr. CASSIDY. So I am a doctor, I can look at someone and I can say at times they have liver disease because their eyes are yellow or they have psoriasis because they have a patch of a rash on their elbow or they have HIV because they have a characteristic physical thing that is a side effect of some of the medication.

Now is that appropriate for that computer software to figure out what I as a doctor can figure out?

Mr. BROOKMAN. I am happy to consider that particular technological development.

Mr. CASSIDY. It is very simple, I can promise you. That would be so easily programmed to know if someone is on steroids.

Mr. BROOKMAN. The camera would detect this person is on steroids?

Mr. CASSIDY. Yes.

Mr. BROOKMAN. Should cameras be doing that? I think that is not a good practice. The question becomes should there be a law against it? And that becomes harder because there are First Amendment implications of that. But I think as we saw in the recent Supreme Court Jones case the question whether a car going around in public, can the police use technology to monitor that 24/7? And the majority of justices said, no, even though you are in public and things are observable, you have some sort of privacy interest and the fact that even though you are in public you don't expect you will be watched and monitored and surveilled and your information collected over time. That was a government case.

Mr. CASSIDY. So if I am at Tysons Corner they should not use a facial recognition to figure out——

Mr. BROOKMAN. Right. They should not recognize you or recognize the fact that you were last week shopping at Victoria's Secret.

Mr. CASSIDY. By the way, I wasn't. Thank you, I yield back.

Mrs. BONO MACK. The subcommittee will stand in recess for these two votes. Hopefully we will be able to return within 20, 25 minutes, something like that. Lord only knows. If you will stand by, we will return as quickly as we can. The subcommittee is in brief recess.

[Recess.]

Mrs. BONO MACK. The vice chair of the subcommittee for 5 minutes, Mrs. Blackburn. You are recognized for 5 minutes.

Mrs. BLACKBURN. I am so thrilled that you all are hanging with us today. Little did we know when we planned this hearing that we were going to have five vote series today, but that is where we are.

Berin, I want to come to you. Last panel I talked a little bit about the FTC having sufficient authority to move forward to enforce privacy violations and then if they enforced section 5 and do it right would that be enough. And we talked a little bit about where the gap is, FTC and Commerce. I would love for you to comment on where you think the gap is.

Mr. SZOKA. Thank you, Congresswoman. Remember the FTC has two authorities. The deception authority allows it to enforce statements that a company makes, including participation in self-regulation. I think that becomes the powerful tool by which self-regulation, if a company accedes to it, is legally binding as it should be. The unfairness authority I think is where the FTC can do both the most good and the most damage, depending on how it uses that authority. And I would point the committee in particular to the Frost wire case I mentioned in my testimony where to make a long story short the FTC I think made a solid argument that industry practice against having apps that would share every single file on your phone and not tell you about it and make it difficult for you to stop that, that that was an unfair practice in part because it didn't meet industry practice. In other words, I think that the FTC can use unfairness to punish laggards that do not keep up with industry practice, but I think they need to be very rigorous in their analysis of benefits, harms and the degree to which a consumer can avoid a harmful practice.

Mrs. BLACKBURN. So you see a need for some flexibility?

Mr. SZOKA. Flexibility, but I also think what is important is the FTC explains ahead of time how it is going to apply that authority, and in that respect I would love nothing more than to see from your committee the sort of letter that prompted the FTC in 1980 and 1983 to issue its policy statements on unfairness and deception. And that would be a letter that simply asks the FTC to explain in its recent cases how it has applied those doctrines, how it actually evaluates whether harms outweigh benefits and it provides rigor so that companies, especially startups, can understand and predict what could be considered unfair.

Mrs. BLACKBURN. OK. Let me just tag onto this because I know you have criticized the White House for using the term "Bill of Rights" when they look at their privacy principles. So if you are wanting to see those guidelines and see something that gives you that rigor, if you will, then why criticize that term?

Mr. SZOKA. The White House proposal provides high level principles. I think they are fairly good principles, but they are abstract. And we cannot apply them strictly speaking. For example, to say that consumers have a right to control information about them I think is problematic because in fact the way that our privacy law rightly has developed that sort of concept is to say that in certain circumstances you don't have a right to control, for example, what a credit bureau says about you if it is truthful. What you have a legal right to do is make sure that it is accurate. So the trick again is translating those principles into workable guidelines. I think to call them rights from the outset and put them in strict terms is unhelpful because it is not how we actually apply them.

Mrs. BLACKBURN. So we should keep the terminology stating principles and guidelines and not move into that.

Mr. Zuck, I like all the talk about innovation and jobs growth and potential and I share a lot of that optimism. I enjoy sharing that optimism with you all. What bothers me in spite of all the positive job numbers, opportunities for growth, innovative new products that are there. We are having a hearing essentially about

what big government to do in order to solve these problems and make people safer online.

I would like to hear your thoughts on how we found ourselves in this awkward place where people love the technologies and the applications but they do not trust all the players that are in this online ecosystem. And what do you think is the main driver of that uncertainty? And I am now down to 43 seconds, so have at it.

Mr. ZUCK. Well, I think there are a couple of issues that play there. One of them is the conflation of data breach and privacy. A lot of news, a lot of what caused the panic, if you will, among the everyday consumer are large headlines about the fact that Sony lost 70 million names and credit card numbers. That is the kind of thing no matter what notice they were provided, what other policy was in place, that is something that should have happened. I think data breach is something that has to be dealt with separately and we support that.

The other thing are simply privacy issues that happen on such a large scale and drive headlines, whether it is Facebook with the Beacon incident that happened or Google's almost pathological disregard for privacy or public safety. And I think as that continues to come up in the press it gives people a certain fear, it leads to poll results that say I am worried about my privacy. But then when it comes to metal hits the road and we are talking about let's regulate mobile apps, I think we are really missing the point. I think the real answer lies in reinforcement from organizations like the FTC, but to the extent possible without putative measures so people feel the heat of that enforcement, instead of jumping immediately to regulation.

Mrs. BLACKBURN. Thank you for that. I have a follow-up question, but I will submit that as a question for the record in the interest of time, but I would like to take that discussion a little bit further with you. Thank you, I yield back.

Mrs. BONO MACK. Thank you, Mrs. Blackburn. I am going to start with our second round of questioning and recognize myself for 5 minutes. And Mr. Brookman, just a follow on to your conversation or dialogue earlier with Dr. Cassidy. He drew an analogy between the use of facial recognition technology in the mall to a Supreme Court decision in the U.S. v. Jones which involved the police putting a trace tracking device on a car. The court rightly in my opinion did find the Fourth Amendment did apply in that case. But isn't the government's involvement an important distinction, should we automatically be applying the same protections against non-government actors?

Mr. BROOKMAN. No, I absolutely agree to the fact that the government in that case was the key distinction. I was focusing more on the theory that the plurality of justice, Justice Sotomayor, Justice Alito's opinion focused on the fact that even though we are in public there are some inherent privacy rights. We don't expect to be watched and monitored and surveilled all the time. Yes, it is worse when it is the government who have the guns and can put us in prison. I think the principle also applies if it is the case and I am walking down the street I don't have the ability to stop these nameless and faceless companies from developing really detailed profiles about me or even my own home. Some of the technology

in the government surveillance cases in the nineties were about like these thermal imaging things. You can get them for $5 now, they are available to any person or company.

There is a study recently by some researchers at the University of Washington that pointed out that just by looking at public—the way your phone line or power line vibrates from the outside you can tell what television shows people are watching inside. So it is increasingly the fact that technology is making it really easy not just for the government but also for individuals and companies to surveil us no matter where we are. As people we want to have some zone of privacy where we are not being watched and monitored or assessed.

Even when it is just for beneficial purposes or benign purposes like advertising, I don't think advertising is bad at all. I like advertising. It absolutely does fuel the Internet. That information can still be lost or accessed by the government, or breached, or repurposed in some way I don't necessarily expect. There has to be some sort of basic limitations on collection as technology makes the case that everything becomes inherently observable.

Mrs. BONO MACK. Thank you. I am going to move on to Ms. Horan. You know that Mrs. Blackburn and I for all of our careers here have been focused on intellectual property. We want to make sure that people who create valuable content not only are rewarded, but we encourage people to create whether they are a reporter needing to write an article, like an earlier example of the New York Times. That is what this has been all about for a long time. I think in your world the newspapers and online publishers have scrambled to adapt to the disruptive technologies. And some have succeeded and some failed. There is no doubt about it. But I agree with you or agree with the people that believe consumers realize free content is supported by advertising.

However, do you think that most consumers know that advertising is conducted by third parties rather than your members Web sites? The administration's proposal recognizes that data may be used by first parties for marketing, but do any or even a majority of your members conduct their own marketing or do they use third party networks?

Ms. HORAN. So I think consumers are getting smarter. I think that is part of the responsibility of industry to continue to educate. And our members have been active in the program that the DAA has done to do an educational program. Our members, some of our members do work with ad networks, it is a subset of the membership. And the majority of the advertising that our members serve is actually contextual. Those that are working with ad networks it only represents a very small portion, it is only about 2 percent.

So in terms of the experience that we are delivering, it tends to be tied to the context of the content versus interest based experiences.

Mrs. BONO MACK. Do you think in many of your membership that there are examples of people of newspapers, publishers who learned to survive simply because of this that otherwise would have done by the wayside?

Ms. HORAN. Advertising in general, that is the major element that fuels the business. So being able to deliver an experience to

consumers where they do feel like they are in a trusted environment is something that is absolutely paramount, as I mention in my testimony. Obviously I am speaking for the members that we represent and these are obviously brands that have had long-term relationships across different media, as you mention, newspapers and TV broadcasters for some time. But it certainly is and will always be a priority that we deliver an experience that consumers feel they are in a trusted environment.

Mrs. BONO MACK. Have you noticed compared to the good old fashioned, whether we called classified ads in the history books almost anymore, have you noticed though consumers are really preferring the new method over the old classified ads?

Ms. HORAN. In terms of looking at the sheer amount of time consumers are spending online, it has become more and more where they are getting their news, information and entertainment. The business model itself is something we are absolutely committed to looking at how we evolve because you are absolutely right, a significant portion of the advertising revenue that has been part of the print world has diminished. And so online we are looking at ways to try to augment that. Certainly advertising will always be the most substantial revenue that our members garner, but we are certainly looking for other ways to complement that revenue in order to sustain the business.

Mrs. BONO MACK. Thank you. Mr. Zaneis, do you want to respond?

Mr. ZANEIS. I know we are short on time. I just want to make a couple quick points. It is not just about behavioral advertising, it is really about data collection. So we represent many of the original content producers as OPA does as well. And for them it is key that they have to be able to do things like frequency cap, marketing message, so they don't deliver the same ad 15 times. If the consumer didn't click on that ad the first 14 times, they are not going do it the 15th. It is also about content customization which requires information exchange. And I think one problem with the FTC's report is that they don't recognize affiliates as first party. And so you can't have this synergy and we know that companies build brands, and that the ability online to kind of bring those Web sites together to create a richer, more vibrant experience to the consumer is key. We ought to respect all of those as first parties.

Mrs. BONO MACK. Thank you. My time has expired. Mr. Butterfield, you are recognized for 5 minutes.

Mr. BUTTERFIELD. Thank you. Mr. Brookman, I am going to try a question on you that I posed to the first panel. The administration's privacy report advances a framework that includes the development and implementation of industry codes of conduct in parallel with Congress working on and passing baseline privacy legislation. To the extent that the FTC intends to participate in the development of these codes and has also endorsed the idea of Congress passing baseline privacy legislation, it also seems to endorse the idea that these things should happen in tandem or in concert with each other. Some are already arguing that these two pieces should be delinked from one another; that is, the development and implementation of codes of conduct should completely play out before Congress takes any action on baseline legislation.

I get the sense that you would be among those who would disagree with this view. Can you elaborate on that for me.

Mr. BROOKMAN. Yes, I definitely would. I think the administration kind of come out and said it would be better it if we had a law right now that gives everyone an incentive to come to the table to develop reasonable codes. With that said, we don't have a law right now, so we are going do what we can with the limited tools we have. I mean I think they have the ability maybe in some ads cases with a lot of attention to use the bully pulpit to get some folks to come to the table to agree to some strong rule. But by and large they are not. They can probably get Google and Facebook and Yahoo and Microsoft into the room. But the smaller players really don't have any incentive, there is no requirement, there is no substantive law out there saying you have to tell people what you are doing with the information, let's create a safe harbor program to say what that means.

So I think the convenings in the meantime I think were hopeful, I think there is a role they can serve, but they are not going to be a comprehensive solution by any stretch of the imagination. I think there should be a law passed to give everyone reason to kind of come forward and say you know what, this is a reasonable code of conduct for my industry, I will agree to that and so consumers can have some certainty about what happens to their information online.

Mr. BUTTERFIELD. Would you support requiring all Web sites or mobile apps to have a privacy policy?

Mr. BROOKMAN. Yes. I think—I mean I think all Web sites are kind of required to today by California law. And I think industry self-regulation requires that. That said, we said that mobile applications should probably do the same. Private policies in and of themselves are not that great. We have had privacy policies 15 years. I don't think anyone on this panel or elsewhere thinks that solved privacy problems. They are dense, they are inscrutable, and they are not really recitations of what the companies are actually doing. They are just often reservations of rights. They are written defensively because the limited law the FTC has is just don't deceive. So the easiest way to get in trouble under FTC law is to go out of your way to make a misrepresentation.

Mr. BUTTERFIELD. Are these policies recommended by the FTC report?

Mr. BROOKMAN. I believe the FTC report thinks yes, they should require——

Mr. BUTTERFIELD. OK, let me go down the line and ask if you agree or disagree and then we will be done.

Mr. SZOKA. I think it is premature for Congress to legislate a prescriptive solution precisely because, as said, the devil here is in the details. It is a question of trans——

Mr. BUTTERFIELD. You are talking about apps and Web sites?

Mr. SZOKA. Well, in general. I think translating principles that are in the White House report and the legislation is premature. I am actually sympathetic to the idea of requiring Web sites and apps to disclose their privacy practices. I think there again though the question is about the implementation of that requirement and how to do it in a way that allows sites to accurately describe what

they are doing and give themselves up for enforcement if they fail do that, but not if they fail to put a round peg in a square hole.

Mr. BUTTERFIELD. I guess my question is would you support or not support requiring all Web sites and mobile apps to have a privacy policy?

Mr. SZOKA. I think in principle that is a much better place for legislation to start than actually prescribing practices.

Mr. BUTTERFIELD. So you don't have a fixed opinion on that?

Mr. SZOKA. I think it is a promising idea in principle but in practice——

Mr. BUTTERFIELD. Mr. Zuck, let's try you and then Ms. Horan.

Mr. ZUCK. I think the discussion here is an opportunity for me to reiterate some of the problems with big companies versus small companies. Mr. Brookman suggested that somehow the bully pulpit was more effective for big companies than small ones. But I would suggest the small companies because of their proximity to their customers are actually engaged in an ongoing dialogue and amending their policies on a day-to-day basis. Moms with apps, for example, have come up with a series of privacy icons in order to better communicate——

Mr. BUTTERFIELD. So do I take that as a yes or no?

Mr. ZUCK. Well, I think it is complicated question. I think the FTC's focus on sharing data with third parties unduly benefits large companies that own their own ad networks to the disadvantage of small businesses that wouldn't survive.

Mr. BUTTERFIELD. Let me try the next witness. We are running out of time. Ms. Horan.

Ms. HORAN. Based on California law today all of ours do have privacy policies.

Mr. BUTTERFIELD. And so you agree with extending that nationwide?

Ms. HORAN. [Nods.]

Mr. ZANEIS. I think the FTC report, the chairman was very clear it was not a regulation, it was not a law, it was best practice. So as a best practice companies should have privacy policies. What we shouldn't do is not make those a stagnant practice, we should innovate the ad choices icon as an example of notice innovation. Just as you pointed out, Mr. Butterfield, Google's new comprehensive privacy policy is a wonderful innovation for consumers to bring all of those disparate policies together in a simple, very clear way. That is what the industry should be doing instead of having codified very detailed privacy policies, and Justin and everybody else agrees it doesn't really works for consumers.

Mr. BUTTERFIELD. All right. Thank you.

Mrs. BONO MACK. Thank you, Mr. Butterfield. Mrs. Blackburn, you are recognized for 5 minutes.

Mrs. BLACKBURN. We are going to try to get you all out of here before the next vote series. Mr. Zaneis, let me ask you this one. I talked with the FTC about their report, their privacy report, and I think the thing is absolutely fascinating. But let me talk to you about this definition on the information brokers. And I am quoting from the report. The Commission recommends that Congress consider enacting targeted legislation to provide greater transparency for and control over the practices of information brokers. Further,

the report says that data brokers are companies that collect information from a wide variety of sources for the purpose of reselling such information to their customers for various purposes.

Now with my constituents in Tennessee, as we have discussed privacy, one of the things they have brought up to me most often is, hey, you know we don't want be classified as a data broker. This is not what we do. And they are very concerned about having a web, throwing a real big web out there. So given the broad and ill-defined language that is in this report, looking at it in that manner, how many data brokers would you say that the universe of data brokers is that the FTC is going to find in the U.S. marketplace?

Mr. ZANEIS. I think there is the real threat that they could cover basically the entire Internet, virtually every Web site, especially if you remember the fact that the FTC does not treat affiliates as first parties. They are now a data broker. Virtually every Web site has multiple sites.

Congressman, in your State you have more than 25,000 people that depend upon, their jobs upon Internet advertising directly, and I think all of them would fall under this bill.

Mrs. BLACKBURN. OK. So all of these innovators in the auto industry, and the financial service industry, and the banking industry, and the insurance industry, the entertainment industry, the health care industry, all of those guys that have been saying don't cast this net so widely, they would be trapped in that, or then it would be an enormous bureaucracy, I would think, that the FTC would have to build to start to regulate this.

Mr. ZANEIS. I think if they used their definition that you read aloud in the report, and they put the restrictions on that we have seen in other very narrowly-tailored data broker bills and have passed this committee in the past because they were so narrow, you absolutely would have an all-encompassing regulatory net.

Mrs. BLACKBURN. OK. Let me move on. I have got a poster that I want to put up and talk with you about. With Mr. Strickling and Mr. Leibowitz I talked a little bit about my concern over the EU-style Do Not Track. And I wanted to look at these ad revenues. And I have these out of an article, it is 11 Trends for 2011, eMarketer. Now, this shows that American Web sites would lose $33 billion over 5 years if Congress mandated the EU-style opt-in consent for interest-based advertising. So what I would like to hear from you all, looking at the potential of over a 5-year period losing that amount of money, do you agree with these numbers? Would it have that enormous an effect? How would you rank that? What are your thoughts?

Mr. Brookman, let me start with you and just work down. We have got 1 minute left.

Mr. BROOKMAN. I think this is an extrapolation of the Catherine Tucker MIT study which, again, did not actually say that they would lose this sort of massive amounts of money. That study basically just showed people ads in both Europe and the United States. They didn't know whether the ads were targeted or not, didn't know whether targeting was happening at all. So the people in the United States reacted—just said, they didn't buy, said they more

likely to buy a product as a result of an ad. As a result of that mere study—so the study did not show this at all.

Mrs. BLACKBURN. Let me move on. We are running out of time. Mr. Zaneis.

Mr. ZANEIS. The study measured the effectiveness of advertising. One thing we know is that based on the NAI study, targeted ads are 2.5 times more effective than nontargeted ads. I think actually the effect might be even higher, because some of these economic numbers are a little bit old, they are based on an IAB study of the Internet economy.

Mrs. BLACKBURN. OK.

Ms. HORAN. It would have huge implications. As I mentioned, just the CNET example, the ability to customize content and be able to provide an enhanced experience online.

Mrs. BLACKBURN. So you would say we are looking at at least that much. Mr. Zuck?

Mr. ZUCK. I definitely would agree that we are looking at at least this much. And you only need to take a step back from the numbers and realize that the EU data privacy practices have eliminated the ability really to introduce products for free. And that is why there is this distinction in the innovation between the two places.

Mrs. BLACKBURN. Mr. Szoka.

Mr. SZOKA. I think the chart is helpful because it is directional. It helps people understand the implications of what is otherwise a difficult thing to understand, which is the difference between two techniques and how they are used. And to say that of course this is an extrapolation, as Justin says, and the important thing is not the total number, but to say that that difference in, you know, technique A versus technique B because of a regulatory mandate does have a large effect.

Mrs. BLACKBURN. Excellent. I yield back.

Mrs. BONO MACK. I thank the gentlelady, and want to thank our panel very much for your hard work and your expertise in these areas. We thank you for being here today before us.

At this point, I am going to ask unanimous consent to submit for the record Commissioner Rosch's dissenting statement regarding the FTC's privacy report dated last Friday, March 26.

Mr. BUTTERFIELD. Without objection. And I would like to be recognized for a similar request.

[The information follows:]

Dissenting Statement of Commissioner J. Thomas Rosch
Issuance of Federal Trade Commission Report
Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers
March 26, 2012

Introduction

I agree in several respects with what the "final" Privacy Report says. Specifically, although I disagree that the consumer has traditionally ever been given any "choice" about information collection practices (other than to "take-it-or-leave-it" after reviewing a firm's privacy notice), I agree that consumers ought to be given a broader range of choices if for no other reason than to customize their privacy protection. However, I still worry about the constitutionality of banning take-it-or-leave-it choice (in circumstances where the consumer has few alternatives); as a practical matter, that prohibition may chill information collection, and thus impact innovation, regardless whether one's privacy policy is deceptive or not.[1]

I also applaud the Report's recommendation that Congress enact "targeted" legislation giving consumers "access" to correct misinformation about them held by a data broker.[2] I also support the Report's recommendation that Congress implement federal legislation that would require entities to maintain reasonable security and to notify consumers in the event of certain security breaches.[3]

---

[1] *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* ("Report") at 50-52.

[2] *Id.* at 14, 73.

[3] *Id.* at 26. I also support the recommendation that such legislation authorize the Commission to seek civil penalties for violations. However, despite its bow to "targeted" legislation, the Report elsewhere counsels that the Commission support privacy legislation generally. *See, e.g.*, *id.* at 16. To the extent that those recommendations are not defined, or narrowly targeted, I disagree with them.

Finally, I concur with the Report insofar as it recommends that information brokers who compile data for marketing purposes must disclose to consumers how they collect and use consumer data.[4] I have long felt that we had no business counseling Congress or other agencies about privacy concerns without that information. Although I have suggested that compulsory process be used to obtain such information (because I am convinced that is the only way to ensure that our information is complete and accurate),[5] a voluntary centralized website is arguably a step in the right direction.

Privacy Framework

My disagreement with the "final" Privacy Report is fourfold. First, the Report is rooted in its insistence that the "unfair" prong, rather than the "deceptive" prong, of the Commission's Section 5 consumer protection statute, should govern information gathering practices (including "tracking"). "Unfairness" is an elastic and elusive concept. What is "unfair" is in the eye of the beholder. For example, most consumer advocacy groups consider behavioral tracking to be unfair, whether or not the information being tracked is personally identifiable ("PII") and regardless of the circumstances under which an entity does the tracking. But, as I have said, consumer surveys are inconclusive, and individual consumers by and large do not "opt out" from tracking when given the chance to do so.[6] Not surprisingly, large enterprises in highly

---

[4] *Id.* at 14, 68-70.

[5] *See* J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Information and Privacy: In Search of a Data-Driven Policy, Remarks at the Technology Policy Institute Aspen Forum (Aug. 22, 2011), *available at* http://www.ftc.gov/speeches/rosch/110822aspeninfospeech.pdf.

[6] *See* Katy Bachman, *Study: Internet User Adoption of DNT Hard to Predict*, adweek.com, March 20, 2012, *available at* http://www.adweek.com/news/technology/study-internet-user-adoption-dnt-hard-predict-139091 (reporting on a survey that found that what Internet users say they are going to do about using a

concentrated industries, which may be tempted to raise the privacy bar so high that it will disadvantage rivals, also support adopting more stringent privacy principles.[7]

The "final" Privacy Report (incorporating the preliminary staff report) repeatedly sides with consumer organizations and large enterprises. It proceeds on the premise that behavioral tracking is "unfair."[8] Thus, the Report expressly recommends that "reputational harm" be considered a type of harm that the Commission should redress.[9] The Report also expressly says that privacy be the default setting for commercial data practices.[10] Indeed, the Report says that the "traditional distinction between PII and non-PII has blurred,"[11] and it recommends "shifting the burdens away from consumers and placing obligations on businesses."[12] To the extent the

---

Do Not Track button and what they are currently doing about blocking tracking on the Internet, are two different things); *see also* Concurring Statement of Commissioner J. Thomas Rosch, Issuance of Preliminary FTC Staff Report "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (Dec. 1, 2010), *available at* http://www.ftc.gov/speeches/rosch/101201privacyreport.pdf.

[7] *See* J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Do Not Track: Privacy in an Internet Age, Remarks at Loyola Chicago Antitrust Institute Forum (Oct. 14, 2011), *available at* http://www.ftc.gov/speeches/rosch/111014-dnt-loyola.pdf; *see also* Report at 9.

[8] Report at 8 & n.37.

[9] *Id.* at 2. The Report seems to imply that the Do Not Call Rule would support this extension of the definition of harm. *See id.* ("unwarranted intrusions into their daily lives"). However, it must be emphasized that the *Congress* granted the FTC underlying authority under the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108, to promulgate the Do Not Call provisions and other substantial amendments to the TSR. The Commission did not do so unilaterally.

[10] *Id.*

[11] *Id.* at 19.

[12] *Id.* at 23, *see also id.* at 24.

Report seeks consistency with international privacy standards,[13] I would urge caution. We should always carefully consider whether each individual policy choice regarding privacy is appropriate for this country in all contexts.

That is not how the Commission itself has traditionally proceeded. To the contrary, the Commission represented in its 1980, and 1982, Statements to Congress that, absent deception, it will not generally enforce Section 5 against alleged intangible harm.[14] In other contexts, the Commission has tried, through its advocacy, to convince others that our policy judgments are sensible and ought to be adopted. And, as I stated in connection with the recent *Intel* complaint, in the competition context, one of the principal virtues of applying Section 5 was that that provision was "self-limiting," and I advocated that Section 5 be applied on a stand-alone basis only to a firm with monopoly or near-monopoly power.[15] Indeed, as I have remarked, absent such a limiting principle, privacy may be used as a weapon by firms having monopoly or near-monopoly power.[16]

---

[13] *Id.* at 9-10. This does not mean that I am an isolationist or am impervious to the benefits of a global solution. But, as stated below, there is more than one way to skin this cat.

[14] *See* Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Committee on Commerce, Science and Transportation, United States Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), *reprinted in International Harvester Co.*, 104 F.T.C. 949, 1070, 1073 (1984) ("Unfairness Policy Statement") *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm; Letter from the FTC to Hon. Bob Packwood and Hon. Bob Kasten, Committee on Commerce, Science and Transportation, United States Senate, *reprinted in* FTC Antitrust & Trade Reg. Rep. (BNA) 1055, at 568-570 ("Packwood-Kasten letter"); and 15 U.S.C. § 45(n), which codified the FTC's modern approach.

[15] *See* Concurring and Dissenting Statement of Commissioner J. Thomas Rosch, *In re Intel Corp.*, Docket No. 9341 (Dec. 16, 2009), *available at* http://www.ftc.gov/os/adjpro/d9341/091216intelstatement.pdf.

[16] *See* Rosch, *supra* note 7 at 20.

There does not appear to be any such limiting principle applicable to many of the recommendations of the Report. If implemented as written, many of the Report's recommendations would instead apply to almost all firms and to most information collection practices. It would install "Big Brother" as the watchdog over these practices not only in the online world but in the offline world.[17] That is not only paternalistic, but it goes well beyond what the Commission said in the early 1980s that it would do, and well beyond what Congress has permitted the Commission to do under Section 5(n).[18] I would instead stand by what we have said and challenge information collection practices, including behavioral tracking, only when these practices are deceptive, "unfair" within the strictures of Section 5(n) and our commitments to Congress, or employed by a firm with market power and therefore challengeable on a stand-alone basis under Section 5's prohibition of unfair methods of competition.

Second, the current self-regulation and browser mechanisms for implementing Do Not Track solutions may have advanced since the issuance of the preliminary staff Report.[19] But, as the final Report concedes, they are far from perfect,[20] and they may never be, despite efforts to create a standard through the World Wide Web Consortium ("W3C") for the browser mechanism.[21]

---

[17] *See* Report at 13.

[18] Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312.

[19] Report at 4, 52.

[20] *Id.* at 53, 54; *see esp. id.* at 53 n.250.

[21] *Id.* at 5, 54.

More specifically, as I have said before, the major browser firms' interest in developing Do Not Track mechanisms begs the question of whether and to what extent those major browser firms will act strategically and opportunistically (to use privacy to protect their own entrenched interests).[22]

In addition, the recent announcement by the Digital Advertising Alliance (DAA) that it will honor the tracking choices consumers make through their browsers raises more questions than answers for me. The Report is not clear, and I am concerned, about the extent to which this latest initiative will displace the standard-setting effort that has recently been undertaken by the W3C. Furthermore, it is not clear that all the interested players in the Do Not Track arena – whether it be the DAA, the browser firms, the W3C, or consumer advocacy groups – will be able to come to agreement about what "Do Not Track" even means.[23] It may be that the firms professing an interest in self-regulation are really talking about a "Do Not Target" mechanism, which would only prevent a firm from serving targeted ads, rather than a "Do Not Track" mechanism, which would prevent the collection of consumer data altogether. For example, the DAA's Self-Regulatory Principles for Multi-Site Data do not apply to data collected for "market research" or "product development."[24] For their part, the major consumer advocacy groups may

---

[22] *See* Rosch, *supra* note 7 at 20-21.

[23] Tony Romm, *What Exactly Does 'Do Not Track' Mean?*, Politico, Mar. 13, 2012, *available at* http://www.politico.com/news/stories/0312/73976.html; *see also* Report at 4 (DAA allows consumer to opt out of "targeted advertising").

[24] *See Self-Regulatory Principles for Multi-Site Data,* Digital Advertising Alliance, Nov. 2011, at 3, 10, 11, *available at* http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf; *see also* Tanzina Vega, *Opt-Out Provision Would Halt Some, but Not All, Web Tracking*, New York Times, Feb. 26, 2012, *available at* http://www.nytimes.com/2012/02/27/technology/opt-out-provision-would-halt-some-but-not-all-

not be interested in a true "Do Not Track" mechanism either. They may only be interested in a mechanism that prevents data brokers from compiling consumer profiles instead of a comprehensive solution. It is hard to see how the W3C can adopt a standard unless and until there is an agreement about what the standard is supposed to prevent.[25]

It is also not clear whether or to what extent the lessons of the Carnegie Mellon Study respecting the lack of consumer understanding of how to access and use Do Not Track will be heeded.[26] Similarly, it is not clear whether and to what extent Commissioner Brill's concern that consumers' choices, whether it be "Do Not Collect" or merely "Do Not Target," will be honored.[27] Along the same lines, it is also not clear whether and to what extent a "partial" Do Not Track solution (offering nuanced choice) will be offered or whether it is "all or nothing." Indeed, it is not clear whether consumers can or will be given complete and accurate information about the pros and the cons of subscribing to Do Not Track before they choose it. I find this last

---

web-tracking.html?pagewanted=all.

[25] *See* Vega, *supra* note 24.

[26] *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*, Carnegie Mellon University CyLab, Oct. 31, 2011, *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf; *see also Search Engine Use 2012,* at 25, Pew Internet & American Life Project, Pew Research Center, Mar. 9, 2012, *available at* http://pewinternet.org/~/media/Files/Reports/2012/PIP_Search_Engine_Use_2012.pdf ("[j]ust 38% of internet users say they are generally aware of ways they themselves can limit how much information about them is collected by a website").

[27] *See* Julie Brill, Comm'r, Fed. Trade Comm'n, Big Data, Big Issues, Remarks at Fordham University School of Law (Mar. 2, 2012) *available at* http://ftc.gov/speeches/brill/120228fordhamlawschool.pdf.

question especially vexing in light of a recent study that indicated 84% of users polled prefer targeted advertising in exchange for free online content.[28]

Third, I am concerned that "opt-in" will necessarily be selected as the *de facto* method of consumer choice for a wide swath of entities that have a first-party relationship with consumers but who can potentially track consumers' activities across unrelated websites, under circumstances where it is unlikely, because of the "context" (which is undefined) for such tracking to be "consistent" (which is undefined) with that first-party relationship:[29] 1) companies with multiple lines of business that allow data collection in different contexts (such as Google);[30] 2) "social networks," (such as Facebook and Twitter), which could potentially use "cookies," "plug-ins," applications, or other mechanisms to track a consumer's activities across the Internet;[31] and 3) "retargeters," (such as Amazon or Pacers), which include a retailer who delivers an ad on a third-party website based on the consumer's previous activity on the retailer's website.[32]

---

[28] *See* Bachman, *supra* note 6.

[29] Report at 41.

[30] *Id.* Notwithstanding that Google's prospective conduct seems to fit perfectly the circumstances set forth on this page of the Report (describing a company with multiple lines of business including a search engine and ad network), where the Commission states "consumer choice" is warranted, the Report goes on to conclude on page 56 that Google's practices do not require affirmative express consent because they "currently are not so widespread that they could track a consumer's every movement across the Internet."

[31] *Id.* at 40. *See also supra* note 30. That observation also applies to "social networks" like Facebook.

[32] *Id.* at 41.

These entities might have to give consumers "opt-in" choice now or in the future: 1) regardless whether the entity's privacy policy and notices adequately describe the information collection practices at issue; 2) regardless of the sensitivity of the information being collected; 3) regardless whether the consumer cares whether "tracking" is actually occurring; 4) regardless of the entity's market position (whether the entity can use privacy strategically – *i.e.*, an opt-in requirement – in order to cripple or eliminate a rival); and 5) conversely, regardless whether the entity can compete effectively or innovate, as a practical matter, if it must offer "opt in" choice.[33]

Fourth, I question the Report's apparent mandate that ISPs (like Verizon, AT&T and Comcast), with respect to uses of deep packet inspection, be required to use opt-in choice.[34] This is not to say there is no basis for requiring ISPs to use opt-in choice without requiring opt-in choice for other large platform providers. But that kind of "discrimination" cannot be justified, as the Report says, because ISPs have "are in a position to develop highly detailed and comprehensive profiles of their customers."[35] So does any large platform provider who makes available a browser or operating system to consumers.[36]

Nor can that "discrimination" be justified on the ground that ISPs may potentially use that data to "track" customer behavior in a fashion that is contrary to consumer expectations. There is no reliable data establishing that most ISPs presently do so. Indeed, with a business

---

[33] *See id.* at 60 ("Final Principle").

[34] *Id.* at 56 ("the Commission has strong concerns about the use of DPI for purposes inconsistent with an ISP's interaction with a consumer, without express affirmative consent or more robust protection").

[35] *Id.*

[36] *Id.*

model based on subscription revenue, ISPs arguably lack the same incentives as do other platform providers whose business model is based on attracting advertising and advertising revenue: ISPs assert that they track data only to perform operational and security functions; whereas other platform providers that have business models based on advertising revenue track data in order to maximize their advertising revenue.

What really distinguishes ISPs from most other "large platform providers" is that their markets can be highly concentrated.[37] Moreover, even when an ISP operates in a less concentrated market, switching costs can be, or can be perceived as being, high.[38] As I said in connection with the *Intel* complaint, a monopolist or near monopolist may have obligations which others do not have.[39] The only similarly situated platform provider may be Google, which, because of its alleged monopoly power in the search advertising market, has similar power. For any of these "large platform providers," however, affirmative express consent should be required only when the provider *actually* wants to use the data in this fashion, not just when it *has the potential* to do so.[40]

---

[37] Federal Communications Commission, *Connecting America: The National Broadband Plan, Broadband Competition and Innovation Policy, Section 4.1, Networks, Competition in Residential Broadband Markets* at 36, *available at* http://www.broadband.gov/plan/4-broadband-competition-and-innovation-policy/.

[38] Federal Communications Commission Working Paper, *Broadband decisions: What drives consumers to switch – or stick with – their broadband Internet provider* (Dec. 2010), at 3, 8, *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2010/db1206/DOC-303264A1.pdf.

[39] *See* Rosch, *supra* note 15.

[40] *See, e.g.*, Report at 56.

Conclusion

Although the Chairman testified recently before the House Appropriations Subcommittee chaired by Congresswoman Emerson that the recommendations of the final Report are supposed to be nothing more than "best practices,"[41] I am concerned that the language of the Report indicates otherwise, and broadly hints at the prospect of enforcement.[42] The Report also acknowledges that it is intended to serve as a template for legislative recommendations.[43] Moreover, to the extent that the Report's "best practices" mirror the Administration's privacy "Bill of Rights," the President has specifically asked either that the "Bill of Rights" be adopted by the Congress or that they be distilled into "enforceable codes of conduct."[44] As I testified before the same subcommittee, this is a "tautology;" either these practices are to be adopted voluntarily by the firms involved or else there is a federal requirement that they be adopted, in

---

[41] Testimony of Jon Leibowitz and J. Thomas Rosch, Chairman and Comm'r, FTC, *The FTC in FY2013: Protecting Consumers and Competition: Hearing on Budget Before the H. Comm. on Appropriations Subcomm. on Financial Services and General Government*, 112th Cong. 2 (2012), text from CQ Roll Call, available from: LexisNexis® Congressional.

[42] One notable example is found where the Report discusses the articulation of privacy harms and enforcement actions brought on the basis of *deception*. The Report then notes "[l]ike these enforcement actions, a privacy framework should address practices that unexpectedly reveal previously private information even absent physical or financial harm, or unwarranted intrusions." Report at 8. The accompanying footnote concludes that "even in the absence of such misrepresentations, revealing previously-private consumer data could cause consumer harm." *See also infra* note 43.

[43] *Id.* at 16 ("to the extent Congress enacts any of the Commission's recommendations through legislation"); *see also id.* at 12-13 ("the Commission calls on Congress to develop baseline privacy legislation that is technologically neutral and sufficiently flexible to allow companies to continue to innovate").

[44] *See* Letter from President Barack Obama, *appended to* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

which case there can be no pretense that they are "voluntary."[45] It makes no difference whether the federal requirement is in the form of enforceable codes of conduct or in the form of an act of Congress. Indeed, it is arguable that neither is needed if these firms feel obliged to comply with the "best practices" or face the wrath of "the Commission" or its staff.

---

[45] *See* FTC Testimony, *supra* note 41.

Mrs. BONO MACK. The gentleman is recognized.

Mr. BUTTERFIELD. Thank you, Madam Chairman. I too would like to ask unanimous consent to include two reports in the record. One is the White House report dated February 2012 that we have talked about throughout this hearing, as well as the FTC report that is dated March 2012.

Mrs. BONO MACK. Without objection.

[The information is available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf and http://www.ftc.gov/os/2012/03/120326privacyreport.pdf]

Mrs. BONO MACK. And so as I mentioned earlier, this was the sixth in our series of privacy hearings in the past year. And if we have learned one thing, it is simply this, that there are no easy answers or quick fixes when it comes to protecting consumer privacy online. But as a subcommittee, we are going to keep working hard at it. And I look forward to our continued discussions.

I remind members that they have 10 business days to submit questions for the record, and ask the witnesses to please respond promptly to any questions you might receive. And the hearing is now adjourned.

[Whereupon, at 12:38 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

UNITED STATES DEPARTMENT OF COMMERCE
The Assistant Secretary for Communications and Information
Washington, D.C. 20230

AUG 9 2012

The Honorable Mary Bono Mack
Chairman
Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
House of Representatives
Washington, DC 20515

Dear Chairman Bono Mack:

Thank you for the opportunity to testify on March 29, 2012 before the Subcommittee on Commerce, Manufacturing, and Trade at the hearing entitled "Balancing Privacy and Innovation Does the President's Proposal Tip the Scale?" I appreciate your forwarding additional questions for the record to me on June 15, 2012.

My responses to the questions are enclosed. If you or your staff have any additional questions, please do not hesitate to contact me or James Wasilewski, NTIA's Director of Congressional Affairs, at (202) 482-1840.

Sincerely,

Lawrence E. Strickling

cc: The Honorable G.K. Butterfield, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Enclosure

Responses to Questions from the Honorable Mary Bono Mack

1. **Is "personal data", which is defined in the report as "any data, including aggregations of data, which is linkable to a specific individual" or "a specific computer or other device", a euphemism for "PII" (personally identifiable information)? With a definition so broad, what type of information would be left outside of that definition?**

The Privacy Blueprint uses the term "personal data" to describe information that is linkable to an individual or linked to a device. Depending on the circumstances, the definition can include a substantial amount of data. A broad definition is necessary to capture the wide array of data that implicates individual privacy interests. However, the privacy risks associated with personal data use vary widely, and the Privacy Blueprint sets forth guidance for handling personal data across a broad array of commercial settings, as appropriate for the scale, scope, and sensitivity of the data.

Moreover, data that cannot reasonably be associated with an individual does not fall under the Privacy Blueprint's definition of "personal data." Some commercially important practices depend on such data. For example, companies often collect and retain information from consumers that they do not use to analyze the activities of specific consumers or devices. Instead, this data is useful to develop an aggregate picture of how groups of consumers use a service or website. The insights gathered from this kind of analysis can lead to valuable improvements in products and services.

2. **The Framework endorses the consumer's ability to access and correct data held about them, but in a sliding scale based on the nature and sensitivity of the data. Can you please describe examples at both ends of the spectrum – data that would require access and correct (where not already provided by law) and data that would not require access and correct?**

The Privacy Blueprint discusses access, accuracy, and correction as related but distinct facets of a principle that protects consumers from the harmful consequences of erroneous information. Each of these elements serves a different purpose and creates different costs and benefits. Access enables consumers to learn about, and potentially obtain, information that companies have about them. Accuracy requires companies to take reasonable steps to ensure that the information they collect about consumers is correct. A right to correction (or deletion or suppression), as discussed in the Blueprint, is appropriate when consumers may be exposed to financial, physical, or material harm. Consumers' right to access and correct personal information is important. Consumers currently lack that right outside of sectors covered by laws like the Fair Credit Reporting Act and Health Insurance Portability and Accountability Act.

The right to access and accuracy is informed by the context of the data collection and user interaction. Factors used to determine the context can include the sensitivity of the data, the consequences that might result from inaccuracy, and the scope of the personal data.

Some circumstances dictate that consumers have robust means and opportunities to access and correct personal information about them that is held by others. For example, many web sites and mobile applications offer services that allow consumers to obtain background checks concerning social acquaintances. These services are often marketed as tools for consumers to vet prospective dates or social acquaintances. The background check reports can contain large amounts of personal information, including criminal background information. These sorts of background checks can be useful tools, but only if the data is accurate. The reports are not typically subject to the Fair Credit Reporting Act's access and accuracy requirements. If inaccurate criminal history information is listed in such a report, the risk of potential reputational harm is high. Therefore, the Privacy Blueprint would require that consumers have the opportunity to access and correct personal information in these circumstances.

Other circumstances might not require that consumers have the opportunity to correct personal information about them that is held by others, based on low risk for material harm to consumers. For example, Internet users often sign up for services that deliver free, daily email messages to them – one example is an online "recipe-a-day" service. These services can be very simple in design and implicate little personal information. A hypothetical service might only collect a consumer's email address, name, and hometown. This is personal information. If the consumer moves, the hometown information might then be incorrect, but there may be no consequences that flow from the error. In this particular context, the data at issue is small in scope and not particularly sensitive, and so it may not be necessary for the service to provide a way for consumers to correct the information, especially if the service provides consumers with an easy mechanism to cancel their subscription entirely.

3. **Many people have pointed to the Digital Advertising Alliance (DAA) agreement as a successful example of self-regulation. What is your opinion on the DAA agreement and do you intend to convene a multi-stakeholder group to revisit it?**

The Digital Advertising Alliance's commitment to "Do Not Track" is a positive step and has the potential to provide benefits to consumers. While a positive step, the Do Not Track system is still evolving – businesses, consumer advocates, and technical experts are currently working to implement the system.

NTIA is convening a different process, which will put great emphasis on openness and transparency. We identified mobile application transparency as the focus of the first process and convened the first meeting of that process on July 12, 2012. We currently have no plans to convene a process concerning Do Not Track. Given the range of outstanding privacy issues, we do not expect to focus on areas that have already been addressed through existing self-regulatory efforts, absent broad consensus that we should do so. Further, Do Not Track implementation is currently the subject of a multistakeholder process convened by the World Wide Web Consortium, and we would be very unlikely to establish a competing effort.

4. **How do you intend to resolve what are often vast differences between privacy advocates and the private sector during the multi-stakeholder process?**

NTIA's role in the privacy multistakeholder process is to provide a forum for discussion and consensus-building among stakeholders. In situations where stakeholders disagree over how best to interpret the Consumer Privacy Bill of Rights, we will help the parties reach clarity on what their positions are and whether there are options for compromise toward consensus, rather than substitute our own judgment.

We recognize that privacy advocates and the private sector may have different views on any number of issues. However, I think that all reasonable stakeholders can agree that transparency is critically important – companies must disclose relevant data practices to consumers. And transparency poses particular challenges in the mobile application context. We think that stakeholders can build on this basic agreement to develop a meaningful code of conduct concerning mobile application transparency. A code of conduct concerning mobile application transparency will not solve all privacy problems in the mobile space. However, a code of conduct concerning mobile application transparency will provide substantial, concrete benefits to consumers in a reasonable timeframe.

5. **If all negotiations leading up to the DAA agreement had taken place in open session, observers believe it would have been far more difficult to reach agreement. Do you anticipate some of the multi-stakeholder meetings will need to be closed?**

We are committed to ensuring that the multistakeholder process will be transparent. Given the broad range of interests in consumer data privacy, it is important for anyone who has an interest in the privacy multistakeholder process, whether or not they participate, to understand the basis for decisions made within the group. The proposals that are under discussion and participants' arguments for or against such proposals will be useful to gaining this understanding. It will be crucial for relevant information to be made available and accessible in a timely fashion.

We fully recognize, however, that stakeholders will not conduct all of their conversations in public. We expect that companies and consumer groups will want to hold discussions on their own to develop common perspectives. Our role will be to ensure that the stakeholders integrate these private discussions into a process that allows everyone a chance to work from common proposals and understand the public rationales that stakeholders offer to support their positions.

6. **Mr. Szoka testified that the Administration missed an opportunity to promote the concept of "smart disclosure" through machine-readable formats, which was proposed by Cass Sunstein, currently director of the Office of Information and Regulatory Affairs (OIRA). Have you considered that concept?**

The Privacy Blueprint encourages companies to make "smart disclosures" – to make personal data available in useful formats to properly authenticated individuals over the Internet. Smart disclosures may not be appropriate in all circumstances. But these sorts of disclosures can help consumers make more informed choices.

At NTIA's July 12, 2012 multistakeholder meeting, some stakeholders suggested that machine readable disclosures might be an appropriate part of a code of conduct regarding mobile application transparency. We look forward to stakeholders' efforts on this subject as they work toward drafting a code of conduct for mobile application transparency.

7. **One of the advantages of self-regulation is the ability to adjust rapidly to changes in technology. Will multi-stakeholder panels be able to move as quickly? Must those bound by an existing code of conduct seek the Administration's permission to revise it?**

We believe that multistakeholder processes can quickly produce meaningful codes of conduct. Multistakeholder institutions derive their legitimacy from the support and active participation of all stakeholders. Accordingly, they are more likely than regulatory regimes to adapt to change and evolve when the stakeholders demand it. Stakeholders are not required to seek the Administration's permission to revise a code of conduct. At heart, the multistakeholder process is bottom-up, not top-down. If stakeholders reach a broad consensus that a code of conduct is ripe for revision, they may initiate an open, transparent, consensus-based process to revise the code.

8. **What harms to individual consumers need to be addressed by legislation that cannot be adequately addressed under the FTC's existing unfairness jurisdiction?**

Unfortunately, companies do not always meet consumers' expectations of fair and responsible handling of personal data. As a result, consumers suffer individual harms. These harms include reputational harms, severe embarrassment, identity theft, and financial harms. Consumers can also suffer repeated inconveniences arising from the requirement that they manage personal data in the absence of consistent baseline principles. For example, consumers may find that they need to go through cumbersome or repetitive procedures to opt out of certain kinds of personal data collection or use. This kind of process may be manageable in small doses, but it does not work well for consumers in the long term, particularly when hundreds of different entities may collect information about them. These harms can result from practices that do not run afoul of the FTC's existing unfairness jurisdiction, but are nonetheless serious.

In areas that are not covered by existing Federal data privacy laws, consumers have few indications of how information about them is collected and used. Consumers are often surprised to learn that various companies hold personal data about them. They express concern about having their Internet use tracked. They worry about whether companies' privacy policies protect their information, or if they can understand the policies at all.

Privacy policies often do not address consumers in an intelligible, clear, and understandable manner, and have even further to go in the mobile realm. Many mobile applications lack privacy policies altogether. Too often, mobile privacy policies are not formatted with small screens in mind, effectively hiding important terms from consumers who are unwilling to scroll through dozens of screens of dense text. Clearer baseline protections would help consumers understand what they can expect from companies that handle data about them, and allow consumers to more meaningfully assess their choices.

Consumers and American businesses share a strong interest in better defining and protecting privacy interests in the digital age to maintain the trust that is necessary to keep the Internet growing and supporting innovation. Consumers should not be subject to constant uncertainty about what information is collected about them and how it may be used. They need and deserve a baseline set of protections. Conversely, companies should have clear obligations to meet, and companies that handle personal data responsibly should not be disadvantaged by those who behave carelessly or ignore consumer privacy preferences.

9. **If the harm requiring legislation is that the lack of consumer trust may cause consumers to stop adopting Internet services, where's your evidence for that beyond opinion surveys?**

Experts agree that lack of consumer trust is a real concern for Internet users. NTIA reached out to many stakeholders during the development of the Privacy Blueprint. During NTIA's outreach, we received comments from consumer groups, industry, and leading privacy scholars, and we saw broad agreement that large proportions of Americans do not fully understand and appreciate what information is being collected about them, and how they are able to stop certain practices from taking place.

Consumer advocates told us that consumers face privacy risks arising from unscrupulous practices – practices which lead to diminished consumer trust in Internet data collection, thus stunting growth and innovation. Consumer groups commented on individuals' inability to distinguish among companies' privacy practices, which may lead consumers to conclude that all companies engage in equally invasive practices. Some of the leading innovators in the Internet economy see things the same way. One leading IT company challenged the argument that baseline consumer data privacy protections would slow innovation. Instead, the company told us that well-crafted legislation can enable small business e-commerce growth. Other companies supported Federal privacy legislation; especially a baseline for privacy regulation that is flexible, scalable, and proportional. Uncertainty over keeping the trust of consumers online is as unsettling for some businesses as it is for consumers.

In addition, consumers victimized by identity theft arising from Internet transactions may lose trust in online services. Identity theft results from the theft of individuals' personal information and can result in financial, reputational, and other harms. Identity theft has been the most common consumer complaint to the Federal Trade Commission for the past 12 years. These complaints are not opinion surveys, but instead are specific allegations of unlawful practices filed by consumers. The FTC publishes an annual complaint list derived from the Consumer Sentinel Network, a secure online database of millions of consumer complaints available only to law enforcement. The list includes complaints to the Commission, law enforcement agencies, and non-governmental organizations. Of more than 1.8 million complaints filed in 2011, 15 percent were identity theft complaints.

Responses to Questions from the Honorable Cliff Stearns

10. **At the hearing we heard that allowing all consumers to access whatever data companies have about them presents significant technical challenges and could actually increase risk to consumers. But what about a narrower bill that would allow consumers to ask companies for categories of information that companies have on them. Wouldn't this alleviate the risk of harm to the consumer and burden on the company while at the same time help educate consumers on data collection?**

It is important for consumers to be able to access and correct personal data in a manner that is appropriate to the sensitivity of the information. We understand that providing access to data can pose technical challenges for companies in some circumstances. The key factor in providing access to personal data is context. When handling highly sensitive data, companies should provide robust access capabilities even in the face of technical challenges. When handling data that is less sensitive, it might be appropriate to provide less elaborate access capabilities.

One approach – allowing consumers to access categories of information, rather than all the underlying data – might be appropriate in some circumstances. But access to these categories may not in other contexts be a sufficient replacement for access to the full record of personal data held by a company about an individual.

11. **Are you familiar with my bill, H.R. 1528, the Consumer Privacy Protection Act of 2011? This bill calls for clear, easy to understand privacy policy statements and provides for the FTC to approve a five-year self-regulatory program. Would you support this bill advancing through the Subcommittee?**

At this time, the Administration has not taken a position on H.R. 1528, although we do support clear, easy to understand statements that make businesses' privacy policies and practices available to consumers.

In NTIA's view, the framework that the Obama Administration has proposed for consumer data privacy will provide consumers with transparency and control. The Privacy Blueprint includes a consumer privacy bill of rights that recognizes consumers' right to easily understandable and accessible information about privacy and security practices. The Blueprint also includes an open, transparent multistakeholder process to develop enforceable codes of conduct that implement the consumer privacy bill of rights in specific contexts, as well as specific authority for the Federal Trade Commission to enforce the consumer privacy bill of rights.

We look forward to working with you, other Members of Congress, privacy and consumer advocates, industry, and the FTC on this important issue.

Responses to Questions from the Honorable Jim Matheson

12. **One of the goals of the Administration's proposal is to create and then convene a group of stakeholders to develop legally enforceable codes of conduct that specify how the Consumer Privacy Bill of Rights applies in specific business contexts. I understand that the NTIA is currently seeking comments from interested stakeholders on how the multi-stakeholder process should work, what constitutes consensus and what issues should be addressed. Do you have any idea of when the first stakeholder meeting might be scheduled? What is the timeline for this process?**

NTIA received more than eighty responses to its request for comments on the privacy multistakeholder process. Individuals and entities in the commercial, academic, civil society, and government sectors filed comments. On July 12, 2012, NTIA held the first meeting of the privacy multistakeholder process in the Department of Commerce auditorium, focused on mobile application transparency. Nearly 300 people participated in the event, more than 200 of them in person. The first meeting provided a forum for stakeholders to have an initial discussion concerning mobile app transparency, and also to discuss the schedule and format of future meetings. The next meeting is scheduled for August 22, 2012.

13. **As we all know, the borderless nature of the Internet is one of the factors that makes the Internet a strong economic driver. It allows companies of all sizes to reach a global audience with very little effort or overhead. Many U.S. based companies have used the Internet to create tremendous business opportunities around the world. Although the Internet has no borders, countries still have laws and regulations governing how data can be used and transferred. Complying with these various privacy laws can be extremely difficult for businesses as they engage in global commerce. One of the chapters in the Administration's proposal discusses the importance of promoting international interoperability in privacy laws by pursuing mutual recognition. Is this an effort that the Department of Commerce is going to undertake? What steps are you going to take to promote greater harmony among international privacy laws? Does the Department of Commerce have any concerns with the latest EU Data Directive and how that might impact U.S. based businesses?**

NTIA recognizes that interoperability helps ease privacy compliance burdens for companies doing business globally.

We are working closely with our counterparts in the Commerce Department, including at the International Trade Administration, and throughout the Executive Branch to pursue greater interoperability of privacy frameworks. Promoting interoperability is an important objective of the National Science and Technology Council Subcommittee on Privacy, which is co-chaired by Department of Commerce General Counsel Cameron Kerry. This subcommittee's international engagement working group, which is co-chaired by NTIA, develops interagency positions on a number of international consumer privacy issues, including interoperability.

We are committed to demonstrating to our international partners that a principles-based framework, combined with a stakeholder-driven process to create more specific guidelines, can

effectively address consumer data privacy issues. Enacting baseline consumer privacy legislation could also expand international recognition of codes of conduct. Legislation would clarify the legal standards that underlie codes of conduct as well as their enforceability, which would reinforce our commitment to consumer privacy and influence global Internet policy debates.

The Commerce Department continues to promote current enforceable codes of conduct that play an important role in global interoperability. For example, the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks are a source of legally enforceable privacy commitments and will continue to play a critical role in facilitating transatlantic trade. Another example, the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules system ("CBPR"), was finalized and publicly announced during the APEC Leaders' Summit in November 2011. The United States, represented by the Department of Commerce and the Federal Trade Commission, was part of a dedicated group of APEC member economies that developed the CBPR system. The CBPR system does not seek to harmonize or homogenize domestic privacy legislation; rather, it focuses more narrowly on the issue of how to ensure a basic consistency of consumer privacy protections, including enforcement, as data moves from one member economy to the other. In July, Acting U.S. Commerce Secretary Rebecca Blank announced the United States' participation in the CBPR system.

The United States and European Union are both committed to protecting consumer privacy and encouraging innovation, entrepreneurship, and supporting jobs and growth. This commitment is underscored in the March 19, 2012 U.S.-EU Joint Statement on Privacy from then-Commerce Secretary Bryson and EU Commission Vice President Viviane Reding. The European Commission recently proposed a new legal framework for the protection of personal data in the EU. The proposed legal framework consists of two legislative proposals – a Regulation and a Directive. The United States has expressed concerns about the proposed General Data Protection Regulation ("Regulation").

The Department of Commerce has some specific thoughts about the proposed Regulation. For example, several Articles of the Regulation grant broad technical standards-setting authority to the European Commission. We are concerned that such authority could lead to overly-prescriptive technical standards, which could in turn fragment global markets and adversely affect interoperability. Instead, we support privacy regulations that focus on achieving objectives as opposed to mandating technologies. Technical standards developed within consensus-based, multistakeholder organizations are the bedrock of the open, globally-interconnected Internet. The openness, transparency, and user choice of today's Internet can best be sustained and advanced in a world in which all stakeholders participate in relevant decision making, rather than one in which governments, or particular groups of stakeholders, dominate. Some aspects of the proposed Regulation may be inconsistent with this approach.

The Department of Commerce is in frequent contact with officials from the European Commission, European Member States and European Parliament. We have reached out to these European colleagues to convey some of our views on the proposed EU Regulation and its potential impact on cross border data flows. Other U.S. government agencies, such as the Department of State, have also conveyed their views on the proposed EU Regulation to their

European colleagues. We will also continue to address this issue in the National Science and Technology Council Subcommittee on Privacy, which will inform our continued engagement with the EU on improving interoperability between our consumer data privacy frameworks.

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

June 15, 2012

The Honorable Jon Leibowitz
Chairman
Federal Trade Commission
600 Pennsylvania Avenue
Washington, D.C. 20580

Dear Chairman Leibowitz,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Thursday, March 29, 2012, to testify at the hearing entitled "Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?"

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 respond to these questions by the close of business on Friday, June 29, 2012. Your responses should be e-mailed to the Legislative Clerk, in Word or PDF format, at Kirby.Howard@mail.house.gov.

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: G.K. Butterfield, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Attachment

The Honorable Mary Bono Mack

1. The Framework indicates the consumer privacy bill of rights does not replace existing privacy law, but to the extent it provides additional rights or protections, does that alter existing privacy laws you enforce? Do existing laws need to be amended if Congress were to statutorily define a privacy bill of rights?

Answer: In the final privacy report, the Commission was careful to note the limitations on its framework. The report states that "[t]o the extent that the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC." Thus, the final privacy report did not alter existing privacy laws. Should Congress decide to statutorily define a privacy bill of rights, Congress would determine at that point the extent to which the bill of rights would supplant existing statutes or would, alternatively, fill in gaps that existing statutes do not address.

2. You repeated your call for a more robust "Do Not Track" function that is persistent, covers all parties that track consumers, and opts them out of any behavioral data collection beyond the context of the interaction.

    a. What does "context of the interaction" mean (the Administration's Framework also incorporates this concept)? Does context mean data can only be used for those purposes that are obvious to the consumer – i.e., a consumer provides a retailer her address to mail a purchase? What if information is collected for the purpose of driving advertisements?

Answer: The context of the interaction standard is intended to encompass uses of data that are consistent with the context of a particular transaction or with the consumer's relationship with the business. For example, if a consumer is purchasing a book on an online retailer's website, the consumer would understand from the context of that transaction that the retailer would use and potentially share the consumer's address to deliver the book. The consumer would also anticipate that the retailer would use the consumer's information to offer similar products to market back to the consumer. Similarly, a consumer would understand that an online retailer would need to use information about its customers to (1) protect against fraud and security breaches and (2) improve its website, as long as such improvements don't involve sharing information with third parties.

When we used this phrase in connection with the Do Not Track discussion, we were referring to a few basic activities that are important and necessary to the proper functioning of businesses, such as preventing click fraud or using de-identified data for analytics purposes. The context of the interaction does not, however, include general, undefined activities that would create broad carve outs to Do Not Track and allow third parties to drive additional advertisements without offering consumer choice.

    b. Who is collecting data for purposes outside of advertising?

Answer: As we discussed in our privacy report, the information broker industry is largely opaque, and a detailed analysis of the activities of all information brokers is challenging. We do know, however, that there are companies collecting information from a variety of sources and using it or selling it for

purposes other than advertising. Our recent case against Spokeo is a good example. The FTC alleged that Spokeo collected information about consumers from hundreds of online and offline sources, including social networks. It created profiles and sold those profiles to human resource professionals, job recruiters and others for employment purposes. The FTC charged that this violated the Fair Credit Reporting Act and reached a settlement with the company requiring it to pay $800,000 and submit to significant injunctive provisions. Although many consumers may be aware of the activities of the three major consumer reporting agencies, it is unlikely that many consumers have ever heard of Spokeo, or any of the other information brokers that may be operating behind the scenes and using data for non-advertising purposes.

c. What data are they collecting that is personally identifiable that the consumer does not give them freely?

Answer: It is very unlikely that consumers willingly provided Spokeo with their personal data – including name, address, email address, hobbies, ethnicity, religion, social networking information, and photos – because most consumers did not realize that Spokeo existed.

It is equally unlikely that any of the women whose location was obtained and published by a recent controversial mobile application marketed to people interested in a "one-night stand" knew that their "check-ins" on foursquare and Facebook were being collected, re-packaged, and sold for other purposes. *See, e.g.*, Nick Bilton, N.Y. Times BITS Blog, *Girls Around Me: An App Takes Creepy to a New Level* (Mar. 30, 2012), *at* http://bits.blogs.nytimes.com/2012/03/30/girls-around-me-ios-app-takes-creepy-to-a-new-level/.

Our recent cases against Facebook and Myspace offer additional examples of sharing of personally identifiable information without authorization. In both those cases, we alleged that the companies promised consumers they would not share personally identifiable information with advertisers and yet the companies did just that, sharing with advertisers information about the users maintained on their social networking profiles.

d. Why are the current Do-Not-Track browser mechanisms insufficient?

Answer: Some browsers have implemented a setting that can send a Do Not Track signal to websites consumers visit. Currently, there is no browser setting that is universally honored. The Digital Advertising Alliance (DAA) has agreed to honor browser Do Not Track settings by the end of the year, but not all trackers are members of the DAA. The W3C has brought together a broader set of stakeholders to set a standard for what a company should do when it receives a Do Not Track browser signal. Once stakeholders achieve consensus, we are confident that consumers will have an effective Do Not Track mechanism.

e. How do you envision the implementation of a universal "Do Not Track" system in practicality? Would the "Do Not Track" system consist of a technological solution that actually prevents tracking if an individual invokes it or a legal solution that requires each individual site to honor an individual's request?

Answer: We have stated that consumers should be able to exercise meaningful choice and control about the collection of their data. The W3C is currently working on a standard for Do Not Track that would define how it will operate in practice. At this point, we do not believe that Do Not Track will operate as a technological block on tracking or collection. Instead, Do Not Track will specify a protocol for the transmission of a user's preference not to be tracked and for websites and other companies to respond to and honor that preference.

f. How do the recent DAA rules that block secondary uses of data and commitment to honor persistence affect the Commission's opinion regarding Do Not Track?

Answer: The DAA's commitments to honor persistence and to address some secondary uses of collected data are very important commitments by the advertising industry. We will watch closely to see how these commitments are implemented. At the same time, DAA members are making very important contributions to the discussions taking place in the W3C, and we are optimistic that industry participants and other stakeholders can reach consensus on a Do Not Track standard through the W3C.

3. One of the chief concerns from all parties is whether the Administration's multi-stakeholder process can yield results. The FTC hosted a number of stakeholder forums where participants discussed views from across the spectrum. Based on this experience and knowledge, what is your confidence level in what are essentially stakeholder negotiations?

Answer: I am optimistic that the Administration's multi-stakeholder processes can yield results. Although there was vigorous debate on key issues at our privacy roundtables, we also saw significant agreement on a number of key issues, such as the need for improved transparency and consumer choice about online tracking.

4. The term "harm" in the privacy context does not have universal meaning. When one person feels their privacy has been invaded is different from when another person feels his or her privacy has been invaded because the harm depends on one's personal attitude about privacy. When there is no universal meaning to what harm is in the privacy context, how can the FTC define harm?

Answer: For purposes of enforcing the FTC Act, we are bound by Section 5, which prohibits deceptive and unfair acts or practices. The question of harm arises in our unfairness cases. Section 5 sets forth a three-part test we must apply in order to find a particular practice unfair: 1) there must be a likelihood of substantial injury, 2) not reasonably avoidable by consumers, and 3) not offset by countervailing benefits. The cases we have brought alleging unfairness have all involved injury that is clear. We will continue to follow the dictates of Section 5 in future enforcement actions.

In our privacy report, we acknowledged that the concept of harm may extend beyond financial or physical impacts or unwanted intrusions and may include, for example, the unexpected revelation of private information, including both sensitive information (*e.g.*, health information, precise geolocation information) and less sensitive information (*e.g.*, purchase history, employment history) to unauthorized third parties. As one example, in the Commission's case against Google, the complaint alleged that Google used the information of consumers who signed up for Gmail to populate a new social network, Google Buzz. The creation of that social network in some cases revealed previously private information about Gmail users' most frequent email contacts.

Similarly, the Commission's complaint against Facebook alleged that Facebook's sharing of users' personal information beyond their privacy settings was harmful.

We acknowledge that these concerns may be viewed or weighed differently by different consumers and that's why we proposed that companies implement best practices for increased transparency and consumer choice and for scalable access to the information maintained about them. Consumers should understand and have a choice about when their data is collected, and when private information may be shared or used in ways they did not expect when they first provided the information. This allows those consumers who care about the misuse of their personal data to be aware of and exercise a choice about it.

5. One of the practices you recommend in your most recent privacy report is providing simpler and more streamlined choices to consumers. Google recently simplified and streamlined its privacy policies, and some people immediately criticized the policy as not explaining the company's practices in enough detail. What is your view on Google's effort to simplify and streamline its privacy policies?

Answer: Although I should not comment on a particular company's practices, I can say that we encourage companies to engage in creative ways to simplify and streamline their privacy policies. We have long maintained that the traditional model of lengthy privacy policies is not an effective way to let consumers know what a company is doing with consumers' personal data and what choices they have with respect to those practices. Instead, for example, our privacy report encourages companies to develop simpler, more streamlined notices to consumers that are easy to understand, and to provide just in time choices to consumers so that they can make informed decisions about their data.

The Honorable Cliff Stearns

1. At the hearing we heard that allowing all consumers to access whatever data companies have about them presents significant technical challenges and could actually increase risk to consumers. But what about a narrower bill that would allow consumers to ask companies for categories of information that companies have on them. Wouldn't this alleviate the risk of harm to the consumer and burden on the company while at the same time help educate consumers on data collection?

Answer: Our privacy report called on companies to provide reasonable access to the data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use. For example, access and correction rights are extremely important when data is used for an eligibility decision, such as employment or insurance purposes. It is less critical when the data is used purely for marketing purposes where, as you suggest, consumers could ask companies for categories of information the companies have about them and have the option to suppress data for future marketing use. Some companies that use data for marketing purposes have adopted the practice of giving consumers access to the categories of information about them, and we think this is a positive step for industry.

2. Are you familiar with my bill, H.R. 1528, the Consumer Privacy Protection Act of 2011? This bill calls for clear, easy to understand privacy policy statements and provides for the FTC to approve a five-year self-regulatory program. Would you support this bill advancing through the Subcommittee?

Answer: Although the Commission has not taken a position on H.R. 1528, we support the goals of this bill, and we are happy to work with you and your staff on this legislation.

The Honorable Jim Matheson

1. Chairman, recently the FTC released their long awaited report on privacy, entitled Protecting Consumer Privacy in an Era of Rapid Change. As in your preliminary report, Do Not Track is a key focus and the report consistently calls on industry to provide consumers access to Do Not Track mechanisms that offer consumers a universal, one-stop choice mechanism for online behavioral tracking. Do Not Track has been a very hotly debated issue since you first mentioned it at a Senate Commerce Committee hearing in 2009. There has also been concern from those within the security community that a Do Not Track mechanism could impede the ability of companies to monitor and prevent fraud and abuse on their sites. Can you speak to this concern?

Answer: We agree that it is important that companies be able to monitor and prevent fraud and abuse on their sites. However, we believe that an effective Do Not Track mechanism can be developed and implemented in a manner that would not undercut companies' abilities to engage in security and fraud detection. In particular, we know that security and fraud detection are receiving significant attention in the discussions currently taking place through the W3C standards-setting group. We expect that any standard developed by the W3C will take into account these very important concerns.

Responses to Questions for the Record of
Berin Szoka
President, TechFreedom[1]
on
Balancing Privacy and Innovation:
Does the President's Proposal Tip the Scale?

Hearing of the Subcommittee on Commerce, Manufacturing, and Trade
Energy & Commerce Committee
United States House of Representatives

March 29, 2012[2]

The Honorable Mary Bono Mack

1. You suggested that before granting the FTC new authority in the privacy arena, Congress should wait to learn from the self-regulatory process. By its nature, it may take quite a while before that process plays out fully. What should happen in the meantime?

My recent testimony before the Senate Commerce Committee[3] expanded upon my testimony before your committee. Congress should focus on enhancing the existing legal framework as a more resilient approach to privacy concerns than enacting "baseline" legislation in six ways:

1. Ensure the FTC has adequate institutional resources and expertise.
2. Require the FTC to explain how it has applied its baseline doctrines of consumer protection—deception and unfairness—in past privacy cases. A retrospective analysis in the form of guidelines analogous to the Antitrust Guidelines issued jointly by the FTC

---

[1] Berin Szoka (bszoka@techfreedom.org, @BerinSzoka) is President of TechFreedom, a non-profit, non-partisan technology policy think tank. He has written and commented extensively on consumer privacy. In particular, he has testified on privacy and the self-regulatory process before the House Energy & Commerce Committee on March 29, 2012, available at http://tch.fm/KCrz8k ("Szoka Testimony I"),and the Senate Commerce Committee on June 28, 2012, available at http://techfreedom.org/sites/default/files/Szoka%20Testimony%20at %20Senate%20Privacy%20Self-Regulation%20Hearing%20v2.pdf ("Szoka Testimony II").

[2] Available at http://energycommerce.house.gov/hearing/balancing-privacy-and-innovation-does-presidents-proposal-tip-scale

[3] *See* Szoka Testimony II, *supra* note 1.

and Department of Justice[4] would serve two ends: (1) making the future course of the FTC's quasi-common law of privacy more predictable and (2) identifying areas the FTC truly cannot address without new legislative authority. In particular, the FTC ought to explain the scope of harm under the unfairness doctrine.

3. Require the FTC to do more to explain its application of the unfairness and deception doctrines in the future, such as through regular updates to these guidelines, better justifying consent decrees, and issuing no-action letters and advisory opinions.
4. Craft new legislation, if at all, to address (1) non-conjectural harms that cannot be addressed by a more robust development of quasi-common law by the FTC, (2) that are not outweighed by countervailing benefits, and (3) that consumers themselves cannot reasonably avoid—in other words, to focus a realistic assessment of costs and benefits, and a preference for user empowerment over regulation. This is the basic concept behind the unfairness doctrine but there may well be harms that do not fit into the unfairness doctrine that nonetheless merit government intervention—and that would be better addressed through targeted legislation than by attempting to shoehorn them into unfairness by expanding the definition of "substantial injury." For example, this might include restrictions on employers' ability to obtain the social networking credentials of their employees.
5. Explore the use of "smart disclosure" to empower consumers through greater transparency as an alternative to prescriptive mandates, starting with increasing the kinds of information collected by data brokers (properly defined).
6. Ensure that self-regulation in name does not become *co*-regulation in fact, where government regulates by having final approval to certify industry codes of conduct—or simply through extra-legal pressure. No matter how well-intentioned, "agency threats" undermine the rule of law.

In addition, Congress should take two other steps:

7. Support education - If the problem is a lack of consumer awareness, Congress should fund consumer education campaigns, as it has done in the past for privacy and child safety.
8. Focus on getting government's house in order - the greatest threat to our privacy lies with government itself, in that Congress has failed to update laws intended to extend Fourth Amendment Protections to data held by third parties.[5]

---

[4] Dept. of Justice, Guidelines and Policy Statements, http://www.justice.gov/atr/public/guidelines/.

[5] See Joint Letter to S. Comm. on Judiciary in support of ECPA Reform (Sep. 17, 2012), at http://net.educause.edu/ir/library/pdf/EPO1212.pdf.

Elaboration upon these points follows immediately below.

FTC Resources & Expertise

Congress should assess whether the FTC has adequate institutional resources and expertise. If the FTC had heeded Peter Swire's call for the FTC to build a an office of information technology five years ago,[6] our layered privacy approach would today be far more effective in protecting consumers and ensuring their trust, and less easily dismissed as inadequate by foreign privacy regulators. Chairman Leibowitz deserves credit for appointing the agency's first Chief Technologist. But even with someone as talented as Ed Felten in that position, the FTC is still way behind the curve: His title was not Chief Technology *Officer* because there is no office behind him to support the agency.

The FTC needs a clear strategic plan outlining:

1. How to build the in-house technical expertise it needs (beyond basic IT infrastructure) to identify enforcement actions, support successful litigation, monitor compliance, and conduct long-term planning and policy work, and
2. The resources necessary to achieve that goal through a combination of re-prioritizing current agency spending and additional appropriations.

Importantly, this organization should function as a cohesive team that meets the needs for technical expertise of all the FTC's bureaus and offices (including the Bureau of Competition). A stand-alone organization could, like the Bureau of Economics, better attract and retain talent.

FTC Quasi-Common Law

The proper measure of the FTC's effectiveness is not how many suits it successfully settles, but how well it builds a quasi-common law of privacy that can guide companies pushing the envelope with new data-driven technologies—without stifling innovation that ultimately serves consumers. The chief problem today is that we have essentially no privacy case law to look to, so companies have only FTC complaints and consent decrees to guide them in predicting the course of privacy law. These documents offer very little explanation of how the facts of a particular case satisfy the FTC's Policy Statements on unfairness and deception. And these summary assertions are never tested in court (at least until the recent *Wyndham* case), both because of the cost of litigation relative to settlement, and because of the cost to a defendant company of bad publicity from being perceived as anti-privacy exceed the benefits of taking the FTC to court—even when they would likely prevail given the FTC's overreach. While this should

---

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

reassure us that reputation markets exert far greater pressure to discipline companies on privacy than is commonly appreciated,[7] it also means that we lack the key ingredient for building a true common law: judicial scrutiny in an adversarial process.

It is possible that Wyndham's pending challenge may clarify some of these issues.[8] But unless the court significantly curtails the scope of the FTC's authority, which seems unlikely given the facts of the case, this case may well be only a brief interruption to the general and long-established pattern of the FTC acting without judicial scrutiny. The forces that keep privacy adjudication out of the courts and prevent development of privacy common law by judges are not likely to be easily overcome by FTC—or even Congressional—action. So we need to find alternative ways to replicate the adversarial process of careful analysis by which courts build upon simple rules to address the challenges of a complex world. I suggest the following nine possible ways for the FTC to make better use of its existing authority to build a quasi-common law:

1. The Commission (or individual Commissioners) should provide greater analysis of its rationale under its Unfairness and Deception Policy Statements for issuing each consent decree.

2. Congress should hold hearings to explore how the model of the Tunney Act could be applied to consumer protection settlements, to require judicial approval of the consent decrees by which the FTC builds the quasi-common law of privacy, just as the DOJ must get approval for antitrust settlements.[9] This would ensure some degree of oversight of the Commission's legal analysis—and give the agency an incentive to explain that analysis more.

3. The FTC should, when it closes an investigation by deciding not to bring a complaint, issue a "no action" letter explaining why it decided the practice at issue was lawful under Section 5.[10] Such letters, issued by other agencies like the Securities and Exchange Commission, provide an invaluable source of guidance to innovators. Congress should even consider requiring the FTC to issue such letters.

4. The FTC should consider how it could use advisory opinions more effectively to provide guidance to industry on how the agency might evaluate new privacy practices—especially for companies working on the cutting edge of technology, which are often

---

[7] See Daniel Klein, *Reputation: Studies in the Voluntary Elicitation of Good Conduct* (1997), at http://books.google.com/books/about/Reputation.html?id=p3gUN-oD2n0C.

[8] *See* FTC v. Wyndham, Case No. CV 12-1365-PHX PGR (D. Ariz.).

[9] 15 U.S.C. §16 (2012).

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

small and early-stage. The FTC issues such letters on a wide range of topics,[11] yet does not appear to have issued advisory opinions regarding the application of Section 5 to privacy.

5. Congress should reassert the vital oversight it exercised in 1980 and 1983 when it ordered the agency to issue the Policy Statements on Unfairness and Deception. At a minimum, the FTC should be required to explain, in detailed analysis, how it has applied those venerable standards in past privacy enforcement cases, and how it plans to do so in the future—because it is "easier to learn from history than it is to learn from the future."[12] Such guidelines are routine in other areas, and provided for in the Commission's current procedures.[13] Indeed, the antitrust guidelines issued by the FTC and DOJ form a key element of the American common law of competition. The FTC has issued a number of Guides[14] to explain its approach to consumer protection—but none for consumer privacy.[15] The FTC's recently issued Privacy Report is no substitute for such a Guide because it describes what companies ought to do on privacy rather than how the FTC has decided companies must not act, and why. Indeed, the Report has little grounding in the twin Policy Statements that are supposed to be the FTC's lodestars. To replicate some of the adversarial nature of actual litigation, the process of drafting such guidelines must be the result of a substantive dialogue with affected stakeholders, and it must be subject to involved oversight from the full Commission and from Congress.

6. In particular, the FTC must clarify the boundaries of privacy harm under the Unfairness Doctrine. The FTC's leadership seems to be trying to have it both ways: playing down publicly what the agency can do with its existing legal authority (to support their argument for new statutory authority) while, at the same time, making bold claims about the scope of harm in their enforcement actions. If the concept of harm is

---

[11] 16 C.F.R .§ 1.1 (2012) ("Any person, partnership, or corporation may request advice from the Commission with respect to a course of action which the requesting party proposes to pursue. The Commission will consider such requests for advice and inform the requesting party of the Commission's views, where practicable, under the following circumstances... (1) The matter involves a substantial or novel question of fact or law and there is no clear Commission or court precedent; or (2) The subject matter of the request and consequent publication of Commission advice is of significant public interest."); see also Judith A. Moreland, Overview of the Advisory Opinion Process at the Federal Trade Commission, available at http://www.ftc.gov/bc/speech2.shtm.

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

[13] Federal Trade Comm'n, FTC Operating Manual §8, *available at* http://www.ftc.gov/foia/ch08industryguidance.pdf.

[14] Federal Trade Comm'n, FTC Bureau of Consumer Protection - Resources: Guidance Documents, http://ftc.gov/bcp/menus/resources/guidance.shtm (last visited June 26, 2012).

[15] Federal Trade Comm'n, Legal Resources | BCP Business Center, http://business.ftc.gov/legal-resources/48/33 (last visited June 26, 2012).

stretched too far, the Unfairness Doctrine will become again, as it was in the 1970s, a blank check for the FTC to become a "second national legislature" capable of regulating business practices across the economy.[16] I explained my concerns about the potential for the unfairness doctrine to be abused, but also my belief that the doctrine should be used to the greatest extent with the 1980 Policy Statement, in my March testimony before this Committee.[17]

7. Hold a public workshop on how the FTC could use its existing Magnuson-Moss rulemaking powers[18] to apply the Unfairness and Deception Doctrines industry-wide, rather than through adjudication.

8. Congress should hold hearings to explore making the FTC subject to the same cost-benefit analysis that all Executive Branch agencies have long been required to perform (but not independent agencies like the FTC and FCC).[19] Ideally, such a requirement should apply in some form to all consent decrees, since these are the key means by which the FTC regulates, but at a minimum, the requirement should apply to all reports issued by the FTC.

9. Congress should ensure the FTC has the adequate resources to engage in this detailed analysis. To dismiss the current legal model as inadequate simply because it has not been fully utilized, and to adopt instead a new legislative framework whose true costs are unknown, would be truly "penny wise, pound foolish." Given the clear need to reduce federal spending across the board, and the decidedly mixed record of antitrust law in actually serving consumers, Congress could simply reallocate funding from the FTC's Bureau of Competition—or, more dramatically, consolidate antitrust enforcement at the DOJ and allocate the cost savings from streamlining to the FTC's Bureau of Consumer Protection.[20]

I expand upon some of these suggestions below.

---

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

[17] *See* Szoka Testimony I, *supra* note 1.

[18] See generally, *FTC Operating Manual*, Chapter 7, http://www.ftc.gov/foia/ch07rulemaking.pdf

[19] Executive Order 13563 -- Improving Regulation and Regulatory Review, *available at* http://www.whitehouse.gov/the-press-office/2011/01/18/improving-regulation-and-regulatory-review-executive-order.

[20] *See* William E. Kovacic, *The Institutions af Antitrust Law: How Structure Shopes Substance*, 110 Mich. L. Rev. 1019, 1034 (2012) (identifying several problems with federal duality of antitrust jurisdiction).

Codification When Necessary

As explained by Nobel Prize winner, F.A. Hayek, in *Law, Legislation, and Liberty* (1973), the common law is the best system for coordinating the behavior of persons in light of dispersed knowledge. Legislation is best used to correct established problems resulting from the common law.[21] The FTC should first allow a quasi-common law of privacy to emerge before pushing for legislation to correct a problem which may not exist. While many would insist that the FTC model has failed, necessitating legislation, I do not think we can say the FTC model has really been tried until the FTC is required—either by Congress, by the courts, or perhaps by a Chairman with a very different approach—to explain its analysis thoroughly and consistently. Codification of common law can be useful to promote certainty in the law, but first the common law must be allowed to develop.

Rather than dismissing its existing Magnuson-Moss rulemaking authority[22] as "medieval" in order to justify Chairman Leibowitz's push for streamlined rulemaking authority,[23] the agency should make use of the powers it already has to help create this quasi-common law using its Section 5 authority to prosecute "Unfairness" and "Deception", as outlined above.

If the FTC uses this power to the fullest, it will reveal those areas where codification is appropriate—either by Congress or by the FTC itself. The latter means actually using Magnuson-Moss to issue rules when appropriate. The relevant section of the FTC Operating Manual merits inclusion here:

> WHEN IS PROMULGATION OF AN INDUSTRY-WIDE RULE APPROPRIATE?
>
> When staff becomes aware of allegedly unfair or deceptive acts or practices that appear widespread, it should consider whether rulemaking, as contrasted with adjudication, is appropriate. Some of the relevant factors to be considered include:

---

[21] Hayek argued that in certain cases the developed common law "may prove too slow to bring about the desirable rapid adaptation of the law to wholly new circumstances," and may lead into intellectual dead ends that are "seen to have undesirable consequences or to be downright wrong"—and in such cases it may be improved upon by legislation. *See* 1 FRIEDRICH A. HAYEK, LAW, LEGISLATION AND LIBERTY 88 (1973).

[22] See generally, *FTC Operating Manual*, Chapter 7, http://www.ftc.gov/foia/ch07rulemaking.pdf

[23] Beth DeSimone, *FTC Chairman Calls for Expanded Consumer Protection Powers over the Financial Services Industry*, Consumer Advertising Law Blog, February 10, 2010, http://www.consumeradvertisinglawblog.com/2010/02/ftc-chairman-calls-for-expanded-consumerprotection-powers-over-the-financial-services-industry.html.

> (1) Prevalence of the acts or practices under investigation. When a practice exists on a widespread basis, rulemaking has advantages over case-by-case adjudication... The precise degree of prevalence appropriate for undertaking a [rulemaking] will vary according to such factors as seriousness of consumer injury, vulnerability of the affected consumer group, amount of money involved in the given transaction, and severity of the contemplated rule's impact both on the affected industry, in general and especially on those industry members who did not engage in the underlying unfair or deceptive practices.
>
> (2) Cost of industry-wide investigation and rulemaking proceedings.
>
> (3) Feasibility of enforcement of the [industry-wide rule] by the Commission

Perhaps most important for the FTC to consider is the degree of "prevalence" required relative to the other factors provided.

Some in industry will doubtless object to any use of Magnuson-Moss, for fear that the FTC will repeat the overreach of the 1970s (when the agency ran wild with its unfairness jurisdiction).[24] Some consumer advocates may object that these procedures work too slowly, and, like some inside the Commission itself, worry that a revival of Magnuson-Moss could undermine efforts to pass new legislation, either comprehensive consumer privacy legislation or expansions of the FTC's powers. But neither should fear the FTC's use of Magnuson-Moss: So long as its essential procedural safeguards are kept in place, it is a difficult statute for the FTC to abuse. On the other hand, privacy advocates might have been able to achieve some of their legitimate demands for greater consumer protection already if they had started that process several years ago, instead of simply pushing for legislation in every new Congress.

If, for example, it can be shown that industry self-regulation permits practices that should be prohibited under the Unfairness Doctrine, the Commission should begin a Magnuson-Moss proceeding to ban them. Even the threat of doing so would likely be enough to cause self-regulatory bodies to update their codes of conduct. Thus, as always, self-regulation could work more expeditiously than government regulation—but the threat of regulation could spur self-regulation on.

Agency Threats

If the Commission could actually stake out a strong case, this would be a legitimate use of an "agency threat" because the pressure brought to bear would be (a) the use of process

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

established by law (Magnuson-Moss rulemaking) (b) justified under well-established legal doctrine. If the Commission's case was not strong enough to survive a legal challenge, the threat would probably not be credible enough to force changes to self-regulation.

But this is a far narrower conception of agency threats than that recently offered by law professor Tim Wu, who famously coined the term "net neutrality" and more recently served as a special advisor at the FTC.[25] As a descriptive matter, Wu is quite right that agencies do use such threats; but whether they should is a question that would make a fine subject for a hearing.

This Commission has made ample use of its soft power to influence Internet governance. In particular, the Commission has played a significant role in shaping the proceedings of the Worldwide Web Consortium's Tracking Protection Group. In September, nine Members of Congress sent a letter to FTC Chairman Jon Leibowitz asking seven questions about the FTC's role in the TPWG.[26] Leibowitz quickly responded with a letter answering several of the questions and promising to follow up with answers to the most difficult questions—about the FTC's communications and meetings with industry players or the W3C about DNT outside of W3C meetings.[27] The FTC has not yet followed up, nearly a month later, leaving unresolved the critical question of what role the FTC played in Microsoft's surprising decision to violate the consensus underpinning the W3C Do Not Track Process by turning on DNT:1 by default in its Internet Explorer 10 browser. In short, Congress has attempted to exert oversight over the agency's extra-legal activities, but apparently without success. This is a disturbing precedent because the FTC seems to be helping certain incumbents gain competitive advantage through a self-regulatory process.

Smart Disclosure

The clearer privacy promises are, the more easily the FTC will be able to enforce them. One important way to achieve this goal would be for the FTC to promote the use of "smart disclosure"—the term used by Cass Sunstein, director of the Office of Information and Regulatory Affairs, a close advisor to President Obama, and a widely respected thinker in law,

---

[25] *See* Tim Wu, *Agency Threats*, 60 Duke L. Rev. 1841 (2011), *available at* http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1506&context=dlj

[26] Letter of Rep. Tom Graves, Rep. Mick Mulvaney, Rep. Reid Ribble, Rep. Marsha Blackburn, Rep. Tim Walberg, Rep. Tim Huelskamp, Rep. Jeff Duncan, Rep. Dennis Ross, Rep. Dan Burton to Jon Leibowitz, Sept. 21, 2012, available at http://www.adotas.com/2012/09/members-of-congress-question-whether-ftc-is-attempting-a-dnt-end-around/

[27] Letter of Jon Leibowitz to Rep. Marsha Blackburn, Sept. 27, 2012, copy on file with author.

policy and technology. Smart disclosure can empower consumers by letting software do the work of reading privacy policies for them—and then implement their privacy preferences. Sunstein offers the following definition:

> the timely release of complex information and data in standardized, machine readable formats in ways that enable consumers to make informed decisions. Smart disclosure will typically take the form of providing individual consumers of goods and services with direct access to relevant information and data sets. Such information might involve, for example, the range of costs associated with various products and services, including costs that might not otherwise be transparent. ... In many cases, smart disclosure enables third parties to analyze, repackage, and reuse information to build tools that help individual consumers to make more informed choices in the marketplace.[28]

While the creation of smart disclosure would probably be best done by self-regulation in light of the complexity of drafting disclosure formats, one area the FTC could be useful is in defining the structured data format for general disclosures or by mandating disclosure of privacy practices.

For example, users could subscribe to the privacy recommendations of, say, Consumer Reports, or any privacy advocacy group, which in turn could set their phone to warn them if they install an app that does not meet the privacy practices those trusted third parties deem adequate. Or, more simply, such a system could work for communicating whether a site, service or app accedes to a particular self-regulatory code of conduct—and phone privacy controls could be set by default to provide special notices when users attempt to install apps that do not certify compliance with self-regulatory codes of conduct. As the FTC Privacy Report notes, smart disclosure could also "give consumers the ability to compare privacy practices among different companies."[29] An app store might illustrate how such comparisons could work, allowing users trying to choose between several competing apps to compare their privacy practices side by side.

While it would be preferable for smart disclosure to arise through self-regulation, especially given the complexity of crafting disclosure formats, mandating disclosure of privacy practices

---

[28] Cass R. Sunstein, Memorandum for the Heads of Executive Departments and Agencies 2 (Sept. 8, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/inforeg/for-agencies/informing-consumers-through-smart-disclosure.pdf.

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

would generally be a better way for government to address demonstrated market failures than by dictating what constitutes fair information practices. Thus, this might be an appropriate area for Congress to explore legislation if industry should fail to produce, and adopt, appropriate smart disclosure formats on their own.

2. You testified that the privacy debate has been biased by overstating the risks of harm and understating the benefits. How would you go about evaluating those factors? Is it possible to evaluate the benefits of future technologies?

This is, indeed, the key question on which tech policy analysts should focus. Among the benefits of data which have not been adequately considered in this debate are the following:

1. Enhanced advertising revenues for publishers of content and services that might otherwise have difficulty funding their offerings by charging for data, especially in markets where marginal costs are lower or zero (and basic economic theory would suggest that competition will inevitably drive prices towards zero).
2. More effective advertising, which in turn means:
    a. More relevant, and potentially less annoying/interruptive advertising for consumers;
    b. Better correlation between the production of content and services, and consumer preferences;
    c. Lower prices for consumers and greater innovation throughout the economy;
    d. More effective non-commercial messaging, including political speech accorded the highest protection by the First Amendment; and
    e. More vibrant media and improved political discourse and communities
3. Serendipitous innovation based on the discovery of unexpected uses of data.

But it is impossible to categorize all the benefits of technology, because they are largely unseen. The danger is that policymakers will focus on the seen risks of harm while understating unseen benefits, including future innovation. Frédéric Bastiat (1801-1850), the great French popularizer of economics, put it best when he wrote, in 1848:

> In the economic sphere an act, a habit, an institution, a law produces not only one effect, but a series of effects. Of these effects, the first alone is immediate; it appears simultaneously with its cause; it is seen. The other effects emerge only subsequently; they are not seen; we are fortunate if we foresee them. There is only one difference between a bad economist and a good one: the bad economist confines himself to the visible effect; the good economist takes into

> account both the effect that can be seen and those effects that must be foreseen.[30]

Developing the capacity to understand and effectively regulate technology is as much about ensuring that regulators understand how innovative technology confers benefits on consumers as it is about ensuring that regulators understand how new technology *doesn't* impose imaginary costs. As technological advance brings about ever more effective means of collecting and analyzing information, there is a tendency to view this through the lens of harm—to see such advances as ever more intrusive and potentially harmful. Forty years ago, the great economist Ronald Coase warned us:

> If an economist finds something—a business practice of one sort or another—that he does not understand, he looks for a monopoly explanation. And as in this field we are very ignorant, the number of understandable practices tends to be very large, and the reliance on a monopoly explanation, frequent.[31]

The same risk arises here—that, finding a technology that they don't understand, regulators will look for a nefarious (or "unfair") explanation, overestimating harms to users (the more easily seen) and understating benefits (the more likely unseen). Ensuring that regulators have the capacity to keep up with technological change is thus essential to facilitating both effective and appropriately restrained enforcement. This is what separates good policymakers from bad policymakers.

Of course it is impossible to fully anticipate the benefits of new technologies—because it is impossible to conceive of what new technologies might be developed, and how they might change the basic paradigms shaping the role of technology in our lives. The most important thing is for policymakers to adopt a posture of humility about technology. TechFreedom recently joined a number of other civil society groups from around the world in a Declaration of Internet Freedom, which began with the following two core principles:

> **Humility**. First, do no harm. No one can anticipate what the future holds and what tradeoffs will accompany it. Don't meddle in what you don't understand — and what you can all too easily break, without even seeing what's been lost. Often, government's

---

[30] Frederic Bastiat, *What is Seen and What is Nat Seen* (1848), http://www.econlib.org/library/Bastiat/basEss1.html

[31] Ronald Coase, *Industrial Organization: A Proposol for Research*, *in* 3 POLICY ISSUES AND RESEARCH OPPORTUNITIES IN INDUSTRIAL ORGANIZATION 59, 67 (Victor Fuchs ed. 1972).

> best response is to do nothing. Competition, disruptive technological change, and criticism from civil society tend to resolve problems better, and faster, than government can.
>
> **Rule of Law.** When you must intervene, start small. Regulation and legislation are broad, inflexible, and prone to capture by incumbent firms and entrenched interests. The best kind of "law" evolves one case at a time, based on simple, economic principles of consumer welfare — alongside the codes of conduct and practices developed by companies under pressure from competitors and criticism. Worst of all, when regulators act without legal authority, or regulate by intimidation, they undermine the rule of law, no matter how noble their intentions.

Commissioner Ohlhausen expressed admirable humility in her first testimony after being confirmed to the Commission:

> Clearly, the technology sector is developing at lightning speed and we now face issues unheard of even a few years ago. I wish to proceed cautiously in exploring the need for any additional general privacy legislation, however. I have concerns about the ability of legislative or regulatory efforts to keep up with the innovations and advances of the Internet without also imposing unintended chilling effects on many of the enormous benefits consumers have gained from these advances or without unduly curtailing the development and success of the Internet economy.[32]

The best way for regulators to protect consumers in a constantly evolving world, without chilling technological change, is to follow the common law method of case-by-case adjudication based on the very doctrines the FTC already has in place: deception and unfairness. But this is why, as explained above, it is so critical that the FTC do more to explain its conception of "substantial injury" as well as "countervailing benefit"—and how to balance the two. This is no easy task and it is not something that can be written down once and for all. But over time and with the proper scrutiny (ideally from the courts), the FTC could develop a framework to do just this.

---

[32] *The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 112th Cong. (2012) (statement of Maureen K. Ohlhausen, Commissioner, Federal Trade Commission), at 4, *available at* http://commerce.senate.gov/public/?a=Files.Serve&File_id=0b54f847-1e2f-4bee-8d3f-21581465c1f1.

3. There are some types of harm we protect against before it happens. For instance, we lock our car doors but what are the odds of a carjacking? We lock the doors to our homes at night, but how many of us have had our homes invaded? Why should the Federal government not establish baseline rules to guard against the harm of someone accessing damaging or potentially embarrassing information about private citizens as gleaned from search history, online shopping habits, or e-book purchase or video viewing history?

Congress has already addressed certain categories of harm through targeted legislation, such as the Fair Credit Reporting Act and the Video Privacy Protection Act. Even if the basic rationale behind both laws was sound, neither has aged particularly well.[33]

The VPPA, in particular, offers an object lesson in the dangers of legislating specific prescriptions in advance of a technology's development rather than allowing regulators to intervene on a case-by-case basis according to basic principles like unfairness and deception. Passed as a prophylactic response to an incident involving the failed Supreme Court nominee Robert Bork,[34] the VPPA has prevented Netflix from empowering U.S. users to share with their friends what movies they're watching, just as users of Spotify and other services can do with music and other content they're enjoying. Yes, this particular problem appears likely to be remedied soon, with the passage of Sen. Leahy's Video Privacy Protection Amendments Act.[35] But how many other problems go unnoticed, or unaddressed because companies less influential than Netflix cannot make an issue like this even rise above the noise level in Washington? How many startups are never founded because outdated legal requirements like this prevent them from receiving funding? These are all unseen costs of laws that attempt to prevent against speculative future harms.

Congress has already "establish[ed] baseline rules to guard against" real harms—that is the essence of Section 5. But to date, the FTC has done a poor job of conceptualizing harm, as discussed above. The Commission could do much more to explain what it means by harm, and thus protect against harms before they happen without falling into the trap of trying to specifically prescribe speculative harms.

---

[33] *See* Jim Harper, *Reputation Under Regulation: The Fair Credit Reporting Act at 40 and Lessons for the Internet Privacy Debate*, Cato Policy Analysis No. 690 (Dec. 8, 2011), *available at* http://www.cato.org/pubs/pas/PA690.pdf.

[34] *Video Privacy Protection Act: Intraduction*, Electronic Privacy Information Center, http://epic.org/privacy/vppa/ (the VPPA "was passed in reaction to the disclosure of Supreme Court nominee Robert Bork's video rental records in a newspaper.").

[35] S. 3414, 112th Cong. (2012), *available at* https://www.cdt.org/files/pdfs/Leahy-ECPA-Amendment-S3414.pdf.

But again, legislation should be a last resort after it can be shown that a quasi-common law of privacy is insufficient to deal with the problem. First, the FTC should focus on defining harm clearly in order to establish baseline rules to protect privacy. The FTC should help to clarify this uncertainty by convening a public workshop on its unfairness authority, with a special emphasis on defining the boundaries of cognizable harm. Ideally, such a workshop would produce guidelines building on the 1980 Unfairness Policy Statement adequate to help companies predict how to build new and innovative services without running afoul of the unfairness authority. In essence, the workshop should address the questions raised by Commissioner Ohlhausen in her first testimony after being appointed to the Commission:

> "What harms are occurring now that Section 5 cannot reach and how should harm be measured? As my colleague Commissioner Rosch noted in his dissent to the Privacy Report, the Commission has specifically advised Congress that absent deception, it will not enforce Section 5 against alleged intangible harm, (FTC letter to Ford and Danforth, 1984), and the FTC's own unfairness statement suggests that the focus should be on monetary as well as health and safety harms, rather than on more subjective types of harm. Although the Commission's Privacy Report did not reject the fundamental insights of the harm-based approach, it appears to embrace an expansion of the definition of harm to include 'reputational harm,' or 'the fear of being monitored,' or 'other intangible privacy interests' (*see* Report at iii, 20, 31), and, as an initial matter, I have reservations about such an expansion."[36]

The basic analytical framework of the Unfairness Doctrine itself should guide Congress in determining how to supplement the Unfairness Doctrine with legislation targeted at harms that cannot properly be addressed through the Unfairness Doctrine directly—i.e., without stretching the definition of "substantial injury." In other words, just because a harm does not neatly fit within the unfairness doctrine (say, employer access to employees' social media passwords), does not mean it may not be a valid target for legislation; but even in such cases, lawmakers should still weigh that harm against countervailing benefits and intervene only where consumers themselves cannot reasonably avoid the harm, such as through increased transparency and more effective privacy controls.

4. The FTC applauds industry efforts to develop a Do-Not-Track mechanism, however, the Chairman recognized that the industry-developed mechanism is merely an opt-out of

[36] Ohlhausen, *supra* note 30, at 3.

behavioral targeted ads and suggests that such mechanisms should enable consumers to opt out of information collection as well. Most consumers who are bothered by behavioral targeted ads are not troubled by the ad itself but rather by how the ad network knew that particular ad would interest the consumer. If we accept that as true, how is the industry-developed Do-Not-Track mechanism responsive to consumers' privacy concerns when it only stops the delivery of ads but not the collection of the underlying interest information?

It is true that "Do Not Track" is something of a misnomer: the technical specification under development by the Worldwide Web Consortium (W3C) is actually a use-specification mechanism. A true "Do Not Track" mechanism would essentially be an ad-blocker, since blocking *all* tracking makes even the simplest forms of online advertising impossible, because even "contextual" advertising requires tracking of views. Thus, a tool that blocked tracking elements but not the display of ads themselves would still break online advertising. In fact, such mechanisms are already readily available to consumers, most notably the browser plug-in AdBlock Plus, which has nearly fifteen million users on Firefox,[37] and over five and a half million users on Chrome.[38] These users are essentially free-riding on users who don't block ads. Adblocking is, simply put, a form of piracy. As Ken Fisher, the founder & Editor-in-Chief of Ars Technica, eloquently put it:

> Imagine running a restaurant where 40% of the people who came and ate didn't pay. In a way, that's what ad blocking is doing to us. Just like a restaurant, we have to pay to staff, we have to pay for resources, and we have to pay when people consume those resources. The difference, of course, is that our visitors don't pay us directly but indirectly by viewing advertising.[39]

There is simply no reason government should promote the use of such adblocking tools. Fortunately, such mechanisms are still used by only a relatively small percentage of the overall population—below the acceptable loss threshold for most publishers (the point at which it becomes cost-effective for publisher to try to make explicit today's implicit quid-pro-quo). It is far from clear what will happen above that threshold, whether an architecture of explicit negotiation between sites and users (such as contemplated by the "user-granted exception" features of the Do Not Track spec currently being drafted) will produce the same quantity and

---

[37] Ad Block Plus Add-on for Mozilla Firefox, https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/.

[38] Adblock Plus (Beta), https://chrome.google.com/webstore/detail/adblock-plus-beta/cfhdojbkjhnklbpkdaibdccddilifddb.

[39] Ken Fisher, *Why Ad Blocking is devastating to the sites you love*, arstechnica (Mar. 6, 2010), http://arstechnica.com/business/2010/03/why-ad-blocking-is-devastating-to-the-sites-you-love/.

distribution of revenue. In other words, far from simply facilitating users' preferences, such a system may produce outcomes that users would not have chosen on their own—primarily because the increased transactions costs involved may swamp the relatively small value created by each interaction between site and user. Thus, forcing such a change may fundamentally change the nature of the Internet ecosystem.[40]

The essential disconnect here between "consumers' privacy concerns" and technical reality is that the information collected is the same in both cases; it is simply a question of the use to which it is put. The question, then, is what sorts of uses (including data retention and sharing) consumers are opting out of when they send a DNT:1 header saying "Don't track me."

What the Digital Advertising Alliance committed to do in February was to honor signals sent by a DNT:1 header as an opt-out from the use of information about a user's browsing behavior to display behavioral advertising.[41] The W3C's Tracking Protection Working Group (in which I participate as an invited expert) is currently working on developing a technical specification as to exactly what DNT:1 will mean. While the TPWG has to define the term "tracking," it is clear that it will be essentially consistent with the DAA's definition: "Online Behavioral Advertising does not include the activities of First Parties, Ad Delivery or Ad Reporting, or contextual advertising (i.e. advertising based on the content of the Web page being visited, a consumer's current visit to a Web page, or a search query)."[42]

It is worth noting that the DAA has two self-regulatory codes of conduct: the other, Self-Regulatory Principles for Multi-Site Data, issued in November 2011, protects all consumers, whether or not they exercise an opt-out, by specifically restricting the use of data collected across websites for eligibility for employment, credit, health care, or insurance, and requires consent for children's information (consistent with COPPA) as well as health and financial data.

---

[40] *See* Appendix below; Berin Szoka, *The Paradox of Privacy Empawerment: The Unintended Consequences of "Do-Not-Track"* (Position paper for W3C Workshop: Do Not Track and Beyond, Berkeley, California, November 26-27, 2012).

[41] Press Release, Digital Advertising Alliance, White House, DOC and FTC Commend DAA's Self-Regulatory to Protect Consumer Online Privacy: DAA Announces Plans to Expand Program Consumer Choice Mechanisms (Feb. 23, 2012), *available at* http://www.aboutads.info/resource/download/DAA%20White%20House%20Event.pdf.

[42] Interactive Advertising Bureau, et. al, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 11 (July 2009), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf.

The Honorable Cliff Stearns

1. Mr. Szoka, you testified that companies should be encouraged to educate consumers through more accessible forms of notice that explain privacy policies and practices. How can we as Congress encourage companies to do this?

As explained above, smart disclosure could bypass much of the current debate about the failure of effective notice to empower consumers by making "notice" technologically actionable: Users could subscribe to the privacy recommendations of, say, Consumer Reports, or any privacy advocacy group, [43] which in turn could set their phone to warn them if they install an app that does not meet the privacy practices those trusted third parties deem adequate. Or, more simply, such a system could work for communicating whether a site, service or app accedes to a particular self-regulatory code of conduct—and phone privacy controls could be set by default to provide special notices when users attempt to install apps that do not certify compliance with self-regulatory codes of conduct.

Congress should commission the FTC to issue a report on the feasibility of using structured data formats to facilitate actionable privacy disclosures. Such a report should be subject to public input through a workshop, and to review in draft form prior to being finalized. Ideally, the report would be developed by an Chief Technology Officer such as proposed above, with a technical expert in smart disclosure hired to lead work on this report. The report should assess lessons learned from the experience with P3P and the ongoing W3C Tracking Protection Working Group.

Of course, if Congress really wants to help to educate consumers, it can also support campaigns aimed at building consumer awareness. The FTC has conducted such campaigns in the past, such as its "Net Cetera: Chatting with Kids about Being Online" toolkit.[44] Congress could either appropriate money for further such campaigns or, more preferably, support a competitive grant-making program for civil society groups to run their own educational campaigns.

2. At the hearing we heard that allowing all consumers to access whatever data companies have about them presents significant technical challenges and could actually increase risk to consumers. But what about a narrower bill that would allow consumers to

---

[43] *See, e.g.*, Terms of Service - Didn't Read, http://www.indiegogo.com/terms-of-service-didnt-read (offering evaluations of online terms of service from a privacy perspective).

[44] Net Cetera Toolkit, OnGuardOnline, http://www.onguardonline.gov/features/feature-0004-featured-net-cetera-toolkit.

ask companies for categories of information that companies have on them. Wouldn't this alleviate the risk of harm to the consumer and burden on the company while at the same time help educate consumers on data collection?

The flipside of user access is privacy breach—and all that separates the two is effective authentication that the person attempting to access a record is the right person. Congress (and the FTC) should avoid creating new privacy problems in the name of privacy by mandating access or correction rights (two of the Fair Information Practice Principles) in situations where the user is not already authenticated, because doing so would, ironically, require *more* collection of personal information, and create new privacy problems.

Reducing the granularity of information subject to an access right certainly does reduce the potential privacy problem but it does not eliminate it. For example, Microsoft's Personal Data Dashboard (https://choice.live.com/data/) and Google's Ad Preferences Manager (www.google.com/ads/preferences/) both show users the interests associated with their profile (e.g., pets, travel, technology), but still require users to log-in to see even this relatively innocuous information.

As noted by the question, allowing consumers access to whatever data companies have on them could actually increase risk to consumers. If companies had to keep such individualized files tied to authenticated accounts, this could create a honeypot for potential identity thieves. Requiring a log-in, as Microsoft and Google do, would reduce the problem, but if identity thieves could gain access, they would have considerably more information available to them in one convenient location. Such honeypots could also attract the interests of law enforcement, which would probably be able to access them without a warrant because courts have ruled (wrongly) that the Fourth Amendment does not apply to "third party records,"[45] and the Electronic Communications Privacy Act has failed to keep pace as a substitute for Fourth Amendment protection.

So before crafting any kind of disclosure mandate, Congress would have to decide:

1. What kind of information merits a disclosure mandate. Any legislation should be very specific about the justification for mandating disclosure.
2. Whether the costs of disclosure outweigh the benefits.

---

[45] Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 Am. U. L. Rev. 1381 (2008), *available at* http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1045&context=aulr.

There certainly are circumstances when access—and even correction—rights are warranted, such as for credit records. A compelling case can be made for mandating such access by law, where the potential harms of inaccurate information are clear—e.g., eligibility for credit, the basis for the Fair Credit Reporting Act's access and correction mandate. But even then, Congress should be careful not to mandate these rights in such a way that would lead to ossification. As noted by Jim Harper, in his discussion of FCRA:

> Though the information and technology environments have changed dramatically over the last four decades, the credit reporting and reputation marketplace has seen little change or innovation. A potential related market for identity services is also stagnant thanks in part to government policies.[46]

It is difficult to equate the situation of online advertising with credit records, though—especially when the online advertising industry has barred data collected for advertising purposes from being used for employment, credit, health care treatment, or insurance eligibility decisions.[47] Inaccurate advertising and marketing data would at worst result in less relevant advertising. As a result, the costs associated with building the necessary infrastructure to permit access and correction rights for advertising and marketing data might significantly outweigh the benefits.

The legislation posited by the question seems to refer to the FTC Report's proposal regarding "data brokers":

> the data broker industry explore the idea of creating a centralized website where data brokers that compile and sell data for marketing could identify themselves to consumers and describe how they collect consumer data and disclose the types of companies to which they sell the information. Additionally, data brokers could use the website to explain the access rights and other choices they offer consumers, and could offer links to their own sites where consumers could exercise such options. This website will improve transparency and give consumers control over the data practices of companies that maintain and share data about them for marketing purposes.[48]

---

[46] Harper, *supra* note 31, at 1.

[47] Digital Advertising Alliance, SELF-REGULATORY PRINCIPLES FOR MULTI-SITE DATA (Nov. 2011), http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

[48] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* ("FTC Report"), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf, at 69.

This concept merits exploration as a way of remedying the lack of transparency regarding companies that currently lack a direct way of offering transparency to those whose data they collect—provided the term "data broker" is defined appropriately. This could be an excellent test case for encouraging smart disclosure through self-regulation—but only if it can be implemented in a way that actually improves transparency for consumers and proves feasible for companies.

The term "data broker" was defined quite expansively in the FTC Privacy Report. As Linda Wooley, the executive VP of the Digital Marketing Association's Washington operations, rightly asked, "Data is changing the world, but I'm not sure the FTC can define what a 'data broker' is. Is a data broker Acxiom, Google or Macy's? All companies are sharing data in 2012. First parties are now doing collecting and having third parties crunch the data for them. Where do you draw the line?"[49] Drawing the line in the wrong place could lead to fundamental changes in the market for information—to the detriment of consumers.

It would be a mistake to focus on having a single website as an interface for transparency to consumers. Such a site could be built and advertised as a one-stop shop for consumers to learn more about what kinds of information data brokers collect. But it should be only one of many potential interfaces that can display, in a user-friendly way, information provided by data brokers in structured formats. In technical terms, such a site would merely be an aggregator of feeds of raw data provided by each data broker about their practices. For example, if data brokers provided descriptions of their data collection practices in standardized form at a standardized url, e.g., databroker.com/DCP.xml (for "data collection practices"—a parallel to the convention of website.com/RSS.xml), *any* privacy site or tool could pull those feeds automatically and present the information to users in helpful ways. This would be smart disclosure at its best.

3. Are you familiar with my bill, H.R. 1528, the Consumer Privacy Protection Act of 2011? This bill calls for clear, easy to understand privacy policy statements and provides for the FTC to approve a five-year self-regulatory program. Would you support this bill advancing through the Subcommittee?

---

[49] Christopher Hosford, *'Data Brokers' new target of FTC privacy recommendations*, BtoB (Apr. 2, 2012), http://www.btobonline.com/apps/pbcs.dll/article?AID=/20120402/DIRECT0101/303299993/data-brokers-new-target-of-ftc-privacy-recommendations&template=printart.

This bill does perhaps a better job than any of the other privacy bills introduced in this Congress at balancing the competing values at play. In particular, the bill wisely deems an IP address to be Personally Identifiable Information (PII) only when combined with one of the other true identifiers listed in the bill, such as name or email address. That said, I do have several concerns about the bill's likely effects—on both sides of the balancing act.

First, the bill it would convert the U.S. self-regulatory approach into something quite different: the European model of co-regulation. If the FTC must ultimately approve a self-regulatory standard, it will likely play the dominant role in drafting the standard. This will replace the "competitive discipline" of market and reputational pressures with agency threats as the driving factors behind setting codes of conduct. Like all such regulation, the bill risks creating regulatory ceilings above which companies have no incentive to compete with stronger privacy protections.

Indeed, the Digital Advertising Alliance has already implemented many of the practices the bill would require. So why is such intrusion warranted? Is the DAA not *less* likely to continue improving its self-regulatory system once it has been officially sanctioned by the FTC? Whatever the intentions of such an approval requirement, the lesson of regulated industries is clear: the more power an agency has to set approved standards of conducting business, the more prone it is to capture by entrenched interests to insulate themselves from further obligations as well as competition.

Second, the bill appears to take away the ability of consumers to enforce contractual privacy rights directly. Section 10 prescribes the terms of a dispute resolution process for entities in a self-regulatory program and Sections 11 and 12 exclude private rights of action with respect to alleged violations and preempt state laws. This puts a few members of the FTC bureaucracy in charge of privacy protection rather than the interactions of millions in the marketplace, subject to the evolving common law. As Jim Harper argued about FCRA:

> When the Fair Credit Reporting Act preempted state common law remedies against credit bureaus, it foreclosed an option that may have resulted in better protection for consumers and better results for the economy and society. Because Congress imposed a national credit reporting rule, we cannot know how this industry might have developed had it been left free to experiment, subject to simple rules against harming consumers.[50]

[50] Harper, *supra* note 31, at 2.

Third, one aspect of the bill may require clarification: Section 10 provides that "A violation of any provision of this Act by a covered entity is an unfair or deceptive act or practice unlawful under section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)), except that the amount of any civil penalty under such Act shall be doubled for a violation of this Act." Of course, Section 5(a)(1) does not provide for any monetary penalties (for acts or practices the FTC finds unfair or deceptive); only when a company has been placed under a consent order for such practices and violated that order may, under 5(a)(l), the Commission impose a monetary penalty (not more than $10,000 for each violation). Is H.R. 1528 intended to impose monetary penalties for (willful) violations of self-regulatory programs (i.e., double the penalty imposed by Section 5(a)(l) for violations of consent decrees)? If so, the language, or simply the cross reference to the FTC Act, should be clarified.

This is important because the threat of monetary penalties intersects with with the presumption of compliance created under the bill: the greater the risk of monetary penalties, the more a presumption of compliance makes sense; but too great a presumption of compliance is itself a problem, which may suggest reducing the presumption, and accordingly reducing the threat of monetary penalties.

Covered entities in self-regulation programs enjoy a strong presumption of compliance under the proposed bill (§ 9(a)(1)). This presumption may only be overcome by "clear and convincing evidence" of wilful non-compliance (§ 9(d)(4)). I agree that some presumption makes sense and have criticized the FTC for holding Google strictly liable (the opposite of a presumption of compliance) for statements it made about its privacy practices that became untrue only after Apple changed how Safari handled cookies.[51] But should a presumption really protect companies for, say, grossly reckless non-compliance with an industry standard? Might it not make sense for the presumption to give way, in part, if a self-regulatory body recommends that the FTC pursue an enforcement action—even if a company was not wilfully non-compliant? This shifting of traditional evidentiary standards will make it more difficult for the FTC and consumers to win close cases. Creating such a strong presumption may unduly create the impression that the bill exists merely to insulate industry from liability. This is another reason the contract law approach, supplemented with a quasi-common law of privacy from the FTC, would likely be more effective in promoting consumer welfare.

Fourth, the bill risks being tied up in litigation over its application to non-profit entities. Congress has heretofore largely avoided First Amendment challenges to its regulation of the

[51] Berin Szoka & Geoffre Manne, *FTC's Google Settlement a Pyrrhic Victory for Privacy and the Rule of Law*, TechFreedom (Aug. 9, 2012), http://techfreedom.org/node/195.

Internet by exempting non-profit entities from legislation. What is the rationale for including them here? This is especially problematic, given the Supreme Court's recent decision in *Sorrell*, ruling that privacy prior consent requirements for the use of interest data for prescription drug marketing violated the First Amendment. [52]

[52] Sorrell v. IMS Health, Inc., No. 10-779 (2011), http://www.supremecourt.gov/opinions/10pdf/10-779.pdf

TECH FREEDOM

The Paradox of Privacy Empowerment: The Unintended Consequences of "Do Not Track"

Position paper for W3C Workshop: Do Not Track and Beyond
Berkeley, California, November 26-27, 2012

Berin Szoka[53]

The debate over "Do Not Track" offers an excellent microcosm for understanding the larger privacy policy discourse. Arguments for giving users a tool to express their privacy preferences exert enormous rhetorical appeal. Those arguing for versions of DNT that are more restrictive of the collection and use of information about user behavior essentially insist that "We're merely giving users a choice!" Who could possibly be against letting users choose for themselves? Why should anyone else get to choose *for us*—especially companies that seem to be profiting from the ignorance or helplessness of users?

Tools like "Do Not Track" (and "privacy-friendly" interfaces more generally) are usually justified as simply offering users a means of expressing their true preferences. But such choice architectures[54] are anything but neutral: even with the best of intentions and in the name of facilitating user choice, choice architects will produce outcomes that users would not have chosen if they could make fully rational decisions in a frictionless world without transactions costs. This is the essential paradox of user empowerment.

"Privacy advocates" regularly cite opinion polls showing that users demand greater privacy protection—and thus conclude that privacy-friendly choice architectures simply facilitate the true preferences of users. But listening to what consumers *say* they want tells us much less about their preferences than seeing what preferences they *reveal* in the process of making real-world decisions about trade-offs among values. As much as users value privacy, they do not value privacy in isolation or inherently, but relative to other values—including other forms of privacy.

---

[53] This position paper draws testimony I gave to the Senate Commerce Committee in June 2012, http://techfreedom.org/node/185

[54] On term "choice architecture" and its inherent non-neutrality, *see generally* Richard H. Thaler University of Chicago, Cass R. Sunstein & John P. Balz, Choice Architecture, April 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1583509.

To avoid the paradox of user empowerment to the greatest extent possible, choice architects must understand how their proposed choice architecture will shape real-world outcomes, and the impact that will have on these many competing values. Let us consider the unintended consequences of three contested aspects of DNT:

1. **Default setting** - How, and by whom, may a browser be set to send DNT:1?
2. **Definition of tracking** - What is it DNT:1 tells servers not to do?
3. **Architecture of negotiation** - How do sites get users who send DNT:1 headers to opt-in to tracking—and to remain opted-in?

Each is a complicated issue. But all three may be understood, to a degree, in terms of the traditional opt-in and opt-out paradigms. DNT:1 is nothing more than a signal sent by the user's browser expressing a preference not to be "tracked," however defined—after which website publishers, advertisers and other data collectors must somehow negotiate with the user to get him or her to "opt back in" (a term actually used in the TPE[55]) to "tracking" (by granting a site or network a "user-granted exception"). If browsers and other user agents may turn on DNT:1 by default, then the adoption rate of DNT will quickly exceed publishers' "maximum acceptable loss threshold." Below that point it makes little practical sense for publishers and advertisers to bother building an architecture of negotiation, because it is more cost-effective to let DNT:1 users free-ride off those allow tracking (either by setting DNT:0 or by not having it set at all).

Put more simply, if browsers are allowed to turn DNT:1 on by default, most users will live in a world where "tracking" is opt-in. This will be a choice made *for*, not *by*, users. But either way, all of the problems of more general "Opt-In Dystopias" described by Nicklas Lundblad and Betsy Masiello would apply once DNT:1 is turned on. They distill their concerns into four categories:

> **Dual cost structure**: Opt-in is necessarily a partially informed decision because users lack experience with the service and value it provides until after opting-in. Potential costs of the opt-in decision loom larger than potential benefits, whereas potential benefits of the opt-out decision loom larger than potential costs.
>
> **Excessive scope**: Under an opt-in regime, the provider has an incentive to exaggerate the scope of what he asks for, while under the opt-out regime the provider has an incentive to allow for feature-by-feature opt-out.

[55] http://www.w3.org/TR/tracking-dnt/#exceptions-principles

> **Desensitisation**: If everyone requires opt-in to use services, users will be desensitised to the choice, resulting in automatic opt-in.
>
> **Balkanisation**: The increase in switching costs presented by opt-in decisions is likely to lead to proliferation of walled gardens.[56]

The problem is that DNT, like any choice architecture, affects not only "demand" (empowering users to choose) but also the "supply" (the choices available to users). The difficulty of obtaining opt-ins (user-granted exceptions) will serve as a barrier to entry, protecting larger, established incumbents against competition from new entrants. This will be true on some level for individual sites: absent dual-cost structure problem, one might think that any site a user visits will easily be able to get an opt-in. But obtaining such opt-ins is costly, both for user and for sites, which must implement a mechanism for obtaining user-granted exceptions. Some sites will simply decide not to risk alienating users, and forego potential additional revenue, while other better established sites or sites less subject to competition, will gain a competitive advantage.

But the greater problem lies with web-wide exceptions, opt-ins to data collection by an ad network or other data collector across the web. To be sure, these are essential to making DNT work without breaking business models that depend on third-party ad networks, but they will also necessarily favor certain established players in the data and advertising ecosystem over other, generally smaller players. One might dismiss these competitive effects as the necessary consequence of restructuring an industry that is loathed by many (despite the benefits it confers),[57] but this consolidation would likely be accompanied by a qualitative change in the *kind* of information collected. Once a network obtains a web-wide exception, why *not* collect more data across the web? Why not associate it in a richer profile? As Masiello and Lundblad explain:

> service providers may attempt to maximise data collection in every instance that they are forced to use an opt-in framework; once a user consents to data collection, why not collect as much as possible? And the increased transaction costs associated with opt-in will lead service providers to minimise the number of times they request opt-in consent.

---

[56] N Lundblad and B Masiello, "Opt-in Dystopias", (2010) 7:1 SCRIPTed 155, http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp

[57] See generally, Comments of Berin Szoka, *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech*, Dec. 7. 2009 http://ftc.gov/os/comments/privacyroundtable/544506-00035.pdf

> In combination these two behaviours are likely to lead to an excessive scope for opt-in agreements. In turn, users will face more complex decisions as they decide whether or not to participate.[58]

Indeed, why not require users to log-in and provide more information about their real identity? Of course, requiring users to go through an account-creation process would likely turn off many users—if only because it took longer than simply clicking on a dialog box that asked about enabling personalized content. But consumers have become quite accustomed to using Single Sign On systems to log into websites with their Facebook, Twitter, Google or Microsoft Live accounts (and so on). It is not difficult to see such networks becoming federated content networks—the new walled gardens so feared by Tim Wu, Jonathan Zittrain and many others. Leaving a website inside one network and going to the other would require granting another web-wide exception to another network. This isn't necessarily bad but if it ultimately means that *more* information is collected about Internet users, DNT will leave many of its advocates sorely disappointed—and it is certainly not a result any user would have chosen.

This perverse potential (but likely) result simply one example of a larger problem: human rationality is bounded; we are simply not capable of weighing the full implications of choices as complicated as those over privacy. This does not mean that user empowerment is not a worthy goal; it is (and it is generally preferable to more top-down alternatives such as regulatory prescriptions on the use of data). But it *does* mean we should not pretend that choice architects are not, in fact, making important choices for users in the process of designing choice mechanisms like Do Not Track.

The problems described above will become more acute the more broadly "tracking" is defined, the more users turn on DNT:1, and the more cumbersome negotiation is. Two particular contested issues within the TPWG will significantly aggravate the opt-in dystopias problem:

1. **Default Settings** - Although the TPWG has always rested on the consensus that DNT headers must be set by users not user agents like browsers,[59] Microsoft breached that consensus earlier this year when it announced earlier this year that it would choose *for* users by setting DNT:1 on by default in its new IE10 browser. European regulators have

---

[58] *Opt-in Dystopias.*

[59] "The goal of this protocol is to allow a user to express their personal preference regarding tracking to each server and web application that they communicate with... Key to that notion of expression is that it MUST reflect the user's preference, not the choice of some vendor, institution, or network-imposed mechanism outside the user's control." TPE § 3.

essentially endorsed this position, calling for users to "told about any default setting; and prompted to keep or to change it"—even if that setting is DNT:1, and therefore not compliant with the DNT spec—and insisting that servers must not disregard DNT headers, even when sent by browsers that turn on DNT:1 by default.[60] It remains unclear how this issue will be resolved.

2. **Configuration** - The TPWG co-chairs recently rejected a proposal to clarify that, to "reflect the user's preference," user agents must "require equal effort to configure [DNT]"[61]—prompting the first formal objection filed in the TPWG.[62] Thus, unless this decision is ultimately reversed by the W3C, a user agent need not set DNT:1 by default if doing so proved problematic; it need only design a user interface that will achieve the same result.

Ultimately these concerns are likely to be dismissed by insistence that sites and services will simply negotiate around DNT to reach the same outcome they would have reached anyway. But in the real world (as opposed to a frictionless perfect market), transactions costs often swamp the gains created by transactions such as the negotiation between site and user. The online advertising ecosystem currently works because it generated tiny amounts of value from enormous volumes of transactions. Even the small transactions costs of forcing today's implicit quid pro quo to become explicit could produce dramatically different outcomes. Nor is it clear that negotiation or payments would generate as much revenue as advertising—meaning that rising transactions costs would be borne by publishers, and passed on to users in the form of reduced quality, quantity or innovation, or higher prices (if they can actually charge prices).

Building on Ronald Coase's seminal work on the importance of transactions costs, Harold Demsetz offered the basic insight that continues to guide the law and economics of setting defaults (which economists generally refer to as "property rights"): in a frictionless world, if the initial assignment of rights is inefficient, negotiation will inevitably and costlessly solve the problem; but in the real world, that initial assignment may prove sticky, thus we should not assign rights in ways that are inefficient.[63] Once again, choice mechanisms are not neutral. If, the day before Microsoft announced their decision to set DNT:1 by default, it was true that "majority default DNT is not the world this standard will exist in. DNT is going to be a 10%

---

[60] Neelie Kroes, An update on Do Not Track The Centre for European Policy Studies (CEPS)/Brussels, 11 October 2012, http://europa.eu/rapid/press-release_SPEECH-12-716_en.htm

[61] http://lists.w3.org/Archives/Public/public-tracking/2012Sep/0197.html

[62] http://lists.w3.org/Archives/Public/public-tracking/2012Oct/0104.html

[63] Harold Demsetz, *Toward a Theory of Property Rights*, 57:2 Am. Econ. Rev 347 (1967).

[63] http://www.econ.ucsb.edu/~tedb/Courses/Ec100C/Readings/Demsetz_Property_Rights.pdf

solution,"[64] and DNT:1 creates the negative unintended consequences described above (among others), why should choice architects not set the initial assignment to the setting that is more likely to be efficient: DNT:1 *off* by default and not privileged when users configure their browser? An argument could be made to the contrary if it could be shown that "tracking" (as defined by the DNT spec) actually lead to real harm, but as yet, no such argument has been substantiated, and the question of harm has repeatedly been sidestepped within the TPWG.

It is understandable, if ironic, that privacy advocates should desire outcomes that could actually reduce privacy and make consumers worse off—because the chain of causation is attenuated and unclear compared to the noble intentions behind restrictive defaults. Nobody wins Nobel Prizes in Economics for explaining things that are completely obvious, and even once they do, it can take decades (or more) for their insights to permeate areas of discourse outside of economics—such as Internet standard-setting.

It is much more understandable what some market players have to gain by joining forces with well-intentioned but short-sighted privacy advocates: competitive advantage. This is simply another example of the well documented alliance of "bootleggers and baptists."[65] Microsoft, in particular, stands to lose little by disrupting the online advertising market, in which it has struggled to compete. It is by no means clear whether a world of high DNT adoption rates would benefit, in relative terms, Microsoft more than Google (or, for that matter, Facebook), but it might well help Microsoft, since it would generally favor large incumbents with directs relationships with users, such as through the browser and OS. And Microsoft would hardly be the first company to wager that it held a losing hand, and that its odds would be better with a fresh deck of cards.

What lies ahead for choice architects "beyond DNT?" The perpetually difficult task of weighing costs and benefits, and attempting to foresee the unpredictable, in shaping users' choices.

---

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

[65] Bruce Yandle, "Bootleggers and Baptists-The Education of a Regulatory Economist," Regulation 7, no. 3 (1983): 12. http://www.cato.org/pubs/regulation/regv7n3/v7n3-3.pdf

Response to Questions for the Record

of Jonathan Zuck
President
The Association for Competitive Technology

before the
Committee on Energy and Commerce
The Subcommittee on Commerce, Manufacturing, and Trade

on
Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?

Hearing Date March 29, 2012

The Honorable Mary Bono Mack

1. **Question: I understand your point about not regulating technology – we have always strived to remain technology neutral. However, every few months there seems to be a story of software or a device that is discovered collecting information – whether on a phone or on a website – and where the operator claims ignorance.**
    a. **You also state that many of your app developers don't know whether their app creates privacy concerns.**
        i. To clarify, most developers are acutely aware of issues regarding privacy, and take them seriously. However there are areas where information is collected, but may not present "concern". For example, developers use tools like analytics software to understand bugs, track new feature usage, and generally improve their product. Separate and apart from any data breach questions, the collection and use of this information in this manner in unlikely to create "concerns". However we believe even these uses should occur with available consumer notification.

        Therefore we advise app developers to be open with consumers about the information they collect and how it is used. We strongly advocate the use of privacy policies – **even if an app maker believes no information is being collected....**ACT also advises app developers to be mindful of the relationships they have with third parties such as ad networks.

    b. **Is there a role for voluntary technical standards that address performance requirements to limit data collection or indicate what data is collected?**
        i. There is a role for voluntary technical standards. Today, standards and best practices are being developed around three major areas of focus: collection of data; use/sharing of the data; and management of data – we expect these standards to be developed independently, but must be able to work together and have common or compatible definitions and terms.

        We see these standards as vitally essential to a functional system and already exist in similar models. For example, in the telecommunications industry, GSMA and CTIA/ESRB both have guidelines for providers and developers, and CTIA/ESRB has content ratings that include separate privacy notifications. For advertisers, NAI, DAA, IAB, DMA, WOMMA, MMA, and others have guidelines for advertising companies, notifications for consumers, and even best practices for app developers. And advocacy groups like EFF, Public Knowledge, CATO, Mercatus, and others have extensive blog posts, write---ups, and in some cases developer guidance for dealing with consumer information. Most, if not all of these, deal with collection, use/sharing and management of data.

        Voluntary standards provide a system capable of flexibility and quick adjustments to the rapidly changing app marketplace. Moreover, voluntary standards engender industry support and acceptance – acceptance essential to standards for data collection and create clear, functional, and effective notifications to consumers of the types of collection that occurs.

2. **Your testimony described how implementing a regulatory regime for the fast developing and quickly evolving mobile ecosystem is difficult.**

   a. **Will enforceable voluntary standards be any better at keeping pace and remaining relevant?**

      i. Industry self-regulation is capable of moving at the speed of innovation. This is due to the level of expertise in the technology involved, first-hand awareness of upcoming innovations, and a simple business interest to not fall behind competitors. This allows self-regulatory programs to operate prospectively, as opposed to regulatory programs that are often reactive and technologically outdated. Moreover, regulatory processes often try to shoe-horn their existing authority into an ever changing situation and provide a list of prohibitions as opposed to ideals.

      Finally, regulatory rulemakings are governed by long processes that can take months if not years to decide and implement. A rulemaking might finally occur well after the technology has turned a corner, rendering the rulemaking moot and thus ineffective.

3. **You stated a comprehensive approach to the stakeholder process is the "only way" to address consumer privacy. Please explain.**

      i. We need to approach privacy issues in a comprehensive way, not one that creates siloed solutions for each technology, especially since those silos are disappearing every day. Not only does data collection and sharing span all parts of the online and offline worlds, but our industry is moving quickly to blur the lines between smartphones, PCs, cars and even televisions.

      As an example, let's look at one area that NTIA and ACT are both concerned about – ensuring transparency about the data collection and data sharing practices on mobile apps. This is an area that demands improvement and its one reason we've been working with organizations like Mom's With Apps to develop icon-based disclosures that help parents make informed decisions about which kids apps to buy for their kids.

      However, our work in this area has led us to the conclusion that developing disclosures that are designed specifically for an iPhone-sized screen is not the right approach for a broader multistakeholder process. The entire concept of a mobile app that exists only on a smartphone is disappearing as mobile operating systems like Apple's iOS, Google's Android, and Microsoft's Windows Phone are now powering tablets, PC's, televisions, and even car entertainment systems. Mobile apps and the mobile web are going to be running everywhere in the near future, and any solution we develop must be responsive enough to deal with each of these scenarios. Not only will we be dealing with radically different screen sizes, but how will privacy disclosures be handled when the user is downloading an app via voice commands in their new iOS-powered car?

      Everyone in the technology industry must take part and be responsible for improving the state of privacy, security, and transparency across our various

industries. Our app developer members are no different, and we're committed to working this out with government, industry, civil society, and most importantly...our customers.

In the end, we need to create an environment that breeds trust with our customers. That is why we are concerned about approaching these issues based on categories of technology is bound to create incompatibilities, confusion, and most customer distrust.

4. **You object to the process NTIA has set forth in its request for comments because it appears to single out app developers for implementing privacy notices before beginning the rest of the process.**

   a. **Do app developers object to providing consumers a privacy notice?**

      i. No. App developers want to provide consumers with privacy notices to create greater trust with the consumer. In fact ACT has dedicated our resources to helping our developers find improved solutions to providing consumer notice. Additionally, ACT has worked directly with the California State Attorney General to find a way to better provide notice directly on the "app store" page. This uniformity will help developers and help users know where to look to find key privacy information.

I'd like to take a moment to highlight a specific example of ACT's work in this area. We have been working with Moms with Apps, an ACT affiliate group comprised of more than one thousand children's app makers. These developers are parents who decided to make apps to educate their children. They are conscious of privacy concerns and the collection of data because the last thing any of them want is to expose their own children's private information.

Because of their concern, independent developers in Moms with Apps took the initiative to design a parental notification system that identifies the privacy settings of an app in a simple, easy to identify graphical display (below). While this isn't a final solution, it's a great step initiated from within the industry to safeguard user privacy and improve consumer trust.

As you can see from the icons, we are helping to find ways to inform parents quickly, and with a minimum of "legal-eze". We've taken these icons and worked with privacy policy generator privacychoice.org to have them created and added automatically when a developer builds a privacy policy.

b. Should providing consumers a privacy notice be standard practice across the online ecosystem, including apps?

i. Yes. We at ACT strongly advocate the use of privacy policies – even if an app maker believes no information is being collected. We tell this to app developers and help them to create privacy policies at our workshops across the country. While we cannot necessarily speak for the entire industry, much of the online ecosystem already provides consumers with privacy notices. Given recent changes in many app stores, we see providing consumers with a privacy notice as becoming the industry standard, one that is being adopted across all devices.

5. You testified full transparency in the multi-stakeholder process is an impediment to achieving consensus standards. Please explain.

a. ACT fully believes in transparency; within this context I wanted to make a very careful, nuanced point: When *all* proceedings and discussions are required to be public, participants may prevent the kind of frank discussion needed to generate implementable outcomes. Since the NTIA is looking to the ICANN multistakeholder model as template for its privacy process, I look to my experience with the ICANN process.

At ICANN we have seen that if the process takes the form of a public discussion, industry participants will be looking over their shoulders or sitting on their hands instead of offering bold ideas for workable solutions. Fully transparent proceedings will not produce the free exchange of ideas and consensus agreement that is the stated aim of the stakeholder process. For NTIA to get the best results from these efforts, they need to value positive outcomes first.

Moreover, it is important to remember that participants will be searching for a resolution that involves compromise – compromise that could negatively affect their companies' bottom lines or expose their organization to criticism. In order for the best solutions to emerge in a consensus fashion, stakeholders must have confidence that the dialogue provides wide latitude to offer a range of alternatives. To discuss and even reject ideas after listening to peers.

Clearly, we think that the overall process at NTIA, and any event which requires a vote or a decision to be taken be done an open and transparent manner. However we think that all participants should be able to "step away" from the camera at times and have frank discussion, and even disagreements. Furthermore, we think it may even be valuable for NTIA facilitators to hear what they have to say, and keep it confidential.

We understand that this is a subtle point, but effective compromise often takes risk. An environment where no risk goes without immediate public second-guessing is one where no risk is taken.

The Honorable Cliff Stearns

1. **At the hearing we heard that allowing all consumers to access whatever data companies have about them present's significant technical challenges and could actually increase risk to consumers. But what about a narrower bill that would allow consumers to ask companies for categories of information that companies have on them.**
    a. **Wouldn't this alleviate the risk of harm to the consumer and burden on the company while at the same time help educate consumers on data collection?**

        i. We are concerned that a congressionally mandated requirement on businesses to show consumers what categories of information are collected about them will not provide the necessary flexibility and may stifle innovation. However, we do believe that allowing consumers to see this information is helpful to educate consumers and will also alleviate many of their privacy concerns. The good news is that many businesses already make this information available to their customers.

        As I stated in my written testimony, "we advise app developers to be open with consumers about the information they collect and how it is used. We strongly advocate the use of privacy policies – even if an app maker believes no information is being collected." As part of this communication and disclosure, a consumer can identify what types of categories of information have or are being collected about them.

2. **Are you familiar with my bill, H.R. 1528, the Consumer Privacy Protection Act of 2011? This bill calls for clear, easy to understand privacy policy statements and provides for the FTC to approve a five-year self-regulatory program.**
    a. **Would you support this bill advancing through the Subcommittee?**

        i. While ACT supports many aspects of HR 1528, ACT has not taken a public position on H.R. 1528

        Nonetheless, there are many aspects of HR 1528 that we support and even advocate to app developers. We see three valuable features of this legislation:
        1. Your definition of personally identifiable information does not include anonymous data that alone does not "identify a unique living individual."
        2. The preclusion of the private right of action that protects well-intentioned app developers from aggressive plaintiff's bars.
        3. Finally, we like the idea of encouraging businesses to have privacy policies, but we worry that codifying the requirements of a privacy policy may prevent necessary variability in the policies as technology changes.

House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade
Hearing entitled "Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?"
March 29, 2012

Responses to Questions for the Record
Pam Horan, President, Online Publishers Association

The Honorable Mary Bono Mack

1. **You stated your members have every incentive to respect consumer privacy because competitors are only one click away. However, a consumer has little incentive to click to a competitor if all websites operate in the same fashion. Is there a great difference among your members as to how they approach consumer privacy?**

   Our members, which are some of the most well known brands online and offline, work hard to preserve the trusted relationships they enjoy with their audiences. To ensure this trust is maintained, OPA members employ consumer privacy-friendly approaches to data collection, retention and sharing. As you are well aware, there are thousands of websites dedicated to covering news, entertainment, information and sports so our Members are committed to offering its consumers a clean well lighted experience for both the content and environment they deliver.

2. **While it is clear advertisers are paying more for the interest based ads, it is not clear to what extent publishers need the incremental revenue to support their business. Arguments have been made that much of the content provided to consumers for free would disappear if certain advertising models were more difficult to execute, such as behavioral advertising, because website owners and publishers wouldn't be able to earn enough money to support the content. What percentage of your members' online business operates profitably?**

   The majority of the advertising our members serve is contextual (i.e., targeted based on the content of the page that a consumer is viewing at the time an ad is served) -- versus behavioral (i.e., targeted based on actions or behaviors of the consumer observed over time). Based on our most recent survey of OPA members, which reflects figures for the 2011 calendar year, behaviorally-targeted advertisements remain less than 10% of the total paid impressions served for advertising and therefore represent a very small percentage of the revenue.

   a. **What percentage of advertisements are behaviorally targeted ads? What percentage of the total advertising revenue that publishers receive is derived from behavioral advertising?**

   The majority of the advertising our members serve is contextual (i.e., targeted based on the content of the page that a consumer is viewing at the time an ad is served) -- versus behavioral (i.e., targeted based on actions or behaviors of the consumer observed over time). Based on our most recent survey of OPA members, which reflects figures for the 2011 calendar year, behaviorally-targeted advertisements remain less than 10% of the total paid impressions served for advertising and therefore represent a very small percentage of the revenue for our members.

b. **You referenced the DAA program that prohibits using data for employment, credit, healthcare, or insurance purposes – but it does not prohibit the collection of that data. Should such sensitive data be collected at all?**

We share your concern about the collection of "sensitive" data. Typically, publishers do not need to collect this kind of information, and, if they do, it's through an opt-in method.

c. **How do you ensure that if the data is collected it is not sold, resold, and used down the line for those prohibited purposes?**

Our members, which have a unique first-party relationship with their consumers, take great effort to ensure that data, especially sensitive data, is not misused. However, it is nearly impossible for publishers to ensure that unrelated third parties are not providing the same transparency and choice. One of the most important tenets of the DAA self-regulatory program is that the entity collecting data should provide notice and choice regarding the collection of data.

3. **You expressed concerns over the suggestion that first parties be required to disclose the information practices of the third parties with whom they contract. Your two primary concerns were the collection of this practices information and the potential liability for third party actions. Can contract terms address both of these concerns? For instance, could your members propose boilerplate contract language to standardize what the third parties with whom they contract are permitted to do with user information?**

a. **Could your members propose contract terms to indemnify themselves should the third party violate those terms and harm a consumer?**

Indemnification provisions are heavily negotiated terms of contracts and our members do not always have the leverage they need to obtain these contractual protections. Moreover, indemnification clauses offer no protection if the indemnifying party does not have sufficient resources to provide a defense or satisfy an indemnified claim at the time it is made. While contracts are an important tool, they are not a complete solution. One of the important tenets of the DAA self-regulatory program is that the entity collecting data needs to provide transparency and choice to the consumer.

With respect to contractual provisions limiting what third parties can do with audience information, OPA members can and do regularly strive to include such terms in their agreements but our members cannot guarantee that the parties with whom they contract will comply with such restrictions.

OPA has encouraged its members to develop policies governing the collection and use of audience data by technology partners, service providers and other third parties. The terms and implementation of those policies are within the discretion of each member to determine and they will necessarily vary according to the business needs of each company.

Here are three examples illustrative of the efforts of OPA members to safeguard the privacy interests of their users.

ESPN: ESPN has developed a "Verification and Tagging Policy" setting forth requirements regarding the placement of tags and data collection by advertisers and their agencies and third-party vendors in connection with advertising buys on ESPN digital platforms. ESPN's policy requires, among other things, that ESPN must approve all data being collected in connection with

an advertising campaign prior to the commencement of the campaign, and all third-party vendors used by advertisers and agencies, who may be required to agree to abide by ESPN's policies regarding the collection and use of data.

In addition, ESPN regularly checks its site for unknown and unauthorized data collection activity and is reaching out to entities that appear to have tags on ESPN's site that can't be traced to learn about the purpose of those tags and request removal, if appropriate.

The New York Times: The New York Times also published guidelines to clearly communicate with third parties about collection of data and tagging on its site. Its policy states: "Advertisers, their agencies, vendors and other advertising-related third parties are prohibited from collecting user data on NYTimes.com or NYT's other digital properties. These third parties may not capture this data for subsequent ad segmentation or targeting information, or for retargeting messages to those users on other web sites."

The Wall Street Journal: The Wall Street Journal implemented a data policy backed by a comprehensive process that ensures advertisers, agencies, technology partners and other third parties collecting data follow a detailed certification and approval process. The goal is transparency: to know what data is being collected and for what purpose. The approach is backed by regular checks and audits of The Wall Street Journal, for unknown and unauthorized data collection.

While these are just three examples of publishers' initiatives, many publishers include provisions in their contracts that encourage responsible practices by third parties designed to help protect the interests of their site visitors, while ensuring advertisers are getting fair value from their placements.

4. **You expressed concerns over the access and correction proposal, highlighting the burden it places on your members to authenticate users before they are able to access the information your members hold. If so many industries currently authenticate before permitting access to user accounts, why would it be a "significant technical challenge and...actually increase risk to consumers"? For instance, credit card companies and banks are able to quickly and easily authenticate a user both over the phone and online.**

The majority of our members' content doesn't require authentication as it isn't necessary for the access of their content and they are committed to providing a frictionless process. Credit card companies and banks necessarily must collect very personal and sensitive information about a consumer in order to link bank accounts, investments and other financial instruments. Publishers, however, do not usually collect social security numbers or other such personal and sensitive information used to identify a specific individual. The challenge with any "access and correction" requirement would be to correlate data about a specific consumer across multiple websites or services. The only efficient and reliable way to accomplish this would be to assign or collect a unique identifier to each consumer. As a result, we would be forced to collect more personal information about our users, which we believe would increase the risk to the consumer.

The Honorable Cliff Stearns

1. **At the hearing we heard that allowing all consumers to access whatever data companies have about them present's significant technical challenges and could actually increase risk to consumers. But what about a narrower bill that would allow consumers to ask companies for categories of information that companies have on them. Wouldn't this alleviate the risk of harm to the consumer and burden on the company while at the same time help educate consumers on data collection?**

   We don't believe that limiting data requests to categories would alleviate the risk of harm to consumers. The challenge with any "access and correction" requirement would be to correlate data about a specific consumer across multiple websites or services. The only efficient and reliable way to accomplish this would be to assign or collect a unique identifier for each consumer. As a result, the publisher would be forced to collect more personal information about our users, which we believe would increase the risk to the consumer. Even limiting data requests to certain categories would still require publishers to identify the consumer.

2. **Are you familiar with my bill, H.R. 1528, the Consumer Privacy Protection Act of 2011? This bill calls for clear, easy to understand privacy policy statements and provides for the FTC to approve a five-year self-regulatory program. Would you support this bill advancing through the Subcommittee?**

   While the OPA is not endorsing privacy legislation at this time, we appreciate your continued leadership on privacy issues. In particular, we appreciate your understanding that the marketplace is working to develop a solution for consumers. As for clear, easy to understand privacy policy statements, technology changes quickly and many of our members are beginning to utilize new ways to inform consumers about data collection practices and the choices available to them outside of privacy policies by using "just-in-time" notices or other contextually-relevant notices. As for FTC authority, we support the FTC's efforts to use its Section 5 Authority to punish bad actors and support the DAA self regulatory program.

Interactive Advertising Bureau
Public Policy Office
575 7th St., NW
Washington, DC 20004

June 29, 2012

Representative Mary Bono Mack
Chairman, Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Dear Chairman Bono Mack,

Thank you for the opportunity to testify before the Subcommittee on Commerce, Manufacturing, and Trade on Thursday, March 29th, 2012 at the hearing entitled "Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?". Below please find my answers to the written questions from members of the Subcommittee.

<u>The honorable Mary Bono Mack</u>

1. **The Administration's Framework recognizes that targeted ads are generally more valuable and the revenue derived therefrom supports an array of services and content. What percentage of ads served online are targeted versus contextual or randomized?**

The IAB reports quarterly and annual total online advertising revenue as part of our IAB Internet Advertising Report, which we produce in partnership with PwC. This report does not attempt to categorize advertising as either targeted or non-targeted as there is not a commonly agreed upon definition of "targeting". Our end of year report showed that online advertising in the U.S. grew to $31.7 Billion in 2011, a 22% increase over the previous year.

Although we do not routinely report the percentage of ads that are targeted, in 2010 IAB did conduct a survey of the major advertising agencies, or the buy side of the industry, to measure what percentage of the advertising spend would fall under the Federal Trade Commission's (FTC) definition of Third Party Behavioral Advertising. Using the FTC's definition from their February 2009 report entitled, "FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising", <u>we found that greater than 80% of digital advertising campaigns would be covered by the FTC's definition.</u>

Interactive Advertising Bureau
Public Policy Office
575 7th St., NW
Washington, DC 20004

2. How does the IAB's code of conduct differ from the principles put forth in the Administration's framework?

The IAB Membership Code of Conduct incorporates the industry's self regulatory principles, as developed by the Digital Advertising Alliance (DAA), and requires all of IAB's more than 500 member companies to adhere to those practices. The DAA principles cover data transparency, consumer choice, data security, and consumer education practices for the industry. This program was endorsed by the Administration and the DAA was the only industry group that formally participated in the White House press conference on February 23, 2012 where the Administration's privacy report was released. I believe that the DAA program fulfills the consumer privacy goals outlined in these important areas. However, the Administration's privacy report is more expansive than the DAA program, addressing a wide array of global topics such as international harmonization of laws, enforcement of consumer protections, and data security breach notification legislation. The DAA program is not meant to address those broader issues.

3. You testify that NTIA should not interfere with your existing codes of conduct. What role do you see IAB playing in the multi-stakeholder process? What codes of conduct could be covered that are currently not covered by your codes?

As mentioned above, the Administration has lauded the DAA's self regulatory program and endorsed it as a model of success for "enforceable codes of conduct", therefore I do not believe there is a need for the NTIA multi-stakeholder process to delve into the area already covered by the DAA program. However, the DAA program was not developed to address all possible consumer privacy issues, thus there may be areas where the NTIA process can provide guidance and coordination amongst interested parties.

IAB will participate in the first multi-stakeholder meeting currently scheduled for July 12, 2012. That meeting will focus on mobile application notice practices, which is an appropriate topic for a multitude of interest groups to discuss appropriate and implementable options for increasing transparency to the consumer. We look forward to working through this process. We do not believe, however, that the NTIA process should delve into the broader mobile notice and choice issues at this time. The IAB's Mobile Marketing Center of Excellence and the DAA are finalizing mobile privacy principles that will expand the DAA's current program to the mobile platform. Just as the DAA's online behavioral advertising self regulatory program succeeded in increasing consumer transparency and choice in the desktop environment, we believe industry should be afforded the opportunity to deliver real results to consumers in the mobile environment as well.

Interactive Advertising Bureau
Public Policy Office
575 7th St., NW
Washington, DC 20004

4. You state that in general, behavioral advertising is not based on personally identifiable data. On what data is behavioral advertising generally based?

The vast majority of advertising is tailored to the consumer's interest based upon web browsing history that is collected through the use of third party cookies. A cookie is simply a unique identifier that is placed by a single server/entity on a user's web browser. A cookie can only be read by the server that placed it. A typical cookie consists of a randomly generated set of letters and numbers, such as ABC123.

Most advertising on the internet is served by third party advertising networks. If an ad network has a contractual relationship with a website to serve ads on that site, the network's servers will place a cookie on the user's browser. The network will keep a log/record of the site where they served user ABC123 an ad. If that same network is serving ads on another site where user ABC123 visits, the network will be able to read their own cookie and may tailor an ad based upon the previous site that user visited. This practice happens millions of times every second, is performed entirely by servers and algorithms, and is the foundation for the internet's economic model. This type of cookie does not contain personally identifiable data and third party ad networks do not rely upon personally identifiable data to serve relevant ads to consumers.

5. You testify the Council for Better Business Bureaus had the first enforcement action under your self-regulatory program in November, 2001. What is the enforcement mechanism under your program? Are you opposed to FTC enforcement?

The Council of Better Business Bureaus (BBB), founded in 1912, has served as an independent enforcement mechanism for industry advertising and marketing self regulatory programs for many decades. With the trust of consumers and regulators on their side, the trade associations that eventually formed the DAA welcomed the BBB's input as we developed our self regulatory program. Once these principles were published in 2009, the DAA worked with the BBB to establish a new enforcement program to monitor compliance with the DAA principles. The BBB's program, recently renamed the Online Interest-Based Advertising Accountability Program, independently monitors the entire digital advertising ecosystem to detect non-compliance with the DAA program. The BBB program enforces against DAA member and non-member companies, thus ensuring consumers are protected across the internet.

The BBB brought their first round of enforcement cases against 6 companies on November 8, 2011. The BBB recently released a second round of enforcement cases against 7 more

Interactive Advertising Bureau
Public Policy Office
575 7th St., NW
Washington, DC 20004

companies on May 30, 2012. The BBB process is completely transparent and cases of non-compliance are referred to the FTC.

Just as the FTC is an effective and appropriate law enforcement backstop for the BBB enforcement program, the Commission also plays an important role in ensuring compliance with the DAA program through their existing powers under Section 5 of the FTC Act (Unfair Acts or Practices). Participants of the DAA are required to declare their adherence to the DAA principles. If a business is operating outside of their public declaration, the FTC has authority to bring a claim of "deception" against that company. The FTC has successfully settled countless deception cases and their authority here is unquestioned and needs no clarification or expansion in order to be an effective backstop to the DAA program.

<u>The Honorable Cliff Stearns</u>

1. **At the hearing we heard that allowing all consumers to access whatever data companies have about them present's significant technical challenges and could actually increase risk to consumers. But what about a narrower bill that would allow consumers to ask companies for categories of information that companies have on them. Wouldn't this alleviate the risk of harm to the consumer and burden on the company while at the same time help educate consumers on data collection?**

Several companies that operate large third party advertising networks currently offer consumers access to their "profiles". Generally, these profiles contain a number of marketing "buckets" or demographic categories that the company believes best represents the purchase intentions of the various users of a specific computer. Large portals, companies that own both first party websites and third party ad networks like Microsoft, Google, and Yahoo! may be able to combine these profiles with first party registration data from their sites and thus present a specific user an individualized profile. This type of profile access helps increase transparency to the user and I applaud these companies for investing time and resources to develop them.

It is important to note that most third ad networks do not own first party websites and thus are only capable of providing a profile that relates to a computer or specific device, not to the individual. Similarly, these networks do not generally have access to personally identifiable data, which is why most of them do not currently provide user access to profiles. I am worried that any legislative mandate in this area would put an undue burden on third party ad networks to develop these access provisions and would ultimately require these companies to begin to collect more personally identifiably information. This would result in a net/net loss to business activity and consumer privacy.

Interactive Advertising Bureau
Public Policy Office
575 7th St., NW
Washington, DC 20004

2. Are you familiar with my bill, H.R. 1528, the Consumer Privacy Protection Act of 2011? This bill calls for clear, easy to understand privacy policy statements and provides for the FTC to approve a five-year self-regulatory program. Would you support this bill advancing through the Subcommittee?

I am aware of H.R. 1528 and applaud your continued leadership in the area of consumer privacy and protection. I recall the first time I had the pleasure of discussing privacy legislation with you during a U.S. Chamber of Commerce Privacy Retreat. That was in 2002 and your insights into this area were extraordinary back then. We discussed how difficult it could be to legislate in an area where the technology is rapidly evolving and business practice change quickly. Ten years later, these caveats still hold true, which is why I believe that industry self regulation is the most effective means for ensuring we strike the proper balance between protecting consumers and promoting innovation. For example, the DAA issued their original online behavioral advertising principles in 2009, but by the Fall of 2011 we had already updated those principles, and now we are nearing the release of a significant expansion of those principles to cover the mobile platform. There is no way that the Congressional legislative process or the FTC rulemaking process could match this pace of evolution in the marketplace.

As a further example, H.R. 1528 calls for easier to understand privacy policy statements, and while this is a laudable goal, it is unclear whether shorter privacy policies will ever be read by average consumers. Instead of being locked into a codification of best practices, industry self regulation is able to implement new, more creative solutions that deliver real results to consumers. In the area of notice, the DAA program mandates that simple data usage explanations be provided outside of the privacy policy. Today, the industry provides simple to understand, real-time notice via the delivery of the AdChoices Icon. This ubiquitous transparency symbol is being delivered inside more than one Trillion advertisements every single month. This type of innovation would not occur if we had a legislatively-imposed standard.

I appreciate the Subcommittee's interest in my viewpoints and would be happy to provide further details if they would be helpful in the future.

Sincerely,

Mike Zaneis
SVP and General Counsel
IAB

Responses of Justin Brookman to the Additional Questions for the Record for the hearing entitled "Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?" before the Subcommittee on Commerce, Manufacturing, and Trade hearing on Thursday, March 29, 2012.

The Honorable Mary Bono Mack

1. **You testified that it is "well-established that consumers today simply aren't provided with enough insight to make informed choices, even when such choices are available." How do you know consumers are not informed rather than consumers simply choosing not to change the defaults when presented with choices?**

There is overwhelming evidence that consumers by and large do not understand commonplace data collection and transfer practices. For example, a recent study found that 62% of respondents believe that "[i]f a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission."[1] When basic behavioral marketing techniques are described to consumers, a considerable majority state that they would not permit such activity.[2] Moreover, privacy notices are not much help today in informing consumers about actual data practices. Companies are not required to provide information about actual practices, and corporate privacy policies are often written in legalistic boilerplate that the average consumer cannot understand (even if they had the unlimited time in which to read all these policies).[3]

I appreciate that the online advertising industry has committed considerable time and resources to the DAA icon project, but I have no seen meaningful data to support the notion that consumers by and large understand what the icon means. Nor have I seen any user education efforts around the icon despite press releases committing to the same. Anecdotal conversations I have had with ordinary consumers not involved in policy circles suggest that a lot of Americans have not noticed the icons at all. And in the absence of a working "Do Not Track" mechanism, existing tools to opt out of the collection and use of behavioral data are insufficient[4] and confusing.[5] It is to the online industry's credit, however, that they at least allow for the opt out of the usage of behavioral data, as existing law has no such requirement for most consumer information, and there are few (if any) comparable self-regulatory standards around the offline transfer and use of derived consumer data.[6]

I have no problem with people choosing to share information about themselves, including in exchange for goods and services. I do not believe it should be the job of Congress to prevent consumers from "oversharing" with friends or marketers even if I personally would make different choices. Consumers

---

[1] Scott Turow et al., Americans Reject Tailored Advertising and Three Activities that Enable It, September 29, 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.
[2] *Id.*; *accord* Zogby International, Polling Market Research, June 2010, http://www.precursorblog.com/files/pdf/topline-report-key-findings.pdf; Harris Interactive/Westin Poll, April 10, 2008, http://www.harrisinteractive.com/harris_poll/index.asp?PID=894; Annenberg/Samuelson Privacy Policy Findings, November 9, 2007, http://groups.ischool.berkeley.edu/samuelsonclinic/files/annenberg_samuelson_advertising.pdf.
[3] Aleecia McDonald and Lorrie Faith Cranor, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society (2008 Privacy Year in Review issue), available at http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.
[4] Wendy Davis, FTC's Brill: 'Do Not Track' Means Do Not Collect Data, MEDIAPOST, March 2, 2012, http://www.mediapost.com/publications/article/169317/ftcs-brill-do-not-track-means-do-not-collect-d.html.
[5] Peter Leon et al., Why Johnny Can't Opt Out, October 31, 2011, http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html.
[6] Chris Hoofnagle, Privacy Self-Regulation: A Decade of Disappointment, March 4, 2005, http://epic.org/reports/decadedisappoint.html (noting failure of self-regulatory efforts for offline data brokers).

should be empowered to make their own decisions about how and with whom to share personal information. However, for reasons discussed *infra* at Response to Chairman Bono Mack Question 3, existing law strongly disincentives companies from making clear, conspicuous, and detailed disclosures about data collection, usage, and retention practices. Privacy legislation should be introduced to require real transparency about privacy practices.

2. **You referenced the need for baseline privacy protection so that U.S. companies can be competitive in cloud services in the European Union (EU) because consumers and governments distrust U.S. companies with their personal information. A frequent criticism of EU regulators is that, while it is impossible for any company anywhere to comply with certain of their laws and regulations, the EU turns a blind eye to the infractions of EU companies and only enforces against U.S. companies. How much of the push to forego U.S.-based company products, such as cloud services, stems from distrust because the U.S. lacks a formal privacy law and how much stems from competitive favoritism?**

We have yet to see adequate privacy enforcement *at all* from European regulators — against American or European companies — resulting in inadequate protection of user privacy in Europe and uncertainty about the scope of the Data Protection Directive.[7] Certainly there has been aggressive action in recent months with regard to Google and Facebook, though given that no European company can claim as pervasive a web presence, it is difficult to say whether European companies would be treated differently.

I do believe that criticiss of U.S. government access laws are, if not disingenuous, somewhat hypocritical, as European government access laws are in many cases at least as weak as American law and sometimes more so.[8] However, whether some European interests are motivated by protectionist instincts, privacy is regarded as a fundamental right in Europe and regulators I have spoken with have expressed genuine concern about the lack of privacy protection in the United States.[9] While advocacy against U.S. cloud storage may in some cases be overdetermined by both privacy concerns and self-interested favoritism, dissatisfaction about the lack of privacy protection rights in the United States is legitimately held by European institutions.

3. **In your testimony, you mentioned two recent and important FTC enforcement cases in the privacy realm – one against Google and the other against Facebook. It would seem that the FTC has the tools it needs to protect consumers' privacy. Why do you believe we need legislation?**

I disagree with the premise that the Federal Trade Commission has sufficient tools to protect consumers' privacy. Setting aside significant resource issues,[10] the only law that the FTC can typically enforce to

---

[7] Lack of enforcement and the resulting uncertainty about the Directive's scope were identified by the European Commission as two of the primary problems that the proposed Data Protection Regulation are designed to solve. *See* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:HTML.

[8] Winston Maxwell & Christopher Wolf, *A Global Reality: Government Access in the Cloud*, Hogan Lovells White Paper, May 23, 2012, http://www.hldataprotection.com/uploads/file/Hogan%20Lovells%20White%20Paper%20Government%20Access%20to%20Cloud%20Data%20Paper%20(1).pdf.

[9] European Convention on Human Rights, Article 8 ("Everyone has the right to respect for his private and family life, his home and his correspondence.")

[10] Peter Maass, *Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless*, WIRED, June 28, 2012, http://www.wired.com/threatlevel/2012/06/ftc-fail/all/.

protect privacy is Section 5 of the FTC Act which prohibits unfair or deceptive practices. For the most part, the FTC has only brought privacy enforcement actions in cases where there has been *affirmative deception* about privacy practices. That is, a company went out of its way to make a statement about privacy practices (which it didn't have to do) and then later acted in violation of that statement.

In the Google Buzz case, Google had promised users that if it was going to use Gmail information for any purpose other than to provide Gmail service to users, it would get user permission. In later pushing its failed Google Buzz service, Google violated that promise. Similarly, in the Facebook case, Facebook had promised users that they could control who saw their profile information. Later in December 2009, Facebook modified its privacy controls to publicly expose some user information that had in many cases been restricted only to friends.

However, under deceptive practices law, if Google and Facebook had never made those promises, the FTC would not have the authority to enforce against Google and Facebook for misusing consumer information. Certainly, affirmative promises can mold consumer expectations, but in the absence of clear statements, it cannot be the case that consumers have no reasonable expectation that companies are going to treat their information fairly.

For example, with regard to the Google WiFi case, where Google was collecting consumer information broadcast across unencrypted WiFi networks, the FTC was unable to act because Google had never promised not to collect that data, even though consumers should be able to reasonably expect that their wireless communications are not being surveilled.[11] Even though Google was not utilizing the substantive contents of those communications, absent a promise not to do so, they and others may well be able to monitor and use those communications today under existing law. And by conditioning enforcement only on the promises that a company makes, the FTC is strongly discouraging companies from making any privacy promises at all.

The FTC has aggressively exercised its unfairness jurisdiction in *security* cases for the past seven years, and has recently given indications that it may extend its unfairness authority to privacy cases as well. CDT has argued that absent a baseline privacy law, the FTC should seek to enforce the application of the full range of Fair Information Practice Principles through its unfairness authority.[12] However, while the Supreme Court recently stated that an "invasion of privacy" constitutes a "legally cognizable harm,"[13] it is unclear whether courts would uphold the premise that unfairness mandates that companies treat consumer data fairly under the FIPPs. Without more precise legislative or judicial guidance, consumers and companies will operate in a realm of high uncertainty over how data must be treated under the law. We believe that it would be preferable to more clearly articulate the Fair Information Practice Principles in law, and to allow companies to propose safe harbor programs to gain deemed compliance for that law, as has been proposed in legislation introduced by Representative Stearns, Representative Rush, Senators Kerry and McCain, as well as by the European Commission.

4. **There are examples where multi-stakeholder processes have yielded solid results. In this context, however, the various stakeholders' positions are grounded in ideology. With the spectrum of that ideology running so broadly, do you believe the multi-stakeholder process can work?**

---

[11] *Id.*
[12] Refocusing the FTC's role in Privacy Protection, Comments of the Center for Democracy & Technology in regards to the FTC's Consumer Privacy Roundtable, November 6, 2009 https://www.cdt.org/privacy/20091105_ftc_priv_comments.pdf.
[13] *United States v. Alvarez*, 567 U.S. ___ (2012), slip op. at 6-7.

I share the concern that absent privacy legislation (or at least more robust FTC enforcement under unfairness), companies will be in many cases not sufficiently incentivized to participate in a multistakeholder process to negotiate strong privacy protections for consumers.[14] For this reason, we believe that comprehensive privacy legislation should be enacted that allows for the development of voluntary codes of conduct for individual industries to apply the Fair Information Practice Principles to their particular environment. While CDT believes that these codes of conduct would best be worked out in a multistakeholder setting allowing for robust (and early) input from advocates and regulators, we would also support codes developed solely by industry if those codes offered sufficiently privacy protections and were specifically endorsed by the FTC (as provided for in the Rush bill). However, we think a code developed in a multistakeholder format would be more likely to offer strong protections and win the FTC's approval.

5. **You opined that the self-regulatory approach has been a "general failure" and that we need some sort of legislation to set the baseline so the FTC can presumably prosecute those who do not comply with basic privacy practices. However, in its case against Frostwire last year, the FTC established unfairness by arguing that Frostwire employed default settings that were contrary to standard industry practice and that as a result of having different prior experience with other file sharing software, a significant number of consumers could not reasonably avoid unwitting public sharing. The FTC also argued that the non-standard product design conferred no benefits on users. Would you agree this demonstrates that self-regulation works and that the FTC has the authority to prosecute outliers without additional legislation?**

I do not consider the Frostwire case to be a privacy case, but rather a security case that is consistent with the FTC's security enforcement actions of the last several years. In those cases, the FTC has said that failing to utilize reasonable and industry-standard practices to ensure that consumer data is not accidentally exposed to potentially malicious actors constitutes an unfair business practice. It is important to note Frostwire was not trying to encourage users to share information in ways they didn't expect; rather, they happened to design their software poorly in way that exposed user data. Frostwire did not benefit in any way from this feature, which they subsequently called a bug and fixed immediately after it was brought to their attention.[15]

To date, the FTC has failed to extend this concept to privacy cases by arguing that intentional collection, use, retention, and/or transfer of consumer data for a commercial purpose could constitute an unfair practice — whether consistent with industry practices or not. If the FTC were to use unfairness to act against bad privacy practices, industry codes of conduct should constitute one factor in determining what violates a Fair Information Practice Principle but should hardly be dispositive. Industry self-regulation and codes of conduct do provide substantive protections for consumers, but by and large they are too weak in many areas. For example, CDT has previously criticized industry definitions of "sensitive health information" as too narrow, as they encompass only "pharmaceutical prescriptions or medical records" but not web searches or page views on sites related to medical conditions.[16] Similarly, the Digital

---

[14] Justin Brookman, *Two Steps Forward for Privacy*, CDT Blog, February 24, 2012, https://www.cdt.org/blogs/justin-brookman/2402two-steps-forward-privacy.

[15] How an FTC Complaint Helped Frostwire Become Better, GAMECULTURE, October 12, 2011, http://gamepolitics.com/2011/10/12/how-ftc-complaint-helped-frostwire-become-better.

[16] Chart, ONLINE BEHAVIORAL ADVERTISING: INDUSTRY'S CURRENT SELF-REGULATORY FRAMEWORK IS NECESSARY, BUT STILL INSUFFICIENT ON ITS OWN TO PROTECT CONSUMERS, December 2009, at 4 https://www.cdt.org/files/pdfs/CDT%20Online%20Behavioral%20Advertising%20Report%20Comparison%20Charts.pdf.

Advertising Alliance's Self-Regulatory Principles for Multi-Site Data,[17] while a considerable improvement over previous efforts, have been widely criticized as an inadequate response to calls for "Do Not Track" as they allow for substantial collection and retention of consumer data by third parties and focus instead on merely limiting use for targeting ads. [18]

Moreover, industry self-regulation only works (to the extent it works at all) when industry is under intense scrutiny from regulators and advocates. As Professor Peter Swire testified in yesterday's Senate Commerce hearing on privacy, the history of internet self-regulation has shown that when regulators' attention is distracted by other issues, self-regulatory programs have a tendency to fall apart.[19] While we currently live in a time of intense interest in privacy and tracking issues, improved self-regulatory efforts are likely to degenerate if the lens of the press and regulators is turned to other topics, leaving consumers without adequate protection of their privacy.

6. You testified voluntary codes must be endorsed by the FTC to gain consumer trust. Do you believe the advertising industry's code has gained consumer trust?

As noted above in my answer to Chairman Bono Mack's Question 1, it would be very hard to argue that the advertising industry code has yet gained widespread consumer trust. At this point in time, behavioral tracking is not an above-board exchange of value for online content. Today, many users understand that *advertising* funds the content they view on the internet, but the *tracking* is still in most cases obscure to them; they are not making an affirmative choice to provide their data in exchange for content. If consumers were to decide to share information about themselves in exchange for more or better content, or in lieu of paying, I believe that would be a perfectly legitimate market decision. However, I do not believe that is what is happening today.

The Honorable Cliff Stearns

1. At the hearing we heard that allowing all consumers to access whatever data companies have about them presents significant technical challenges and could actually increase risk to consumers. But what about a narrower bill that would allow consumers to ask companies for categories of information that companies have on them. Wouldn't this alleviate the risk of harm to the consumer and burden on the company while at the same time help educate consumers on data collection?

While CDT strongly believes that a comprehensive privacy bill that incorporates all the Fair Information Practice Principles would be best both for companies and consumers, a narrower bill that encompasses a subset of the FIPPs — or even just one — would constitute a marginal improvement for consumes, unless that legislation forestalled legislative process on broader privacy protections. CDT has previously testified[20] in support of information broker access provisions as part of data breach notification laws in the

[17] Website, Digital Advertising Alliance's Self-Regulatory Principles for Multi-Site Data, http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.
[18] Wendy Davis, Lawmakers to W3C: Do-Not-Track Means Do-Not Collect, MEDIAPOST, June 19, 2012, http://www.mediapost.com/publications/article/177140/lawmakers-to-w3c-do-not-track-means-do-not-collec.html.
[19] Testimony of Peter Swire before the Senate Committee of Commerce, Science, and Transportation, on "The Need for Privacy Protections: Is Self-Regulation Adequate?" June 28, 2012, http://commerce.senate.gov/public/?a=Files.Serve&File_id=4c73aa3c-5626-42d6-b6fe-31e3ec6ad1ca.
[20] Testimony of David Sohn before the House Subcommittee on Commerce, Trade, and Consumer Protection, U.S. House of Representatives Committee on Energy and Commerce on "H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act," May 5, 2009, https://www.cdt.org/testimony/testimony-david-sohn-subcommittee-commerce-trade-and-consumer-protection-us-house-represen.

Data Accountability and Trust Act that you have championed.

However, a bill that merely provided consumers with information about the *categories of information* that a company collected and retained about them would be of relatively limited utility. While such a bill would obviate the security risk that data access necessarily creates, it would on the other hand not inform consumers when data held about them is simply wrong, preventing them from correcting inaccurate consumer records.

2. Are you familiar with my bill, H.R. 1528, the Consumer Privacy Protection Act of 2011? This bill calls for clear, easy to understand privacy policy statements and provides for the FTC to approve a five-year self-regulatory program. Would you support this bill advancing through the Subcommittee?

While I am heartened to see good faith, bipartisan efforts to help safeguard user privacy, I do not believe that H.R. 1528 provides sufficient privacy protections in its current iteration. The transparency provisions only require that companies make statements about what they *may* do with data — not what they actually do. To this extent, these transparency statements would likely just mirror existing web privacy policies, which are already mandated by California law, and which have proven to be ineffective in meaningfully protecting user privacy online. As noted above in response to Chairman Bono Mack's Questions 1, 3, absent a requirement to actually describe privacy practices, Section 5 of the FTC Act encourages companies to merely assert a broad reservation of rights that consumers are unlikely to pay attention to.

Moreover, limiting the bill's application to "personally identifiable information" makes less sense in the digital age when the line between identifiable and pseudonymous data is increasingly shrinking and people live more and more of their lives online where their experiences can be dramatically shaped just by the collection and use of pseudonymous data.[21] For this reason, the Federal Trade Commission has moved away from a reliance on PII, as the relevance of that line has "blurred" in recent years.[22] Certainly, focusing only on PII would have no effect whatsoever on most online behavioral advertising, which consumers have expressed significant concerns about and which has dominated (for better or worse) many privacy discussions and self-regulatory efforts in recent years (see Response to Chairman Bono Mack's Questions 1, 5 *supra*).

Furthermore, while mandating choice about secondary usage and transfer of data is a bold and welcome move, the caveat that "information-sharing affiliates" are outside the choice mechanism seems to swallow this rule. Companies can avoid consumer choice merely by committing to follow another company's privacy policy. If that privacy policy can unconditionally assert the right to share with any and all third parties, there is no reason why every company wouldn't gladly agree to be a bound information-sharing affiliate under this rule.

Finally, relying only on notice and choice is unlikely to be sufficient to fully protect user privacy.[23] Other concepts like data minimization and accuracy (see Response to Representative Stearns' Question 1) must be addressed as well. Last year, I testified before this committee on the Sony data breach, when it was reported that Sony had been storing in public-facing databases old credit card information that it no longer

---

[21] Comments of the Center for Democracy & Technology before the Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change" (Interim FTC Privacy Report), February 18, 2011 at 3, https://www.cdt.org/files/pdfs/20110218_ftc_comments.pdf.
[22] FTC Report, Protecting Consumer Privacy in an Era of Rapid Change, http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[23] *Id.*

needed.[24] Privacy law should also require companies to only collect personal information they need, and

to get rid of data that is no longer necessary for the original (or closely related) purposes. To fully protect user privacy, comprehensive privacy law must address the full range of Fair Information Practice Principles.

[24] Testimony of Justin Brookman before the House Subcommittee on Commerce, Manufacturing, and Trade, "The Threat to Data Theft to American Consumers," May 4, 2011, http://republicans.energycommerce.house.gov/Media/file/Hearings/CMT/050411/Brookman.pdf.