RPTS DEAN

DCMN SECKMAN

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

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, D.C.

The subcommittee met, pursuant to call, at 9:05 a.m., in Room 2123, Rayburn House Office Building, Hon. Mary Bono Mack [chairwoman of the subcommittee] presiding.

Present: Representatives Bono Mack, Blackburn, Stearns, Harper, Cassidy, Guthrie, Olson, Pompeo, Kinzinger, Barton, Upton, Butterfield, Gonzalez, Sarbanes, Waxman, and Markey.

Staff Present: Paige Anderson, CMT Coordinator; Charlotte Baker, Press Secretary; Michael Beckerman, Deputy Staff Director; Andy

Duberstein, Deputy Press Secretary; Kirby Howard, Legislative Clerk; Brian McCullough, Sr. Professional Staff Member, CMT; Gib Mullan, Chief Counsel, CMT; Shannon Weinberg, Counsel, CMT; Michelle Ash, Democratic Chief Counsel; 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, 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.

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 exhibit 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 you 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 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, 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. Butterflied of North Carolina, for his opening.

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

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

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.

[The prepared statement of Mr. Butterfield follows:]

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

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

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

The Chairman. Well, good morning, Madam Chair.

Mrs. Bono Mack. Good morning.

The Chairman. 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 customized 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 The Chairman follows:]

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

Mrs. Bono Mack. If the gentleman would yield to Ms. Blackburn.

The Chairman. I am sorry. I yield back the balance of my time.

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.

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

Mrs. Bono Mack. 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.

STATEMENT OF THE HONORABLE 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:]

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

Mrs. Bono Mack. Thank you very much, Mr. Strickling.

Mr. Leibowitz, you are recognized for 5 minutes.

STATEMENT OF THE HONORABLE 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. Strickling follows:]

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

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 yeah, 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:]

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

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 okay. 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 to you 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 majority 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. You don't call 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 consumers 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.

RPTS JOHNSON

DCMN SECKMAN

[10:04 a.m.]

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 broadbased 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 multi-stakeholder 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 and 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. Yeah, for the second violation.

Mr. Stearns. Yeah. Okay. 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. I have had seven

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.

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. Yeah. 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. Yeah, 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 there is 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. Okay. 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. Okay.

Mr. Strickling. I am told 15.

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

Mr. Strickling. Yeah.

Mr. Stearns. Would it make sense, as a first order of business, for the NTIA to formally acknowledge as acceptable those existing, 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.

Dr. 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.

Dr. 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.

Dr. Cassidy. Okay. 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.

Dr. 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.

Dr. 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. 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. Yeah. 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 leaving 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. Okay? 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 principle --

Mr. Markey. No, would you give the right --

Mr. Strickling. 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.

Dr. 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, okay, 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.

Dr. 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.

Dr. Cassidy. Okay. To an extent, it may be caveat emptor; and to an extent, it may be, yeah, they are doing something deceptive.

Mr. Leibowitz. Yeah, 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.

Dr. 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.

Dr. Cassidy. Okay. 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. Okay. 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.

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

Mrs. Bono Mack. 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.

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 subcommittee, 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:]

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

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.

RPTS DEAN

DCMN BURRELL

[11:05 a.m.]

Mr. Zuck. 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 and I 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:]

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

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 websites 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 website'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 website experience.

Last year our members invested over $3 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 websites 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:]

******** INSERT 3-2 ********

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:]

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

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:]

******** INSERT 3-4 ********

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.

Okay, 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

relevant 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. Yeah. By and large I am actually generally okay 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.

Dr. 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 okay, 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 okay?

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 --

Dr. 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.

Dr. 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.

Dr. 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.

Dr. 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.

Dr. 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.

Dr. 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.

Dr. 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?

Dr. 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.

Dr. 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.

Dr. 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. Okay. 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 nongovernment 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 websites? 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 websites 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. Yeah, 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 websites or mobile apps to have a privacy policy?

Mr. Brookman. Yeah. I think --I mean I think all websites 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. Okay, 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 websites?

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 websites 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 websites 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?

RPTS JOHNSON

DCMN BURRELL

[12:15 p.m.]

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. Okay. 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. Okay. 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. Okay.

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 statement of Commissioner Rosch follows:]

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

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 White House and FTC reports follow:]

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

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.

[The prepared statement of Mr. Waxman follows:]

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

[Whereupon, at 12:38 p.m., the subcommittee was adjourned.]