INTERNET PRIVACY: THE VIEWS OF THE FTC, THE FCC, AND NTIA

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

AND THE

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JULY 14, 2011

Serial No. 112–75

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

U.S. GOVERNMENT PRINTING OFFICE

72–908 PDF WASHINGTON : 2012

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

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

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

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

SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE

MARY BONO MACK, California
Chairman

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

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

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

GREG WALDEN, Oregon
Chairman

LEE TERRY, Nebraska
Vice Chairman
CLIFF STEARNS, Florida
JOHN SHIMKUS, Illinois
MARY BONO MACK, California
MIKE ROGERS, Michigan
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
CHARLES F. BASS, New Hampshire
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
BRETT GUTHRIE, Kentucky
ADAM KINZINGER, Illinois
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

ANNA G. ESHOO, California
Ranking Member
EDWARD J. MARKEY, Massachusetts
MICHAEL F. DOYLE, Pennsylvania
DORIS O. MATSUI, California
JOHN BARROW, Georgia
DONNA M. CHRISTENSEN, Virgin Islands
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
DIANA DEGETTE, Colorado
JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California *(ex officio)*

C O N T E N T S

WITNESSES

Page

SUBMITTED MATERIAL

INTERNET PRIVACY: THE VIEWS OF THE FTC, THE FCC, AND NTIA

THURSDAY, JULY 14, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE
JOINT WITH THE
SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittees met, pursuant to call, at 11:04 a.m., in room 2123 of the Rayburn House Office Building, Hon. Mary Bono Mack (chairman of the Subcommittee on Commerce, Manufacturing, and Trade) presiding.

Members present from the Subcommittee on Commerce, Manufacturing, and Trade: Representatives Bono Mack, Blackburn, Stearns, Bass, Harper, Lance, Cassidy, Olson, McKinley, Pompeo, Butterfield, Rush, Schakowsky, and Waxman (ex officio).

Members present from the Subcommittee on Communications and Technology: Representatives Walden, Terry, Bilbray, Gingrey, Scalise, Latta, Guthrie, Kinzinger, Barton, Upton (ex officio), Eshoo, Markey, Matsui, Barrow, and DeGette.

Staff present: Jim Barnette, General Counsel; Ray Baum, Senior Policy Advisor/Director of Coalitions; Allison Busbee, Legislative Clerk; Paul Cancienne, Policy Coordinator, Commerce, Manufacturing, and Trade; Nick Degani, Detailee, Federal Communications Commission; Neil Fried, Chief Counsel, Communications and Technology; Brian McCullough, Senior Professional Staff Member, Commerce, Manufacturing, and Trade; Jeff Mortier, Professional Staff Member; Gib Mullan, Chief Counsel, Commerce, Manufacturing, and Trade; David Redl, Counsel, Telecom; Kelsey Guyselman, Legal Intern; Shannon Weinberg, Counsel, Commerce, Manufacturing, and Trade; Michelle Ash, Democratic Chief Counsel, Commerce, Manufacturing, and Trade; Roger Sherman, Democratic Chief Counsel, Communications and Technology; Felipe Mendoza, Democratic Counsel; William Wallace, Democratic Policy Analyst; Sarah Fisher, Democratic Policy Analyst; and Alex Reynolds, Democratic Legal Intern.

Mrs. BONO MACK. Please come to order. Good morning.

From data breaches in the United States to a cell phone hacking scandal in Great Britain, consumer privacy has become part of our national consciousness. Today, we have a unique opportunity to make a real difference in the lives of millions of Americans, and

I look forward to working with Chairman Walden and members of both of our subcommittees on this unique challenge.

We often hear that privacy laws in Europe are much stricter than they are in the U.S., and if that is so, it is hard to understand how the phone hacking incidents in Britain could have gotten so far out of hand. It raises the question of whether American consumers are as vulnerable as politicians and celebrities in London. I hope that Chairman Genachowski will address this issue as we continue to gather facts.

The chair now recognizes herself for an opening statement.

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

This morning, we begin a very important and, some say, long-overdue debate. When it comes to the Internet, how do we—as Congress and as Americans—balance the need to remain innovative with the need to protect privacy?

The explosive growth of technology has made it possible to collect information about consumers in increasingly sophisticated ways. Sometimes the collection and the use of this information is extremely beneficial; other times, it is not. Frankly, I am somewhat skeptical right now of both industry and government. I don't believe industry has proven that it is doing enough to protect American consumers, while government, unfortunately, tends to overreach whenever it comes to new regulations. That is why this debate must be deliberate and thoughtful, but without question, it is time for this debate to take place.

Even though it serves billions of users worldwide—and this year e-commerce in the U.S. will top $200 billion for the first time—the Internet pretty much remains a work in progress. Still, in just 25 years, the Internet already has spurred transformative innovations. It has indefinite value and it has become a 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.

But the Internet has brought about more subtle cultural changes as well. Think about it for a second. If a total stranger knocked on your door one day and asked you for your name, your birthday, your relationship status, your number of children, your educational background, email address, and Social Security number, would you give that information out freely? Probably not.

Yet today, as consumers, we willingly dole out this personally identifiable information online—literally bit by bit. This information is then compiled and collated by computers to produce personal profiles used in online behavioral marketing and advertising. This data mining helps to pay the freight for all of the information that we get for free on the Internet. But does it come at too great of an expense to consumer privacy? That question cuts to the heart of this very important issue.

Applications providers continue to increase the variety of tools available to American consumers to control their privacy settings, but a nagging problem for most consumers is the lack of a basic understanding about how companies use and collect this informa-

tion. While survey after survey indicates that consumers harbor serious concerns about their privacy, it is unproven and unclear whether more stringent laws and regulations relating to the collection and use of data will satisfy these concerns in a way that encourages continued innovation and an expansion of electronic commerce.

As Congress takes a closer look at online privacy issues, industry has stepped up its self-regulatory efforts relating to the collection and use of consumer information. These industry-wide efforts include expanded consumer education and site transparency to increase consumer comfort with how industry uses their information, as well as the development of new preference profiles so consumers can personalize their browsing experience and control just how much information they actually want to share.

As I listen closely to all of your thoughts, I would also like to share a few of my own with you. First and foremost, greater transparency is needed to empower consumers. While it is still unclear to me whether government regulations are really needed, providing consumers with more transparency is the first step in better protecting Americans.

Consumers should be notified promptly if there is a material change in a privacy policy; no bait-and-switch schemes should be allowed nor tolerated.

Sensitive information should have greater safeguards in place, especially when it comes to financial and personal health records.

We should take a long look at how our children are treated online and how they are marketed to.

And we need to closely re-examine privacy laws that are currently on the books. Do we need a single regulator to protect consumer privacy? While I personally support this concept, we should first look at its potential impact on consumers.

And finally, what part should "no harm, no foul" play in this debate? Over the last few months, the FTC and the Department of Commerce have issued extensive reports concerning online privacy. However, there is little proof of any substantive consumer harm. Before regulations are enacted, there should be a "definable" problem such as we are seeing in the area of data protection.

As we move ahead with our hearings, I look forward to a robust discussion with all of my colleagues on the committee as well as industry and consumer groups. Working together, we can make innovation and privacy a shared priority, and the Internet will be the eighth Wonder of the World.

And now I would like to recognize the gentleman from North Carolina, Mr. Butterfield, the ranking member of the Subcommittee on Commerce, Manufacturing, and Trade for 5 minutes for his opening statement.

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

Opening Statement of the Honorable Mary Bono Mack
Subcommittee on Commerce, Manufacturing and Trade &
Subcommittee on Communications and Technology
"Internet Privacy: The Views of FTC, FCC & NTIA"
July 14, 2011
(Remarks as Prepared for Delivery)

Good morning. From data breaches in the United States to a cell phone hacking scandal in Great Britain, consumer privacy has become part of our national consciousness. Today, we have a unique opportunity to make a real difference in the lives of millions of Americans, and I look forward to working with Chairman Walden and members of both of our subcommittees on this unique challenge.

We often hear that privacy laws in Europe are much stricter than they are in the U.S. If that's so, it's hard to understand how the phone hacking incidents in Britain could have gotten so far out of hand. It raises the question of whether American consumers are as vulnerable as politicians and celebrities in London. I hope that Chairman Genachowski will address this issue as we continue to gather facts.

This morning, we begin a very important and, some say, long overdue debate. When it comes to the Internet, how do we – as Congress and as Americans – balance the need to remain innovative with the need to protect privacy?

The explosive growth of technology has made it possible to collect information about consumers in increasingly sophisticated ways. Sometimes the collection and use of this information is extremely beneficial; other times, it's not. Frankly, I am somewhat skeptical right now of both industry and government. I don't believe industry has proven that it's doing enough to protect American consumers, while government, unfortunately, tends to overreach whenever it comes to new regulations. That's why this debate must be deliberate and thoughtful, but without question, it's time for this debate to take place.

Even though it serves billions of users worldwide – and this year e-commerce in the United States will top $200 billion for the first time – the Internet pretty much remains a work in progress. Still, in just 25 years, the Internet already has spurred transformative innovations. It has incalculable value. It has become part of our daily lives. And it has unlimited potential to affect positive social and political change, as the world dramatically witnessed during The Arab Spring.

But the Internet has brought about more subtle cultural changes as well. Think about it for a second. If a total stranger knocked on your door one day and asked for your name, birth date, relationship status, number of children, educational background, email address and Social Security number, would you give that information out freely? Probably not.

Yet today, as consumers, we willingly dole out this personally identifiable information online – literally bit by bit. This information is then compiled and collated by computers to produce personal profiles used in online behavioral marketing and advertising. This data mining helps to pay the freight for all of the information that we get for free on the Internet. But does it come at too great an expense to consumer privacy? That question cuts to the heart of this very important issue.

Applications providers continue to increase the variety of tools available to American consumers to control their privacy settings, but a nagging problem for most consumers is the lack of a basic understanding about how companies use and collect this information. While survey after survey indicates that consumers harbor serious concerns about their privacy, it is unproven and unclear whether more stringent laws and regulations relating to the collection and use of data will satisfy these concerns in a way that encourages continued innovation and an expansion of electronic commerce.

As Congress takes a closer look at online privacy issues, industry has stepped up its self-regulatory efforts relating to the collection and use of consumer information. These industry-wide efforts include expanded consumer education and site transparency to increase consumer comfort with how industry uses their information, as well as the development of new preference profiles so consumers can personalize their browsing experience and control just how much information they actually want to share.

As I listen closely to all of your thoughts, I would also like to share a few of my own thoughts with you.

First and foremost, greater transparency is needed to empower consumers. While it's still unclear to me whether government regulations are really needed, providing consumers with more transparency is the first step in better protecting Americans.

Consumers should be notified promptly if there is a material change in a privacy policy; no bait and switch schemes should be allowed nor tolerated.

Sensitive information should have greater safeguards in place, especially when it comes to financial and personal health records.

We should take a long look at how our children are treated online and how they are marketed to.

We need to closely re-examine privacy laws that are currently on the books. Do we need a single regulator to protect consumer privacy? While I personally support this concept, we should first look at its potential impact on consumers.

And finally, what part should "no harm, no foul" play in this debate. Over the last few months, the Federal Trade Commission and the Department of Commerce have issued extensive reports concerning online privacy. However, there is little proof of any substantive consumer harm. Before regulations are enacted, there should be a "definable" problem, such as we are seeing in the area of data protection.

As we move ahead with our hearings, I look forward to a robust discussion with all of my colleagues on the committee as well as industry and consumer groups. Working together, we can make innovation and privacy a shared priority, and the Internet the 8th Wonder of the World.

Mr. BUTTERFIELD. Let me inquire. Was it my understanding that this side was going to be allowed 20 minutes to make opening statements and I can yield those as I see fit? Is that right?

Mrs. BONO MACK. I will yield them for you.

Mr. BUTTERFIELD. I see. That will be fine. That will be fine.

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

Let me thank the two chairmen for holding today's joint hearing on Internet privacy. I look forward to the testimony from the three witnesses as we begin to talk about this very important issue. I also look forward to learning how Congress can better equip these three agencies so that we can best protect American's online privacy.

With nearly every aspect of our lives now containing an online component, it is vitally important that American's have reasonable protections for the personal information held and sold by the data-gathering industry. That personal information can include specific Web sites a user has visited, how long they spent on that Web site, whether or not they purchased something, what they purchased, and what they looked at while they were there. It can even record their keystrokes. The personal information is collected often without a user's knowledge and without their consent.

When a Web site installs tiny files on a user's computer to record Internet activity, these files are called cookies or flash cookies or beacons. While the term "cookie" doesn't sound particularly invasive, a recent investigation by the Wall Street Journal found that a test computer visiting the 50 most popular Web sites resulted in more than 2,000 cookies being installed without notification or consent on the test computer. What is worse is that the top 50 Web sites directed at children placed substantially more tracking files on visitors' computers than general audience Web sites. The Wall Street Journal found children's Web sites place 4,100 cookies and other tracking mechanisms on their test computer, again, without notice or consent.

Even more concerning is that the data-gathering industry has developed ways to marry online data with offline data like warranty cards and property records and voter registration records and even driver's licenses to build super-files that are sold for pennies. Some companies are even using these super-files to differentiate which of the same type of product they will offer to potential customers. For example, a life insurance clearing house Web site tested a system that would recommend different policies based on the personal information contained in the files. This practice is called "boxing," and I would argue that it is nothing more than a high-tech form of economic and social discrimination.

In addition, having all this data in one place puts Americans at risk of other more traditional high-tech harms like identity theft and fraud. It is clear that businesses need to collect some information for their operational needs. Beyond that, however, I think it is well past the time to put in place some clear and comprehensive rules to let consumers know and exercise some control over what

data gatherers can collect, how they can collect, and what they can do with it once they have it.

Madam Chairman, I hope you will work with me to craft legislation that will safeguard American's personal information so they can continue to use the amazing and infinite potential of the Internet in the safest and most secure ways possible.

Thank you. I yield back the balance of my time.

Mrs. BONO MACK. I thank the gentleman. The chair now recognizes Mr. Walden, chairman of the Subcommittee on Communications and Technology, for 5 minutes.

Mr. WALDEN. Thank you, Madam Chairman. I want to welcome our witnesses.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

As consumers are increasingly living their lives on the Internet—and even more on their Smartphones—concern is obviously growing over electronic communications privacy. Indeed, the Energy and Commerce Committee has taken an active role in investigating online privacy in the last few Congresses. Mr. Barton, for example, has sought out information from a number of companies about their practices regarding Internet advertising and consumers' online information. Members of the committee have reached out to Google about privacy concerns arising from "Google Buzz," as well as their collection of data from personal Wi-Fi networks, something I know the FCC is examining.

And just this past April, Chairman Upton, Chairwoman Bono Mack, and myself, along with our Democratic colleagues, also sent letters to several mobile operating system providers such as Apple asking hard questions about the location-based services they provide and about the privacy protections attached to those services. And both the Communications and Technology and the Commerce, Manufacturing, and Trade Subcommittees have had a number of hearings in recent years.

Now, we are having this hearing because we want to make sure Americans have adequate information regarding how data about them and their Internet use is collected, used, and shared, and to make sure their privacy is protected. But we must balance that need with the recognition that regulatory overreach could curb the ability of entrepreneurs to invest, innovate, and create jobs and new technologies. At this point, it is not clear what legislation—if any—is necessary, but this hearing will help shed light on this question.

As we move forward, one thing stands out in my mind: Today's regime is neither competitively nor technologically neutral. Section 222 of the Communications Act gives the Federal Communications Commission broad authority to implement privacy protections for consumers of wireline and wireless telephone services. Section 222 also specifically calls out location-based services for regulation, but applies that regulation only to carriers and not providers of devices, operating systems, or applications. Other parts of the Communications Act give the Commission authority over cable operators and satellite television providers under a "prior consent" framework.

In stark contrast, there are few if any communications privacy regulations governing web-based companies, even those that can access a user's search queries, emails, voice and video online conversations, web browser, and even operating systems.

So why should a wireless provider that transmits data to and from a Smartphone be subject to Federal oversight but not an operating system provider that has access to the exact same data?

If we move forward with legislation, how do we create a fair playing field? Do we regulate web-based companies up? Do we deregulate traditional phone and video companies down? Do we create a unified regime at the FCC? At the FTC? Or do we have both agencies administer equivalent regimes over different subsets of companies or devices?

So I look forward to hearing from our witnesses on what steps they are taking on electronic communications privacy and what recommendations they have for us as we examine these issues.

One more thing: Although we are here today to talk about Internet privacy, I want to echo Mrs. Bono Mack's concerns about what happened in the United Kingdom. And I will be interested in hearing from Chairman Genachowski if things like this have happened in the United States, whether it falls within the FCC's purview and, if so, what the FCC and other Federal agencies typically do about it.

With that, I appreciate the opportunity to share those comments and yield the balance of my time to the vice chairman of the Communications and Technology Subcommittee, the gentleman from Nebraska, Mr. Terry.

[The prepared statement of Mr. Walden follows:]

Statement of the Honorable Greg Walden
Chairman, Subcommittee on Communications and Technology
Hearing on Internet Privacy
July 14, 2011
(Remarks Prepared for Delivery)

Welcome Chairman Genachowski, Assistant Secretary Strickling, and Commissioner Ramirez, and thank you for coming to testify about your respective agencies' work in the area of Internet privacy.

As consumers are increasingly living their lives on the Internet—and even more on their smartphones—concern is growing over electronic communications privacy.

Indeed, the Energy and Commerce Committee has taken an active role in investigating online privacy in the last few Congresses. Mr. Barton, for example, has sought out information from a number of companies about their practices regarding Internet advertising and consumers' online information. Members of the committee have reached out to Google about privacy concerns arising from "Google Buzz," as well as their collection of data from personal Wi-Fi networks, something the FCC is examining. Just this past April, Chairman Upton, Chairwoman Bono Mack, and I, along with our Democratic colleagues, also sent letters to several mobile operating system providers such as Apple asking hard questions about the location-based services they provide and about the privacy protections attached to those services. And both the Communications and Technology and the Commerce, Manufacturing, and Trade Subcommittees have had a number of hearings in recent years.

We are having this hearing because we want to make sure Americans have adequate information regarding how data about them and their Internet use is collected, used, and shared, and to make sure their privacy is protected. But we must balance that need with the recognition that regulatory overreach may curb the ability of entrepreneurs to invest, innovate, and create jobs. At this point, it is not clear what legislation—if any—is necessary, but the hope is that this hearing will help shed additional light on that question.

As we move forward, one thing stands out in my mind: Today's regime is neither competitively nor technologically neutral. Section 222 of the Communications Act gives the Federal Communications Commission broad authority to implement privacy protections for consumers of wireline and wireless telephone services. Section 222 also specifically calls out location-based services for regulation, but applies that regulation only to carriers and not providers of devices, operating systems, or applications. Other parts of the Communications Act give the Commission authority over cable operators and satellite television providers under a "prior consent" framework. In stark contrast, there are few if any communications privacy regulations governing web-based companies, even those that can access a user's search queries, emails, voice and video online conversations, web browser, and even operating systems.

Why should a wireless provider that transmits data to and from a smartphone be subject to federal oversight, but not an operating system provider that has access to the exact same data?

If we move forward with legislation, how do we create a fair playing field? Do we regulate web-based companies up? Do we deregulate traditional phone and video companies down? Do we create a unified regime at the FCC? At the FTC? Or do we have both agencies administer equivalent regimes over different subsets of companies or services?

I look forward to hearing from our witnesses on what steps they are taking on electronic communications privacy, and what recommendations they have for us as we examine these issues.

One more thing: Although we're here today to talk about Internet privacy, I want to echo Ms. Bono Mack's concerns about what happened in the United Kingdom. I will be interested in hearing from Chairman Genachowski if things like this have happened in the United States, whether it falls within the FCC's purview and, if so, what the FCC and other federal agencies typically do about it.

###

OPENING STATEMENT OF HON. LEE TERRY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEBRASKA

Mr. TERRY. Thank you, Mr. Chairman.

And this is a necessary hearing and I want to thank our panel. It is a powerhouse panel and I thank you for coming up here, Mr. Strickling. I think we should have an office for you you are up here so much anymore.

I think two words or two principles regarding privacy policy—one is balance and the next is transparency. There is no doubt that if there is one drawback or inhibition about ecommerce, it is the consumers fear over violation of privacy. We know when we do a transaction online that we have to provide information to the entity that we are doing business with or engaging in some type of commerce with. What we don't expect—unless it is transparent and open to us to help make our decision—is the use of that data. It has to be easy for the consumer and for the company but also something that everyone knows up front.

What we can't have and what degrades the confidence is what has occurred with Google Buzz, a trusted company that now has obtained personal information and we have no idea what it can be used for or will be used for. Or when major companies or entities hack to obtain personal information. All of these things should be clear. They are not transparent. There is no balance involved in those and that is what we need to deal with.

Mrs. BONO MACK. I thank the chair and the vice chair and I am happy to now recognize the ranking member of the Communications and Technology Subcommittee, Ms. Eshoo, for her 5 minutes.

Ms. ESHOO. Thank you, Madam Chair. It is nice to see you in the chair.

OPENING STATEMENT OF HON. ANNA G. ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Today marks our first joint subcommittee hearing of the 112th Congress on Internet privacy. And I welcome it and welcome the distinguished witnesses that we are going to hear from.

The government agencies that are testifying today have taken initial steps to address the issue of Internet privacy, but I think we need a unified approach that leverages the expertise of both the public and the private sectors. The FTC has conducted a series of roundtables exploring privacy issues and has proposed a framework for approaching these issues. The FCC brings years of experience managing communications, privacy issues dating back to wiretap legislation in the late 1960s. And the NTIA has played a significant role in establishing the Department of Commerce's Internet Policy Taskforce's Report on Commercial Data Privacy and Innovation in the Internet Economy. That is a real mouthful. There should be some acronym for that I guess.

Personal privacy is, I believe, a very closely held American value. I think it is in our DNA. We don't want the government to know; we don't want companies to know. We just hold it very, very close. And today, information is shared more freely and faster than ever before, especially by the younger generation. We need in our coun-

try a comprehensive approach to privacy. And it may be appropriate to start by updating the rules protecting children online.

Children on the Internet share photos, email addresses and phone numbers with friends and family. There are advancements in Smartphone technology, which enables parents to monitor the location of their children. But based on a town hall meeting that I had on the issue, parents need an awful lot of education on this. They have a sense of what is going on but they don't know what to do with it or how to.

The Children's Online Privacy Protection Act enacted more than 10 years ago—I can't believe that over a decade has passed since we did that—never really anticipated these advancements. So whether dealing with children, teens, or adults, transparency really needs to be the coin of the realm. It should be the central focus of ours.

Consumers should know what personal information is being collected, how it is being used, and who has access to that data. At a minimum, companies should be required to disclose if they buy or sell consumers' information or if they track the whereabouts of consumers even after they have left a company's Web site. Both the public and private sectors have a lot of work to do to educate consumers and businesses and ensure that the collection of data is done in a transparent and secure manner.

I think it is also important that we don't overlook the proactive steps being taken by industry to enhance user privacy. According to Facebook, almost 35 percent of their 350 million users customize their privacy settings using options provided by the company. Similarly, millions of users of the popular Web browser Mozilla Firefox install add-ons to prevent online advertisers from collecting their information. And Reputation.com, based in my district, is developing tools to help consumers and businesses protect their online privacy. But it is spotty. There isn't anything that ties all of this together and I think that is why we are here today.

So I think with the right balance, we can protect privacy without inhibiting job creation and the development of new innovative data-driven apps and services. There is such a demand for that in our country and we don't want to stand in the way of it. Our government agencies have a difficult task ahead of them, I think. Each of our agency witnesses today is going to provide an expert view on the issue of Internet privacy and I really look forward to hearing what you have to say.

Specifically, I would like to know what each agency thinks their role should be, what their hand is in this, and how we can leverage the wide range of online privacy tools developed by the private sector because it is both. And how do we increase coordination between government agencies, as well as industry?

At this point, Madam Chair, it has been mentioned today, I would like to call on the Chairman of the full committee to use the jurisdictions of this committee to probe the whole issue of privacy, hacking, and this burgeoning scandal of News Corporation. It fits with the subject matter that we are here in a joint hearing today for. This is one of the most powerful committees in the Congress. We certainly have the jurisdiction and I think it needs to be exercised.

So again, I welcome the panel and I thank you for the testimony that you are going to give and look forward to hearing it.

And I yield back.

Mrs. BONO MACK. The gentlelady's time has expired. And the chair is pleased to recognize the Chairman of the full committee, Mr. Upton, for 3 minutes.

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

Mr. UPTON. Thank you, Madam Chair. I am excited about the hearing. This committee has been at the forefront of protecting the privacy of Americans for many, many years. And that mission certainly continues today.

When I became Chairman of this great committee about 6 months ago, I guaranteed that our focus would be on jobs, the economy, and the preservation of individual freedoms. And I ask everyone to look at our mid-year report, which we released last week. There is a good deal in there about the literally millions—hundreds of thousands of jobs that this committee has worked to protect and create.

Today, though, we begin a very thorough analysis of what has become an essential freedom for all Americans. The Internet has changed all of our lives in so many ways. Our freedom—unlike that elsewhere in the world—to use the Internet for information, commercial purposes, consumer needs, even healthcare—is unrivalled. And anyone who has access to a computer, even a BlackBerry, has access to the entire world. But that freedom also brings some very serious challenges. Privacy is chief among them.

So I commend these two subcommittees for holding this hearing. And as we begin the effort, it is entirely appropriate to hear first from our Federal witnesses, and I certainly welcome them.

But I want to get the issue right. We all do. It is not and should not be partisan in any way and I don't believe that it is. If it means that the CMT and the C and T Subcommittees, even Oversight, need to hold multiple hearings, so be it. We need to hear from everyone with a stake in Internet privacy before we contemplate legislating.

I yield now the balance of time to the gentlelady from Tennessee, Ms. Blackburn.

[The prepared statement of Mr. Upton follows:]

Opening Statement, Energy and Commerce Chairman Fred Upton
Joint Hearing of the Subcommittees on Commerce, Manufacturing, and Trade and Communications and Technology
Internet Privacy: The Views of the FTC, the FCC, and NTIA
July 14, 2011
(Remarks as Prepared for Delivery)

I am excited about this hearing. The Energy and Commerce Committee has been at the forefront of protecting the privacy of Americans for many years. That mission continues today.

When I became Chairman of this great Committee just about six months ago, I guaranteed that our focus would be on jobs, the economy, and the preservation of individual freedom. I ask everyone to look at our mid-year report, which I released last week – there is a great deal in there about the millions of jobs that this Committee has worked to protect and create.

Today, though, we begin a very thorough analysis of what has become an essential freedom for all Americans. The Internet has changed all of our lives in so many ways. Our freedom – unlike that elsewhere in the world – to use the Internet for information, commercial purposes, consumer needs, even our health care – is unrivalled. Anyone who has access to a computer has access to the entire world.

That freedom brings some very serious challenges. Privacy is chief among them.

So I commend my leader in this effort, Chairman Bono Mack, and my good friend from Oregon, Chairman Walden, for holding this hearing today. As we begin this effort, it is entirely appropriate to hear first from our federal witnesses, and I welcome them.

I want to get this issue right. It is not, and should not be, partisan in any way. If it means the CMT and/or the C&T Subcommittees need to hold multiple hearings, so be it. We need to hear from everyone with a stake in Internet privacy before we contemplate legislating.

Mrs. BLACKBURN. Thank you, Mr. Chairman.

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

And to add a couple of points to the discussion as we move forward with our witnesses today—whom we do welcome and we appreciate your being here—we should bear in mind that online advertising sales, online ad revenue totaled $31 billion last year and that represented 40 percent of global online sales. That spending sustains much of our free press and free content online. That is something we should be mindful on as we look at regulation in a space that really is growing by leaps and bounds, creating jobs, and providing consumers with a dynamic platform for free content and innovative services. I think the European-style Do Not Track technology would short-circuit much of this innovation. And as Chairman Bono Mack said, it did not stop this situation there in the U.K.

I think that what we also have to do is be mindful of moving forward with anything where there is an ill-defined harm standard without respect to the cost that would be placed on private innovators and on the industry that is experiencing growth. We need to be cautious, thoughtful, and well-measured in our approach to this evolving issue.

And I yield back my time.

Mrs. BONO MACK. I thank the gentlelady. And the chair now recognizes Mr. Stearns for 1 minute.

Mr. STEARNS. Thank you, Madam Chair.

OPENING STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Having had some experience developing privacy bills—I have with Jim Matheson from Utah this H.R. 1528, the Consumer Privacy Protection Act of 2011—and having been through these hearings, one of the things that clearly came out is exactly what you said, Madam Chairman, when you talked about consumers want transparency and a basic understanding of how their information is used. That came out time and time again so you are absolutely right there.

And I think that when we look at this very important issue and I listen to stakeholders, I find that, Madam Chair, that the stakeholders by and large would like to know if there is one agency that has jurisdiction so they know where to go to, how to comply, and if we are not careful and we have this jurisdiction that is moved between two or three—two or three government agencies can make it more difficult. So I think one of the things that we have today is a hearing to talk about jurisdiction. And I hope in the end that we won't have competing jurisdiction and we will have at least one central agency with this jurisdiction.

Thank you.

Mrs. BONO MACK. Thank the gentleman. And the chair now recognizes the ranking member of the full committee, Mr. Waxman, for 5 minutes.

Mr. WAXMAN. I want to thank our Chairs Bono Mack and Walden for holding this hearing today.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

As the Wall Street Journal just pointed out, firms are stripping away our Internet users' anonymity and "gaining the ability to decide whether or not you would be a good customer before you tell them a single thing about yourself." The collection, use, and dissemination of consumer information provides many benefits to consumers, businesses, and the marketplace, but they raise legitimate concerns about whether consumers have adequate control over personal information that is shared.

Sophisticated business models and rapidly evolving technologies allow vast amounts of data to be collected, aggregated, analyzed, mined, and sold in ways that were unimaginable only 10 years ago. Many of these business practices conflict with consumers' expectation of privacy.

I understand that the Republican majority is weary of passing any piece of legislation that calls for new regulations. We have heard the repeated calls for self-regulation. The problem is that self-regulation isn't working. Just this week, Stanford researcher Jonathan Mayer reported in Tracking the Trackers that eight members of the self-regulatory group Network Advertising Initiative, NAI, seemed to outright violate their own privacy policies. That is nearly 13 percent of the 64 companies investigated. In addition, NAI is just one of many self-regulatory efforts. So the consumer is not left knowing where to turn.

Furthermore, even if the firms were complying, the self-regulatory efforts seem to be limited to allowing the consumer to opt out of behaviorally targeted advertising, but not the collection of information that makes targeting possible. The Tracking of the Trackers study found that 33 members of NAI either left tracking cookies on users' computers or installed tracking cookies after the users opted out. The firm seemed to argue that they could continue to keep cookies on your machine as long as those cookies aren't being used to create specifically targeted ads.

I also understand that the Republican majority has stated that it is not sure whether legislation is needed or that it does not intend to move too quickly on this important issue. I think it is well past time to move ahead. There were six privacy hearings in the 111th Congress. At each of those six hearings, they made me more and more convinced that current law does not ensure proper privacy protections for consumer information.

As I have stated in the past, I stand ready to work with my colleagues. This is not a partisan issue. It should not be a partisan issue. We have got to give the consumers the tools to protect their privacy without unduly burdening industry or stifling innovation. That should be our goal. This hearing can move us in that direction and I look forward to the testimony that we are going to receive.

Am I permitted to reserve the time or do I have to yield?

Mrs. BONO MACK. You are allowed to yield your time.

Mr. WAXMAN. I would like to yield to Mr. Markey.

OPENING STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF MASSACHUSETTS

Mr. MARKEY. I thank the gentleman very much. And it is good to see you in the chair, Madam Chair. Nancy Pelosi has acclimated the Democrats to a woman in the chair and it is good to see a Republican woman as well in such a position.

In May, I introduced bipartisan legislation with Joe Barton to strengthen privacy safeguards for children and teenagers. A bill—the Do Not Track Kids Act—would update the Children's Online Privacy Protection Act for the 21st Century to cover newer applications and services like geo-location technologies that didn't exist when we passed the Children's Privacy Act 13 years ago that I was the author of. That bill is the communications constitution when it comes to protecting kids online, but we need to amend it to take into account the explosive growth and innovation in the online ecosystem since 1998. 1998 was way back in the BF era, the before-Facebook era.

And in addition to updating that law, our bill also contains commonsense protections for teenagers. Our bill's digital marketing bill of rights stipulates that Web sites, online apps, operators, and operators of mobile apps directed to teens clearly explain why they need to collect the data. Our bill also prohibits operators from collecting geo-location information without permission from parents when we are talking about children. And it finally includes an eraser button. That is an important privacy protection which requires operators of Web sites' online applications that contain or display personal information about children or minors to enable users to erase or otherwise eliminate publicly available personal information on a Web site about children.

I would hope that the least that we can accomplish this year is to provide a privacy bill of rights for children in our country. We can see now what the implications are if that information gets hacked, and my hope is that we can update the 1999 law to accomplish that goal.

I thank you, Madam Chair. I thank the gentleman from California.

Mrs. BONO MACK. I thank the gentleman. And the chair now recognizes Mr. Barton for 5 minutes.

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

Mr. BARTON. Thank you, Madam Chairwoman. I appreciate you and Chairman Walden holding this hearing. I want to associate myself with what Mr. Waxman and Mr. Markey just said. If you have Joe Barton and Ed Markey on a bill, you pretty well covered the political spectrum not only of this committee but of the Congress.

And I couldn't agree more with what former Chairman Waxman and current Ranking Member Waxman said, that privacy is not a partisan issue, and I do believe, as he said, that it is time to act. And hopefully, this hearing and several others that we have already had with the testimony we hope to hear from our administration officials will lead to action in this Congress.

I am cochairman of the bipartisan Privacy Caucus. I have been an advocate for privacy for almost 20 years in the Congress. In this year alone I have sent letters, most of them with Mr. Markey or Mr. Walden or Mr. Stearns or others to Facebook, AT&T, Sprint, the College Board, ACT, and even the Social Security Administration questioning activities that they have engaged in that appear to impinge on our citizens' privacy.

As Mr. Markey indicated, I have also introduced H.R. 1895, the Do Not Track Kids Act of 2011. And this legislation does five important things. First of all, it updates the Children's Online Privacy Protection Act of 1998. It adds protections for our citizens between the ages of 13 and 17. It would prohibit an Internet company from sending targeting advertising to children and minors. It would also prohibit Internet companies from collecting personal and location information from anyone who is less than 13 years of age without parental consent, and anyone less than 18 without individual consent. It would require Web site operators to develop something called an eraser button, which would give children and minors the ability to request deletion of their personal information that they do not wish to be available on the Internet.

The time has come, Mr. Chairman and Madam Chairwoman. We know that we need a vigorous Internet, we know that we need a vibrant economy, but we should all agree that we certainly need to protect our privacy in the Internet age just as much as we did in the age before the Internet.

With that, I would like to yield the balance of my time to Mr. Olson of Texas for such comments as he wishes to make.

[The prepared statement of Mr. Barton follows:]

Opening Statement of the Honorable Joe Barton
Chairman Emeritus, Committee on Energy and Commerce
Subcommittee on Communications, Technology, and the Internet
"Internet Privacy: The Views of the FTC, the FCC, and NTIA"
July 14, 2011

I am glad to know that the committee is beginning to discuss the issue of online privacy. I would like to thank the chairman for holding this hearing, and I would like to welcome our witnesses. I look forward to hearing their views on this important topic.

As a co-chairman of the bi-partisan privacy caucus, I serve as an advocate and leading voice for online consumer protection. I have sent countless letters to various companies, businesses, and agencies to inquire about their online privacy protections. In this Congress, for instance, I have sent letters to companies such as Facebook, AT&T, Sprint, College Board, and ACT. I have even sent a letter to the Social Security Administration questioning their practices of discontinuing the mailings of earned-entitlement statements.

In addition, I introduced H.R. 1895, the Do Not Track Kids Act of 2011 with my friend from across the aisle Mr. Markey. This legislation does five important things:

1. Updates the Children's Online Privacy Protection Act of 1998 (COPPA) to make the act applicable to advanced mobile technologies and applications;

2. Adds protections to those ages 13-17,this is called the "Digital Marketing Bill of Rights for Teens," and it reinforces protections for those 12 and under;

3. Prohibits internet companies from sending targeted advertising to children and minors;

4. Prohibits internet companies from collecting personal and location information from anyone less than 13 years of age without parental consent and anyone less than 18 without individual consent. This prohibition is designed to prevent internet companies from developing online profiles of children; and

5. Requires website operators to develop an "eraser button" method to give children and minors the ability to request a deletion of all of their personal information they do not wish to be available on the internet, to the extent technologically feasible.

The issue of online privacy protections has become a hot topic due to the rapid growth of the internet. I think that we can all agree that the internet has become a thriving force in this country, and as of March 2011, there are an estimated 2.1 billion users worldwide. With more people using the internet, there are more opportunities for personal information to be misused, and I believe that all Americans should have a choice in how their personal information is handled.

With that Mr. Chairman, I would like to yield one minute to my friend from Texas Mr. Pete Olson.

OPENING STATEMENT OF HON. PETE OLSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. OLSON. I thank my colleague from Texas. And I thank Chairman Upton, Walden, and Madam Chairman Bono Mack for you all's leadership in calling this important hearing.

As this is my first privacy-related hearing, I am approaching the issue with an open mind but not an empty mind. I think the key with approaching privacy is doubts, transparency, and facts. And that is why we are here today.

Consumers are becoming increasingly aware of their own privacy. It is important for them to know what information is being collected about them and how it is being used. In today's global economy, information is a valuable commodity, but we have to closely examine the many economic benefits the Internet and the data collection provides consumers and our economy and balance those with legitimate privacy concerns. We cannot legislate in search of a problem.

So I look forward to examining this important issue further and to playing a proactive role in the future privacy discussions.

I thank my colleague from Texas for the time and yield back.

Mrs. BONO MACK. I thank the gentleman and am happy to recognize the gentleman from Georgia, Mr. Barrow, for 1 minute.

OPENING STATEMENT OF HON. JOHN BARROW, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

Mr. BARROW. Thank you, Madam Chair.

I am glad we are meeting today to discuss this issue. You know, this issue is a whole lot more important to a lot of people than most folks realize because most folks just don't realize how much they open themselves up when they go online, how much of their personal information is being stolen or misused every time they go online.

In the interest of time, I am going to cut to the chase. I understand industry's need for legitimate and even playing field across the country and customers' need on different sides of the same state boundary to a reasonable expectation of privacy every time they go online. I recognize the need for that. I come down heavily on the side of privacy, though, but I am interested in understanding how we can set forth rules of the road that are good for industry but protect the same shared expectation of privacy that folks have on different sides of the same state boundary. Folks have a right to expect a reasonable degree of privacy when they go online no matter where they live in this country. So I feel the need for us to do that.

I look forward to discussing how we can do this, and I believe today's hearing is a big step in that direction. I want to thank our witnesses for addressing these concerns today. And with that, I yield back.

Mrs. BONO MACK. I thank the gentleman. And the chair recognizes the gentlelady from California, Ms. Matsui, for 2 minutes.

OPENING STATEMENT OF HON. DORIS O. MATSUI, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. MATSUI. Thank you, Madam Chair, and all the other chairs for holding today's hearing. I would like to thank our distinguished panelists for being with us this morning. It is nice to see you all on this important issue.

Today, millions of Americans rely on a variety of services and applications for a number of activities, including social networking and navigation and mapping services, among many others. As we all know, in today's economy, information is everything to everyone. We also know that technology changes continuously, every day. What is new today may not be new tomorrow. We must continue to encourage American innovation and foster growth and development of the next-generation technologies. But it is also essential that we properly protect the private and personal information of consumers, particularly our young people.

Privacy policies and disclosures should be clear and transparent. We should also understand the scope of information that is being collected, what it is being used for, the length of time it is being retained, and its security. Ultimately, meaningful privacy safeguards should be in place while ensuring that we don't stifle innovation. It is clearly a fine balance but we need to do it.

I thank you again for holding this important hearing today, and I look forward to working with my colleagues on this issue, and I yield back my time.

Mrs. BONO MACK. I thank the gentlelady. And the chair recognizes the gentlelady from Illinois, Ms. Schakowsky, for 1 minute.

OPENING STATEMENT OF HON. JANICE D. SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Ms. SCHAKOWSKY. I wanted to thank you, Madam Chairman and Congressman Walden, for holding today's hearing. I especially want to say to you that I appreciate the work that we have done over several years on the issues of Internet security and your leadership on this issue.

As a long-time consumer advocate, I have serious concerns about tracking practices, especially the undisclosed data gathering of user behavior. That is why I am an original sponsor of Congresswoman Speier's Do Not Track Me Online Act. This bill would establish standards for a consumer-friendly do-not-track mechanism. I am also a cosponsor of Congressman Markey's Do Not Track Kids Act, which would offer enhanced protections against the tracking of children and teens, and I urge the committee to consider these and other commonsense solutions to the tracking issue as soon as possible.

I associate myself also with my colleagues who want to investigate the—or want more answers anyway—on the hacking scandal of the Murdoch Enterprises and its implications. We must hold Internet service providers and search engines accountable for their actions and I look forward to hearing from our panel today.

Thank you and I yield back.

Mrs. BONO MACK. I thank the gentlelady and thank my colleagues for their opening statements and now we turn our attention to our panel.

We have one panel of witnesses joining us today. Each of our witnesses has prepared an opening statement that will be placed into the record. Each of you will have 5 minutes to summarize the statement in your remarks.

On our panel we have the Honorable Julius Genachowski, Chairman of the Federal Communications Commission; we have the Honorable Edith Ramirez, Commissioner of the Federal Trade Commission; and our third witness is the Honorable Lawrence Strickling, Assistant Secretary for the National Telecommunications and Information Administration.

Good morning. We welcome you back to the hearing room. And again, you will be each recognized for 5 minutes, and I am sure you are very familiar with the timers on the table. As you know, when the light turns yellow, you will have 1 minute left. So as I have been admonished, please remember to make sure your microphone is on and close to your mouth.

And at this point I am pleased to recognize Commissioner Ramirez for 5 minutes.

STATEMENTS OF EDITH RAMIREZ, COMMISSIONER, FEDERAL TRADE COMMISSION; JULIUS GENACHOWSKI, CHAIRMAN, FEDERAL COMMUNICATIONS COMMISSION; AND LAWRENCE E. STRICKLING, ASSISTANT SECRETARY FOR COMMUNICATIONS AND INFORMATION, AND ADMINISTRATOR, NATIONAL TELECOMMUNICATION AND INFORMATION ADMINISTRATION

STATEMENT OF EDITH RAMIREZ

Ms. RAMIREZ. Thank you. Chairman Bono Mack, Chairman Walden, Ranking Members Butterfield and Eshoo, and members of the subcommittees, I am Edith Ramirez, a commissioner of the Federal Trade Commission. I appreciate the opportunity to present the Commission's testimony on Internet privacy.

Today, personal information about consumers may be collected, sold, and used in almost every conceivable interaction a consumer has both online and offline. For instance, a college freshman sits in her dorm room using the Internet to research depression for a paper she is writing for a psychology class. When her research is done, she applies online for student loans to help her pay for her tuition. Later, heading out of her dorm room, she grabs her smartphone, which she uses to find the closest drugstore. At the drugstore, she uses a loyalty card to get discounts. Afterwards, when the student is back online surfing the Web and keeping up with friends on a social network, she sees advertisements for medication for depression and anxiety, as well as ads for high-interest credit cards and payday loans.

These activities—made possible by technology unimaginable years ago—offer clear benefits to the student. She enjoyed easy access to information, received discounts at the drugstore, and connected with friends, all in the course of a few hours. But the student is likely unaware that data about her drugstore purchases,

Web activities, and location may have been sold to data brokers she has never heard of and added to a growing digital profile about her. She may not know that this information may be used for marketing purposes or to make decisions about her eligibility for credit. And she might be especially surprised to learn that her research into depression may be included in her digital profile and could be used when she applies for life insurance or might be sold to prospective employers when she graduates a few years later.

This student is not alone in her lack of awareness that vast quantities of information about her are mined and sold every day. Most consumers have no idea that so much information about them can be accumulated and shared among so many companies, including employers, retailers, advertisers, data brokers, lenders, and insurance companies.

The FTC wants consumers to have an effective notice and meaningful choices about what data is collected about them and how it is used. That in turn will engender the consumer confidence and trust that are essential for industry to continue to innovate and flourish.

For decades, the FTC has been the Nation's lead law enforcer on consumer privacy and data security. During this time, we have also engaged in substantial policy initiatives and educated consumers and businesses on privacy and data security. In recent months, we have brought a number of significant enforcement actions in this area, as described in our written testimony. Just 2 weeks ago, we announced an action against Teletrack, a company that sold lists identifying cash-strapped consumers to marketers in violation of the Fair Credit Reporting Act. To resolve our allegations, the company has agreed to pay a $1.8 million civil penalty and to submit to a court order that ensures that consumers' sensitive credit report information is not sold for marketing purposes.

Privacy and data security also continue to be at the forefront of the FTC's policy agenda. In December, Commission staff issued a preliminary privacy report that recommended three bedrock principles. The first is privacy by design, the idea that companies should embed privacy protections into their products and services from the start. Second, companies should present choices about the privacy of personal data in a simple way and at the time they are making decisions about that data. Third, companies should improve the transparency of their privacy practices thereby promoting competition on privacy.

Finally, a staff report called for the adoption of Do Not Track, a one-stop tool for consumers to control online behavioral tracking. The Commission has not taken a position on whether Do Not Track legislation is needed, but a majority of commissioners, myself included, supports widespread implementation of Do Not Track.

In closing, I want to note that the Commission appreciates the committee's focus on consumer privacy and data security and we are prepared to provide any assistance that you may need on these critical issues. Thank you.

[The prepared statement of Ms. Ramirez follows:]

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Internet Privacy: The Views of the FTC, the FCC, and NTIA

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

and

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

July 14, 2011

I. Introduction

Chairman Bono-Mack, Chairman Walden, Ranking Member Butterfield, Ranking Member Eshoo, and members of the Subcommittees, I am Edith Ramirez, a Commissioner of the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on consumer privacy.

Privacy has been an important part of the Commission's consumer protection mission for 40 years.[2] During this time, the Commission's goal in the privacy arena has remained constant: to protect consumers' personal information and ensure that they have the confidence to take advantage of the many benefits offered by the dynamic and ever-changing marketplace. To meet this objective, the Commission has undertaken substantial efforts to promote privacy in the private sector through law enforcement, education, and policy initiatives. For example, since 2001, the Commission has brought 34 cases challenging the practices of companies that failed to adequately protect consumers' personal information; more than 100 spam and spyware cases; and 16 cases for violation of the Children's Online Privacy Protection Act ("COPPA").[3] The

---

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any other Commissioner. Commissioner William E. Kovacic dissents from this testimony to the extent that it endorses a Do Not Track mechanism. Commissioner J. Thomas Rosch dissents to the portions of the testimony that discuss and describe certain conclusions about the concept of Do Not Track. Commissioner Rosch also has some reservations about the proposals in the preliminary staff privacy report. *See* attached statement, Statement of Commissioner J. Thomas Rosch, Dissenting in Part, *Internet Privacy: The Views of the FTC, FCC, and NTIA*, Before the Subcomm. on Commerce, Manufacturing, and Trade and Subcomm. on Communications and Technology of the H. Comm. on Energy and Commerce, 112th Cong., July 14, 2011 (hereinafter "Rosch Statement").

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

[3] 15 U.S.C. §§ 6501-6508.

Commission also has distributed millions of copies of educational materials for consumers and businesses to address ongoing threats to security and privacy. And the FTC examines the implications of new technologies and business practices on consumer privacy through ongoing policy initiatives, such as a recent proposed privacy framework.

This testimony begins by describing some of the uses of consumer data that affect consumers' privacy today. It then offers an overview of the Commission's recent enforcement, education, and policy efforts. While the testimony does not offer views on general privacy legislation, the Commission continues to encourage Congress to enact data security legislation that would (1) impose data security standards on companies, and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.[4]

II. Information Flows in the Current Marketplace

For today's consumer, understanding the complex transfers of personal information that occur offline and online is a daunting task. Indeed, these information flows take place in almost every conceivable consumer interaction. For example, a consumer goes to work and provides sensitive information to her employer, such as her Social Security Number, to verify her employment eligibility, and bank account number, so that she can get paid. After work, she uses

---

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

an application on her smartphone to locate the closest ATM so that she can withdraw cash. She then visits her local grocery store and signs up for a loyalty card to get discounts on future purchases. Upon returning home, the consumer logs onto her computer and begins browsing the web and updates her social networking profile. Later, her twelve-year old grabs her smartphone and plays games on a mobile app.

All of these activities clearly benefit the consumer – she gets paid, enjoys free and immediate access to information, locates places of interest, obtains discounts on purchases, stays connected with friends, and can entertain herself and her family. Her life is made easier in myriad ways because of information flows.

There are other implications, however, that may be less obvious. Her grocery store purchase history, web activities, and even her location information may be collected and then sold to data brokers and other companies she does not know exist. These companies could use her information to market other products and services to her or to make decisions about her eligibility for credit, employment, or insurance. And the companies with whom she and her family interact may not maintain reasonable safeguards to protect the data they have collected.

Some consumers have no idea that this type of information collection and sharing is taking place. Others may be troubled by the collection and sharing described above. Still others may be aware of this collection and use of their personal information but view it as a worthwhile trade-off for innovative products and services, convenience, and personalization. And some consumers – some teens for example – may be aware of the sharing that takes place, but may not appreciate the risks it poses. Because of these differences in consumer understanding and attitudes, as well as the rapid pace of change in technology, policymaking on privacy issues presents significant challenges.

As the hypothetical described above shows, consumer privacy issues touch many aspects of our lives in both the brick-and-mortar and electronic worlds. In the offline world, data brokers have long gathered information about our retail purchases, and consumer reporting agencies have long made decisions about our eligibility for credit, employment, and insurance based on our past transactions. But new online business models such as online behavioral advertising, social networking, and location-based services have complicated the privacy picture. In addition, the aggregation of data in both the online and offline worlds have in some instances led to increased opportunities for fraud. For instance, entities have used past transaction history gathered from both the online and offline world to sell "sucker lists" of consumers who may be susceptible to different types of fraud. In both the online and offline worlds, data security continues to be an issue. The FTC continues to tackle each of these issues through enforcement, education, and policy initiatives.

III. Enforcement

In the last 15 years, the Commission has brought 34 data security cases; 64 cases against companies for improperly calling consumers on the Do Not Call registry;[5] 86 cases against companies for violating the Fair Credit Reporting Act ("FCRA");[6] 97 spam cases; 15 spyware (or nuisance adware) cases; 16 cases against companies for violating COPPA; and numerous cases against companies for violating the FTC Act by making deceptive claims about the privacy and security protections they afford to consumer data. Where the FTC has authority to seek civil penalties, it has aggressively done so. It has obtained $60 million in civil penalties in Do Not

---

[5] 16 C.F.R. Part 310.

[6] 15 U.S.C. §§ 1681e-i.

Call cases; $21 million in civil penalties under the FCRA; $5.7 million under the CAN-SPAM Act;[7] and $6.2 million under COPPA. Where the Commission does not have authority to seek civil penalties, as in the data security and spyware areas, it has sought such authority from Congress.

And these activities do not fully reflect the scope of the Commission's vigorous enforcement agenda, as not all investigations result in enforcement actions. When an enforcement action is not warranted, staff closes the investigation, and in some cases it issues a closing letter."[8] This testimony highlights the Commission's recent, publicly-announced enforcement efforts to address the types of privacy issues raised by the hypothetical scenario described above.

First, the Commission enforces the FTC Act and several other laws that require companies to maintain reasonable safeguards for the consumer data they maintain.[9] Most recently, the Commission resolved allegations that Ceridian Corporation[10] and Lookout Services, Inc.[11] violated the FTC Act by failing to implement reasonable safeguards to protect the sensitive consumer information they maintained. The companies offered, respectively, payroll processing

---

[7] 15 U.S.C. §§ 7701-7713.

[8] *See* http://www.ftc.gov/os/closings/staffclosing.shtm.

[9] *See* the Commission's Safeguards Rule, 16 C.F.R. Part 314, implementing provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(b), and the Commission's Disposal Rule, 16 C.F.R. Part 682, implementing provisions of the FCRA, 15 U.S.C. §§ 1681e, 1681w.

[10] *Ceridian Corp.*, FTC Docket No. C-4325 (June 8, 2011) (consent order), *available at* www.ftc.gov/opa/2011/05/ceridianlookout.shtm.

[11] *Lookout Servs., Inc.*, FTC Docket No. C-4326 (June 15, 2011) (consent order), *available at* www.ftc.gov/opa/2011/05/ceridianlookout.shtm.

and immigration compliance services for small business employers. As a result, they both obtained, processed, and stored highly-sensitive information – including Social Security numbers – of employees. The Commission alleged that both companies failed to appropriately safeguard this information, which resulted in intruders being able to access it. The orders require the companies to implement a comprehensive data security program and obtain independent audits for 20 years.

Second, the Commission enforces the FCRA, which, among other things, prescribes that companies only sell sensitive consumer report information for "permissible purposes," and not for general marketing purposes. Last month, the Commission announced an FCRA enforcement action against Teletrack, Inc., which provides consumer reporting services to payday lenders, rental purchase stores, and certain auto lenders so that they can determine consumers' eligibility to receive credit.[12] The Commission alleged that Teletrack created a marketing database of consumers and sold lists of consumers who had applied for payday loans to entities that did not have a permissible purpose. The Commission asserted that Teletrack's sale of these lists violated the FCRA because the lists were in fact consumer reports, which cannot be sold for marketing purposes. The Commission's agreement with Teletrack requires it to pay $1.8 million in civil penalties for FCRA violations.

Third, the Commission has been active in ensuring that companies engaged in social networking adhere to any promises to keep consumers' information private.[13] The

---

[12] *See U.S. v. Teletrack, Inc.*, No. 1:11-CV-2060 (N.D. Ga. filed June 24, 2011) (proposed consent order), *available at* http://www.ftc.gov/opa/2011/06/teletrack.shtm.

[13] *See, e.g., Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 2, 2011) (consent order), *available at* http://www.ftc.gov/opa/2010/06/twitter.shtm (resolving allegations that social networking service Twitter deceived its customers by failing to honor their choices after offering

Commission's recent case against Google alleges that the company deceived consumers by using information collected from Gmail users to generate and populate its social network, Google Buzz.[14] The Commission charged that Google made public its Gmail users' associations with their frequent email contacts without the users' consent and in contravention of Google's privacy policy. As part of the Commission's proposed settlement order, Google must implement a comprehensive privacy program and conduct independent audits every other year for the next 20 years.[15] Further, Google must obtain affirmative express consent for product or service enhancements that involve new sharing of previously collected data.

Fourth, the Commission has sought to protect consumers from deceptive practices in the behavioral advertising area. Last month, the Commission finalized a settlement with Chitika, Inc., an online network advertiser that acts as an intermediary between website publishers and advertisers.[16] The Commission's complaint alleged that Chitika violated the FTC Act by offering consumers the ability to opt out of the collection of information to be used for targeted advertising – without telling them that the opt-out lasted only ten days. The Commission's order prohibits Chitika from making future privacy misrepresentations. It also requires Chitika to

---

the opportunity to designate certain "tweets" as private).

[14] *Google, Inc.*, FTC File No. 102 3136 (Mar. 30, 2011) (consent order accepted for public comment), *available at* www.ftc.gov/opa/2011/03/google.shtm. Commissioner Rosch issued a concurring statement expressing concerns about the terms of the proposed consent agreement, *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzstatement.pdf.

[15] This provision would apply to any data collected by Google about users of any Google product or service, including mobile and location-based data.

[16] *Chitika, Inc.*, FTC Docket No. C-4324 (June 7, 2011) (consent order), *available at* http://www.ftc.gov/opa/2011/03/chitika.shtm.

provide consumers with an effective opt-out mechanism, link to this opt-out mechanism in its advertisements, and provide a notice on its website for consumers who may have opted out when Chitika's opt-out mechanism was ineffective. Finally, the order requires Chitika to destroy any data that can be associated with a consumer that it collected during the time its opt-out mechanism was ineffective.

Finally, the Commission has sought to ensure that data brokers respect consumers' choices. In March, the Commission announced a final order against US Search, a data broker that maintained an online service, which allowed consumers to search for information about others.[17] The company allowed consumers to opt out of having their information appear in search results for a fee of $10. The Commission charged that although 4,000 consumers paid the fee and opted out, their personal information still appeared in search results. The Commission's settlement requires US Search to disclose limitations on its opt-out offer and to provide refunds to consumers who had previously opted out.

IV. Education

The FTC conducts outreach to businesses and consumers in the area of consumer privacy. The Commission's well-known OnGuard Online website educates consumers about many online threats to consumer privacy and security, including spam, spyware, phishing, peer-to-peer ("P2P") file sharing, and social networking.[18]

Last month, the FTC issued a new consumer education guide called "Understanding

---

[17] *US Search, Inc.*, FTC Docket No. C-4317 (Mar. 14, 2011) (consent order), *available at* http://www.ftc.gov/opa/2010/09/ussearch.shtm.

[18] *See* www.onguardonline.gov. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alerta en Línea have attracted nearly 12 million unique visits.

Mobile Apps: Questions and Answers." The guide provides consumers with information about mobile apps, including what apps are, the types of data they can collect and share, and why some apps collect geolocation information.[19] The FTC issued the guide to help consumers better understand the privacy and security implications of using mobile apps before downloading them.

The Commission has also issued numerous education materials to help consumers protect themselves from identity theft and to deal with its consequences when it does occur. The FTC has distributed over 3.8 million copies of a victim recovery guide, *Take Charge: Fighting Back Against Identity Theft*, and has recorded over 3.5 million visits to the Web version.[20] In addition, the FTC has developed education resources specifically for children, parents, and teachers to help children stay safe online. In response to the Broadband Data Improvement Act of 2008, the FTC produced the brochure *Net Cetera: Chatting with Kids About Being Online* to give adults practical tips to help children navigate the online world.[21] In less than one year, the Commission distributed more than 7 million copies of *Net Cetera* to schools and communities nationwide.

Business education is also an important priority for the FTC. The Commission developed a widely-distributed guide to help small and medium-sized businesses implement appropriate data security for the personal information they collect and maintain.[22]

---

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

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

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

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

Another way in which the Commission seeks to educate businesses is by publicizing its complaints and orders and issuing public closing letters. For example, the Commission recently sent a letter closing an investigation of Social Intelligence Corporation, a company that sold reports to employers about potential job applicants.[23] The reports included public information gathered from social networking sites. The investigation sought to determine Social Intelligence's compliance with the FCRA.[24] Although the staff decided to close the particular investigation, the public closing letter served to notify similarly situated businesses that, to the extent they collect information from social networking sites for employment determinations, they must comply with the FCRA. The letter included guidance on the obligations of such businesses under the FCRA. For example, companies must take reasonable steps to ensure the maximum possible accuracy of the information reported from social networking sites. They must also provide employers who use their reports with information about the employers' obligation to notify job applicants if they were denied employment on the basis of these reports, and to provide such applicants with information about their rights under the FCRA.

V. Policy Initiatives

The Commission reviews its rules periodically to ensure that they keep pace with changes in the marketplace.[25] The Commission is currently reviewing its rule implementing

---

[23] Letter from Maneesha Mithal, Associate Director, Division of Privacy & Identity Protection to Renee Jackson, Counsel to Social Intelligence Corporation (May 9, 2011), *available at* www.ftc.gov/os/closings/110509socialintelligenceletter.pdf.

[24] FTC staff did not express an opinion on the merits of Social Intelligence's business model.

[25] For example, the Commission recently announced plans to enhance the agency's longstanding program to review rules and guides in order to increase transparency and public participation and reduce burden on business. *See, e.g.*, Prepared Statement of the Federal Trade

COPPA and anticipates that any proposed changes will be announced in the coming months.[26]

In addition to reviewing rules, the Commission's policy initiatives also include public workshops, reports, and policy reviews to examine the implications of new technologies and business practices on consumer privacy. For example, in December 2009, February 2010, and March 2010, the FTC convened three public roundtables to explore consumer privacy issues, including the issues facing the hypothetical consumer discussed in Section II above.[27] The roundtables examined the effectiveness of current privacy approaches in addressing the challenges of the rapidly evolving market for consumer information, including consideration of the risks and benefits of consumer information collection and use; consumer expectations surrounding various information management practices; and the adequacy of existing legal and self-regulatory regimes to address privacy interests. At the roundtables, stakeholders across the board emphasized the need to improve the transparency of businesses' data practices, simplify the ability of consumers to exercise choices about how their information is collected and used, and ensure that businesses take privacy-protective measures as they develop and implement

---

Commission, *The FTC's Regulatory Reform Program: Twenty Years of Systematic Retrospective Rule Reviews & New Prospective Initiatives to Increase Public Participation and Reduce Burdens on Business*, Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce, 112th Cong., July 7, 2011, *available at* http://www.ftc.gov/os/testimony/110707regreview.pdf; Notice Announcing Ten-Year Regulatory Review Schedule and Review of the Federal Trade Commission's Regulatory Review Program (July 7, 2011), *available at* http://www.ftc.gov/os/fedreg/2011/07/110707regulatoryreviewfrn.pdf. More information about the Commission's efforts can be found on the Regulatory Review web page, http://www.ftc.gov/ftc/regreview/index.shtml.

[26] *See generally* COPPA Rulemaking and Rule Reviews web page, business.ftc.gov/documents/coppa-rulemaking-and-rule-reviews.

[27] *See generally* FTC Exploring Privacy web page, www.ftc.gov/bcp/workshops/privacyroundtables.

systems that involve consumer information.[28] At the same time, the roundtable commenters and participants urged regulators to be cautious about restricting the exchange and use of consumer data in order to preserve the substantial consumer benefits made possible through the flow of information.

Staff issued a preliminary privacy report in December 2010 ("Staff Report"),[29] which discusses the major themes that emerged from these roundtables, including the ubiquitous collection and use of consumer data; the extent to which consumers are able to understand and to make informed choices about the collection and use of their data; the importance of privacy to many consumers; the significant benefits enabled by the increasing flow of information; and the blurring of the distinction between personally identifiable information and supposedly anonymous or de-identified information.[30] The Staff Report proposed a new framework to guide policymakers and industry as they consider further steps to improve consumer privacy

---

[28] *See generally 3rd Roundtable, Panel 4: Lessons Learned and Looking Forward* at 242, *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_March2010_Transcript.pdf (industry and consumer representatives suggesting the need to simplify consumer choice and improve transparency); *Written Comment of Centre for Information Policy & Leadership at Hunton & Williams LLP*, cmt. #544506-00059, *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf (industry group comment on improving transparency, choice, and accountability on privacy); Leslie Harris, *Written Comment of Center for Democracy & Technology*, cmt. #544506-00067, *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00067.pdf (urging companies to adopt privacy by design).

[29] *See A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. Commissioners Kovacic and Rosch issued concurring statements available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf at Appendix D and Appendix E, respectively.

[30] *Id.* at 22-38.

protection.

A. The Proposed Framework

The proposed framework included three main concepts. First, FTC staff proposed that companies should adopt a "privacy by design" approach by building privacy protections into their everyday business practices. Such protections include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer in use, and implementing reasonable procedures to promote data accuracy. The Staff Report also urges companies to implement and to enforce procedurally sound privacy practices throughout their organizations, including, for example, assigning personnel to oversee privacy issues, training employees on privacy issues, and conducting privacy reviews when developing new products and services. Such concepts are not new, but the Staff Report indicated that the time has come for industry to implement them systematically. Implementation can be scaled, however, to each company's business operations. For example, the Staff Report recommended that companies that collect and use small amounts of nonsensitive consumer data should not have to devote the same level of resources to implementing privacy programs as companies that collect vast amounts of consumer data or data of a sensitive nature.

Second, the FTC staff proposed that companies provide simpler and more streamlined choices to consumers about their data practices. Under this approach, consumer choice would not be necessary for a limited set of "commonly accepted" data practices, thus allowing clearer, more meaningful choice with respect to practices of greater concern. This component of the proposed framework is premised on the notion that consumers reasonably expect companies to engage in certain practices, such as product and service fulfillment, internal operations such as

assessing the quality of services offered, fraud prevention, legal compliance, and first-party marketing. Some of these practices, such as a retailer's collection of a consumer's address solely to deliver a product the consumer ordered, are obvious from the context of the transaction, and therefore, consumers' consent to them can be inferred. Others are sufficiently accepted or necessary for public policy reasons that companies need not request consent to engage in them. The Staff Report suggested that by clarifying those practices for which consumer consent is unnecessary, companies will be able to streamline their communications with consumers, which will reduce the burden and confusion on consumers and businesses alike.

For data practices that are not "commonly accepted," the Staff Report proposed that consumers should have the ability to make informed and meaningful choices. To be most effective, choices should be clearly and concisely described and offered at a time and in a context in which the consumer is making a decision about his or her data. Depending upon the particular business model, this may entail a "just-in-time" approach, in which the company seeks consent at the point a consumer enters his personal data or before he accepts a product or service. One way to facilitate consumer choice is to provide it in a uniform and comprehensive way. Such an approach has been proposed for behavioral advertising, whereby consumers would be able to choose whether to allow the collection and use of data regarding their online searching and browsing activities. This idea – often referred to as "Do Not Track" – is discussed further below.

Third, the Staff Report proposed a number of measures that companies should take to make their data practices more transparent to consumers. For instance, in addition to providing the contextual disclosures described above, companies should improve their privacy notices so that consumers, advocacy groups, regulators, and others can compare data practices and choices

across companies, thus promoting competition among companies. The Staff Report also proposed providing consumers with reasonable access to the data that companies maintain about them, particularly for non-consumer-facing entities such as data brokers. Because of the significant costs associated with access, the Staff Report noted that the extent of access should be proportional to both the sensitivity of the data and its intended use. In addition, the Staff Report stated that companies must provide prominent disclosures and obtain affirmative consent before using data in a materially different manner than claimed when the data was collected.

Finally, the Staff Report proposed that stakeholders undertake a broad effort to educate consumers about commercial data practices and the choices available to them. Increasing consumer understanding of the commercial collection and use of their information is important to both empowering consumers to make informed choices regarding their privacy and facilitating competition on privacy across companies. In addition to proposing these broad principles, the staff sought comment from all interested parties to help guide further development and refinement of the proposed framework. Close to 450 comments were received and the staff expects to issue a final report this year.

B. Do Not Track

As noted above, the Staff Report included a recommendation to implement Do Not Track – a universal, one-stop choice mechanism for online behavioral tracking, including behavioral advertising.[31] Following the release of the Staff Report, the Commission has testified that any

[31] Commissioner Kovacic believes that the endorsement of a Do Not Track mechanism by staff (in the report) and the Commission (in this testimony) is premature. His concerns about the Commission Staff Report are set forth in his statement on the report. *See* FTC Staff Report, *supra* note 29, at App. D. Commissioner Rosch supported a Do Not Track mechanism only if it were "technically feasible" and implemented in a fashion that provides informed consumer choice regarding all the attributes of such a mechanism. *Id.* at App. E. Commissioner Rosch

Do Not Track system should include certain attributes.[32] First, any Do Not Track system should be implemented universally, so that consumers do not have to repeatedly opt out of tracking on different sites. Second, the choice mechanism should be easy to find, easy to understand, and easy to use. Third, any choices offered should be persistent and should not be deleted if, for example, consumers clear their cookies or update their browsers. Fourth, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes. Finally, an effective Do Not Track system would go beyond simply opting consumers out of receiving targeted advertisements; it would opt them out of collection of behavioral data for all purposes other than product and service fulfillment and other commonly accepted practices.[33]

Of course, any Do Not Track system should not undermine the benefits that online behavioral advertising has to offer, by funding online content and services and providing personalized advertisements that many consumers value. For this reason, any Do Not Track mechanism should be flexible. For example, it should allow companies to explain the benefits of

---

believes that a variety of issues need to be addressed prior to the endorsement of any particular Do Not Track mechanism. *See* Rosch Statement, *supra* note 1.

[32] *See, e.g.*, Prepared Statement of the Federal Trade Commission, *The State of Online Consumer Privacy*, Before the S. Comm. on Commerce, Science and Transportation, 112th Cong., Mar. 16, 2011, *available at* http://www.ftc.gov/os/testimony/110316consumerprivacysenate.pdf; Prepared Statement of the Federal Trade Commission, *Do Not Track*, Before the Subcomm. on Commerce, Trade and Consumer Protection of the H. Comm. on Energy and Commerce, 111th Cong., Dec. 2, 2010, *available at* www.ftc.gov/os/testimony/101202donottrack.pdf (hereinafter "Do Not Track Testimony").

[33] As noted in prior Commission testimony, such a mechanism should be different from the Do Not Call program in that it should not require the creation of a "Registry" of unique identifiers, which could itself cause privacy concerns. *See* Do Not Track Testimony, *supra* note 32.

tracking and to take the opportunity to convince consumers not to opt out of tracking. Further, a Do Not Track system could include an option that enables consumers to control the types of advertising they want to receive and the types of data they are willing to have collected about them, in addition to providing the option to opt out completely.[34]

Industry appears to be receptive to the demand for simple choices. Within the last six months, three of the major browsers offered by Mozilla, Microsoft, and Apple, announced the development of new choice mechanisms for online behavioral advertising that seek to provide increased transparency, greater consumer control and improved ease of use. Recently, Mozilla introduced a version of its browser that enables Do Not Track for mobile web browsing. In addition, an industry coalition of media and marketing associations, the Digital Advertising Alliance, has continued to make progress on implementation of its improved disclosure and consumer choice mechanism offered through a behavioral advertising icon.

VI. Conclusion

The Commission is committed to protecting consumers' privacy and security – both online and offline. We look forward to continuing to work with Congress on these critical issues.

---

[34] For example, use of a Do Not Track browser header would enable consumer customization. The browser could send the header to some sites and not others. Moreover, a particular site could ignore the header to the extent the user has consented to tracking on that site.

Mrs. BONO MACK. Thank you, Commissioner.

And the chair is now pleased to recognize Chairman Genachowski for his 5 minutes.

STATEMENT OF JULIUS GENACHOWSKI

Mr. GENACHOWSKI. Thank you to the chairs and ranking members for holding this important joint hearing.

The right to privacy is a fundamental American value, and the Federal Communications Commission has worked to implement congressional laws that protect the privacy of consumers when they use communications networks. The Internet and other new forms of communications raise new and difficult privacy challenges, particularly when it comes to children. The FCC is committed to working with Congress, the Federal Trade Commission, the Department of Commerce, and our colleagues across government as well as industry and all external stakeholders to tackle these issues.

To understand the importance of privacy challenges in the digital age, one must appreciate the extraordinary opportunities created by broadband Internet services. High-speed Internet, fixed and mobile, is an indispensible platform for innovation and economic growth, for our global competitiveness and opportunities to transform education, healthcare, energy, and public safety. To fully realize the benefits of broadband, people need to trust that the Internet and all communications networks are safe and secure.

As our National Broadband Plan found, privacy concerns are a barrier to broadband adoption. When people and small businesses fear that new technology puts their privacy at risk, they are less likely to use those new technologies. Consider location-based services. McKinsey estimates that this growing sector will deliver $700 billion in value to consumers and businesses over the next decade.

Two weeks ago, the FCC, with the participation of the FTC, hosted a workshop on location-based services, which identified consumer concerns about the use and security of their location information as something that must be addressed to seize the economic and other benefits of this new technology.

In general in this area, we need to strike a smart balance, ensuring that private information is fully protected, and at the same time ensuring a climate that encourages new investment and new innovation that will create jobs and improve our quality of life.

At the FCC, our approach to privacy centers on three overarching goals: consumer control and choice, meaningful transparency about privacy practices, and data security. The Communications Act charges the FCC with implementing a number of privacy protection provisions. Sections 222, 338, and 631 give the FCC authority to protect the privacy and security of the network-related data of telephone, cable, and satellite subscribers. The FCC is also working to educate consumers and small businesses about privacy and data security. For example, we recently released a cybersecurity tip sheet to help small businesses understand and implement basic precautions to secure their networks and data with which we have partnered with both the Chamber of Commerce, the National Urban League, and others to distribute.

To make sure consumers are getting consistent and clear information and guidance from government agencies, we have partnered

with the Federal Trade Commission, the Commerce Department, and the Small Business Administration on a number of education efforts like Net Cetera and OnGuard Online, which offer advice on how to protect children's personal information and guard against identity theft. These education efforts are part of an established track record of effective coordination between the FCC, the FTC, and other agencies.

Now, technology can and must be part of the solution. I continue to encourage industry to take this very seriously, to use its expertise to empower consumers, provide transparency, and protect data. And as the government's expert agency on broadband and communications networks with a long history of taking commonsense steps to protect consumer privacy, the FCC has an important role to play going forward. Our network-focused privacy and data security rules are settled and legally tested. Some updating of the Communications Act network-oriented privacy regime is appropriate for the digital age. This can be done harmoniously with other agencies' implementation of any generally applicable consumer privacy or data security legislation.

We look forward to working with Congress, with my colleagues here at the table and elsewhere, and with all stakeholders outside of government to harness technology to promote innovation, job creation, and economic growth, while protecting fundamentally important principles of privacy.

Thank you again for the opportunity to testify and I look forward to your questions.

[The prepared statement of Mr. Genachowski follows:]

Statement of Chairman Julius Genachowski

Federal Communications Commission

Hearing on "Internet Privacy: The Views of the FTC, the FCC and NTIA"

Before the Subcommittee on Commerce, Manufacturing, and Trade and the Subcommittee on Communications and Technology

U.S. House of Representatives

July 14, 2011

Chairman Bono-Mack, Chairman Walden, Ranking Members Eshoo and Butterfield, Members of both subcommittees, thank you for this opportunity to discuss the issue of Internet privacy.

The right to privacy is a core American value, and the Federal Communications Commission, at the direction of Congress, has worked for years to implement laws that protect the privacy of consumers when they use communications networks and services.

The Internet, which has enabled information sharing on an unprecedented scale, raises new privacy challenges. The FCC is committed to working with Congress, the Federal Trade Commission, the Department of Commerce, and our other colleagues across the government to tackle these issues.

To understand the importance of privacy challenges in the digital age, one must appreciate the extraordinary opportunities created by broadband Internet services. High-speed Internet is an indispensible platform for innovation and economic growth, creating 2.6 new jobs for every job lost according to a recent study. The U.S. captures more than 40 percent of global Internet revenues, making broadband essential to American job creation, as well as our global competitiveness. And broadband has unlocked new opportunities to transform health care, education, energy, and public safety.

To fully realize the benefits of broadband people need to trust that the Internet is safe and secure.

Privacy concerns are a barrier to broadband adoption. When people fear that new technology puts their privacy at risk, they're less likely to use those new technologies. This was one of the important findings of the FCC's National Broadband Plan, in connection with data showing that one-third of Americans aren't online.

Consider cloud computing – a $68 billion global industry that's growing 17% annually, with enormous opportunities to generate job creation and consumer benefits. Trust is essential to the growth of this promising industry and also the broader economy.

If small businesses don't trust the Internet and consequently don't take advantage of cloud-based opportunities to reach new customers and lower costs, that's a lost opportunity for our economy.

Location-based services similarly offer large economic and consumer benefits. McKinsey estimates that this growing sector will deliver $700 billion in value to consumers and business users over the next decade, and businesses that use geo-location technologies are already creating hundreds of jobs a month.

The new opportunities presented by location-based technologies also extend to areas like public safety. And indeed, the FCC is working on an initiative to improve the location accuracy of mobile 911 calls.

Two weeks ago, the FCC, with the participation of the FTC, hosted a workshop on helping consumers harness the potential of location-based services while protecting basic ideals of consumer choice. The discussions at the workshop highlighted the fact that consumers and businesses alike are upbeat on the many opportunities created by location-based services. Stakeholders also recognize the importance of addressing privacy questions, both to protect basic privacy values, and so that consumer concerns about the use and security of their location information do not slow the adoption of innovative services or undermine the opportunities.

It is clear we need to strike a balance – ensuring that personal information and consumer choice is protected, and at the same time ensuring a climate that encourages new investment and new innovations that will create jobs and improve our quality of life.

At the FCC, our approach to privacy centers on three overarching goals: 1) Consumer control and choice; 2) Business transparency about privacy practices, and 3) Data security.

Congress has long recognized that protecting privacy is fundamental to a healthy communications landscape. Congress has also long recognized that, as the nation's expert agency on our communications networks and infrastructure, the FCC has an important role to play in protecting the privacy of consumers using our nation's communications networks.

The Communications Act charges the FCC with implementing a number of privacy protection provisions. Section 222, for example, requires telecommunications carriers to safeguard information about whom consumers communicate with, the length of time they spend using the network, and their location when they use wired or wireless services – what we call customer proprietary network information, or CPNI.

The FCC has adopted rules regarding the handling, use, and sharing of CPNI and vigorously enforces those rules. In the last six months, the Commission issued an Enforcement Advisory, reminding companies of their CPNI obligations, and we have issued 28 Notices of Apparent Liability and warnings for CPNI violations under Section 222.

Through our rulemakings and enforcement, the FCC has addressed difficult issues such as when opt-in and opt-out notifications are appropriate, minimum notice standards, data sharing rules, reasonable data security measures, and notification to law enforcement and consumers in the event of data breaches.

Sections 338 and 631 of the Communications Act require satellite and cable providers to give subscribers clear and conspicuous notice and choice about the collection and use of their personally identifiable information such as name plus address, financial account information, and Social Security number. Those sections of the Communications Act also provide consumers with legal remedies if their personal information is improperly collected, used or disclosed.

At the FCC, we recognize that educating consumers and small businesses about privacy and data security can provide substantial benefits. For example, we want to get the message out to consumers that they need to secure their home Wi-Fi networks, so we've developed an online guide on how to activate the encryption features on wireless routers. Two months ago, the FCC released a cybersecurity tip sheet to help small businesses understand and implement basic precautions to secure their networks and data. We have partnered with the U.S. Chamber of Commerce, the National Urban League and others to develop and distribute this tip sheet and other educational resources.

We have also worked collaboratively with other agencies to educate consumers, making sure they are getting the same clear information and guidance from government agencies like the FCC, the FTC, the Small Business Administration, and the Department of Commerce.

The Small Business Administration was a partner in our small business cybersecurity initiative. We've partnered with the FTC on education efforts like Net Cetera and OnGuard Online, which offer consumers advice on how to protect their children's personal information, guard against identity theft, and avoid email and phishing scams. The FCC also is a member of the National Initiative for Cybersecurity Education partnership led by the Department of Commerce.

Our collaborative efforts extend beyond education.

The FCC and FTC jointly implemented and enforce the "Do-Not-Call" rules. Since 2009, the FCC has issued nearly 150 warning citations and other enforcement actions for Do-Not-Call violations. We have also worked with the FTC in implementing the CAN-SPAM Act to prevent unwanted commercial email messages from being sent to consumers' wireless accounts.

As we tackle privacy issues, it's worth keeping in mind three points about technology that are virtually always true. Technological advances bring great benefits for our economy and consumers. The same technological advances can bring new dangers and challenges. And technology can help address those dangers and challenges.

This is all true of the area we discuss today. Technology can and must be part of the solution. I continue to encourage industry to use its expertise to empower consumers, provide transparency, and protect data.

Many companies are already doing so. For example, in connection with mapping and navigation services offered by wireless providers, in most instances, the first time a consumer uses such a service, he or she sees a pop- up notice asking consent to the collection and use of location information. Providing that kind of timely information and choice to consumers creates a climate of informed trust, which encourages consumer adoption of new products and services, and furthers innovation and economic growth.

To conclude, broadband and the new technologies and services it makes possible are creating incredible opportunities that spur our economy and improve our quality of life. Seizing these opportunities will require us to tackle emerging privacy challenges. As the government's expert agency on broadband and communications networks, with a long history of taking common-sense steps to protect consumer privacy, the FCC has an important role going forward. Our network-focused privacy and data security rules are sound, settled, and legally tested. Some updating of the Communications Act's network-oriented privacy regime is appropriate for the digital age. But that can be done harmoniously with other agencies' implementation of any generally applicable consumer privacy or data security legislation.

We look forward to working with Congress, with my colleagues here at the table and elsewhere, and with all stakeholders outside of government to harness technology to promote innovation, job creation and economic growth, while protecting basic principles of privacy.

Thank you again for this opportunity to testify. I look forward to your questions.

Mrs. BONO MACK. Thank you.
Secretary Strickling, you are recognized for 5 minutes.

STATEMENT OF LAWRENCE E. STRICKLING

Mr. STRICKLING. Chairwoman Bono Mack, Chairman Walden, Ranking Members Butterfield and Eshoo, thank you very much for holding today's hearing and inviting the participation of NTIA. I am also glad to be here with my colleagues Chairman Genachowski and Commissioner Ramirez. All of share a strong commitment to protecting consumers and promoting economic growth.

For the past 2 years, NTIA has been hard at work as part of the Commerce Secretary Locke's Internet Policy Taskforce to conduct a broad assessment of how well our current consumer data privacy framework is serving consumers, businesses, and other participants in the Internet economy. To guide our work, we have focused on two key principles: the first—and you have heard them from the other witnesses this morning—is the idea of trust. It is imperative for the sustainability and continued growth and innovation of the Internet that we preserve the trust of all actors on the Internet, and nowhere is this clearer than in the context of consumer privacy.

Our second key principle is that we want to encourage multi-stakeholder processes to address these key policy issues. We want all stakeholders to come together to deal with these issues in ways that allow for flexibility, speed, and efficiency. We want to avoid the delay, rigidity, and lack of quick response often associated with more traditional regulatory processes.

Last December, the Department issued a "green paper" on consumer data privacy, which offered a set of 10 policy recommendations and asked for public input on a series of additional questions. In this document, we proposed a three-part framework for consumer data privacy. First, we called for the establishment of baseline consumer data privacy protections that are flexible, comprehensive, and enforceable by the Federal Trade Commission. We refer to this baseline as a consumer privacy bill of rights. This set of basic principles would provide clear privacy protections for personal data in which Federal privacy laws that exist today do not apply or offer inadequate protection.

Second, to flesh out the principles into more specific rules of behavior, we recommended that we rely on stakeholders in the industry working with civil society and others to develop enforceable codes of conduct through a multi-stakeholder process. In our proposal, these codes would implement the basic consumer protections, but their adoption would be voluntary.

And third, we recommended strengthening the FTC's consumer data privacy enforcement authority. I believe our approach should welcome and attract bipartisan support. It is neither traditional top-down regulation, nor is it self-regulation. I think to use the word that Vice Chair Terry used in his opening remarks, it provides a real balance between consumer protection and meeting the needs of industry to continue to grow and innovate.

In March of this year, after engaging further with a wide array of stakeholders, the administration announced its support for legislation that would help better protect consumer data privacy in the

digital age by establishing the baseline protections consumers need in legislation. And a broad array of stakeholders—including many businesses—have expressed support for this approach. Specifically, this legislation would provide consumers with more consistent privacy protections, thereby strengthening trust, and preserving the Internet as an engine of economic growth and innovation. Legislation would also provide businesses with a common set of ground rules and would put the United States in a stronger position to work toward reducing international barriers to trade in the free flow of information.

Our recommendations for this baseline are based on a comprehensive set of fair information practice principles. In our "green paper," we drew from existing statements of FIPS as the starting point for principles that should apply in this new commercial context. And as we develop a more definitive administration position, we are now examining how these principles would apply to the interactive and interconnected world of today.

The Department is also continuing to work with others in the Federal Government to develop the administration policy on data security. Without sufficient data security, there cannot be effective data privacy. And in May, the administration submitted a legislative proposal to improve cybersecurity, which includes proposals to strengthen consumer protection in the case of data breaches. The administration proposal would help businesses by simplifying and standardizing the existing patchwork of state laws with a single clear nationwide requirement and would help ensure that consumers receive notification when appropriate standards are met.

I want to thank you again for holding today's hearing and for the two subcommittees' commitment to addressing consumer data privacy issues. Working together, we can protect consumers in the digital age, as well as help businesses expand globally by reducing barriers to trade in international commerce.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Strickling follows:]

Testimony of Lawrence E. Strickling

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

Hearing on Internet Privacy:
The Views of the FTC, the FCC, and NTIA

Subcommittee on Commerce, Manufacturing, and Trade and
Subcommittee on Communications and Technology
Committee on Energy and Commerce
United States House of Representatives

July 14, 2011

I. Introduction.

Chairman Walden, Chairman Bono Mack, Ranking Members Eshoo and Butterfield, and distinguished Committee Members, thank you for the opportunity to testify about the important issue of online privacy. As the principal advisor to the President on communications and information policy, the National Telecommunications and Information Administration (NTIA) within the Department of Commerce ("Department" or "Commerce") has been working over the last two years with Secretary Locke's Internet Policy Task Force and colleagues throughout the Executive Branch to conduct a broad assessment of how well our current consumer data privacy policy framework serves consumers, businesses, and other participants in the Internet economy. I welcome the opportunity to discuss how we can better protect consumer data privacy in the Digital Age. I am pleased to testify here today with Commissioner Edith Ramirez of the Federal Trade Commission (FTC) and Chairman Julius Genachowski of the Federal Communications Commission (FCC).

In March of this year, the Administration announced its support for legislation that would create baseline consumer data privacy protections through a "consumer privacy bill of rights."[1] A guiding principle behind our recommendation is that the requirements in legislation should be general, flexible, actionable on their own, and focus on implementation through options outside the traditional regulatory sphere. We urged Congress to consider legislation that would establish these rights and obligations; to create incentives for the private sector to develop legally-enforceable, industry-specific codes of conduct that can address emerging privacy issues while providing companies some assurance that they are in compliance with the law; and to grant the FTC sufficient authority to enforce the law. My testimony today has three purposes. First, I will highlight the reasons that the Administration views consumer data privacy as an essential element of promoting growth and innovation on the Internet. Second, I will explain how the main elements of the Administration's legislative approach—a consumer privacy bill of rights that is comprehensive but flexible, enforceable codes of conduct developed through a multi-stakeholder process, and clearer FTC enforcement authority—would help to address these issues. Third and finally, I will provide an overview of the Administration's next steps on consumer data privacy here and internationally.

---

[1] Statement of Lawrence E. Strickling, Assistant Secretary for Communications and Information, before the Committee on Commerce, Science, and Transportation, United States Senate, Mar. 16, 2011, http://www.ntia.doc.gov/presentations/2011/Strickling_Senate_Privacy_Testimony_03162011.html.

II. The Need to Strengthen Our Consumer Data Privacy Framework.

Strengthening consumer data privacy protections is integral to the Administration's Internet policy agenda. The Internet economy has sparked tremendous innovation, and the Internet is an essential platform for economic growth, domestically and globally. Consumer data privacy is one of the core issues identified by the Commerce Department's Internet Policy Task Force, convened by Secretary Gary Locke to examine how well U.S. policies on privacy, cybersecurity, copyright protection, and the free flow of information serve consumers, businesses, and other participants in the Internet economy.[2]

A. Privacy Harms to Consumers and Risks to Internet Commerce

Americans deeply value privacy. The value of privacy includes the assertion of a broad "right to be let alone"[3] as well as a right to control personal information.[4] The United States protects privacy in the commercial arena through flexible, adaptable common law and State consumer protection statutes; sector-specific Federal data privacy laws; strong FTC enforcement; open and accountable government; and active policy development efforts that draw on the insights of many stakeholders.

Privacy is also a key requirement for sustaining consumer trust, which is critical to realizing the Internet's full potential for innovation and economic, political, and social development. When consumers provide personal data to a company, they do so in the context of a relationship based on their expectations about how the company will use and disclose the data that it collects. Consumers legitimately expect that companies will use personal data in ways that are consistent with these relationships. Many businesses also recognize that protecting their customers' privacy is critical to maintaining their trust and keeping their business. Many Internet businesses have worked with the FTC and privacy advocates to develop strong privacy

---

[2] U.S. Dept. of Commerce, Commerce Secretary Locke Announces Public Review of Privacy Policy and Innovation in the Internet Economy, Launches Internet Policy Task Force, Apr. 21, 2010, http://www.commerce.gov/print/news/press-releases/2010/04/21/commerce-secretary-locke-announces-public-review-privacy-policy-and-i.

[3] Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 HARVARD LAW REVIEW 193 (1890).

[4] *See* U.S. Dept. of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, at 10 (2010), http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

practices.[5] We are seeking to encourage this practice to spread more broadly and cover businesses that are not exposed to the same degree of customer scrutiny as the leading Internet companies.

In addition, consumers experience a variety of harms when their privacy expectations are violated. There is considerable evidence that U.S. consumers are increasingly uneasy with and unsure about how data about their activities is collected, stored, and used.[6] Web tracking, location tracking, and the exchange of individual-level profiles are all sources of this unease and may feed a reluctance to adopt new applications, services, and devices. The loss of sensitive personal information through security breaches – which can result in identity theft and other harms that cause financial loss, ruin credit, and severely disrupt individuals' lives – also illustrates some of the potential harms that consumer data privacy protections can address.

Many of these uses of personal data fall between gaps among existing Federal privacy laws, leaving companies and consumers without a clear sense of what standards apply to personal data collection, use, and disclosure. The technical and organizational complexity of the digital economy poses steep challenges to individual consumers who want to understand and manage the uses of their personal data, even if they are technically adept. The lengthy, dense, and legalistic privacy policies that many companies post do not appear to be effective in informing consumers of their online privacy choices. Surveys show that most Americans incorrectly believe that a website that has an online privacy policy is prohibited from selling personal information it collects from customers.[7] In addition, many consumers believe that having a privacy policy guarantees strong privacy rights.[8] Moreover, a website's own privacy policy typically does not apply to the potentially numerous third parties that collect information through that site.[9] In other words, to fully understand the privacy implications of using a

---

[5] *See id.* at 15 (discussing the importance of consumer trust in comments on the Department of Commerce's Notice of Inquiry on consumer data privacy and innovation).

[6] According to a recent survey, 83% of adults say they are "more concerned about online privacy than they were five years ago." Common Sense Media, Online Privacy: What Does It Mean to Parents and Kids (2010), *available at* http://www.commonsensemedia.org/sites/default/files/privacypoll.pdf (last visited July 6, 2011).

[7] Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathaniel Good & Jens Grossklags, *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: JOURNAL OF LAW & POLICY 723 (2007), *available at* http://www.is-journal.org/.

[8] Chris Jay Hoofnagle & Jennifer King, Research Report: What Californians Understand About Privacy Offline (2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075.

[9] For example, a *Wall Street Journal* investigation found that "the top 50 US. websites installed an average of 64 tracking tools on visitors' computers. Of those files, an average of 44 were installed by outside companies, primarily advertisers and marketers that track consumer behavior across the Internet." Julia Angwin and Scott Thurn, *Privacy*

particular site, individuals will often have to begin by considering the privacy policies of many other entities that could gain access to data about them.

B. Stakeholder Input Into Our Consumer Data Privacy Framework

The Commerce Internet Policy Task Force has engaged with a broad array of stakeholders, including companies, consumer advocates, academic privacy experts, and other government agencies. Our work produced the Task Force's "Green Paper" on consumer data privacy in the Internet economy, released on December 16, 2010.[10] The privacy Green Paper made ten separate recommendations on how to strengthen consumer data privacy protections while also promoting innovation, but it also brought to light many additional questions.

The comments we received on the privacy Green Paper from businesses, academics, and advocates informed our conclusion that the U.S. consumer data privacy framework would benefit from legislation that establishes a clearer set of rules for businesses and consumers, while preserving the innovation and free flow of information that are hallmarks of the Internet. This conclusion reflects two tenets. First, to harness the full power of the Internet, we need to establish norms and ground rules for uses of information that allow for innovation and economic growth while respecting consumers' legitimate privacy interests. Consumer groups, industry, and leading privacy scholars agree that a large percentage of Americans do not fully understand and appreciate what information is being collected about them, and how they are able to stop certain practices from taking place.[11] Second, as we go about establishing these privacy guidelines, we also need to be careful to avoid creating an overly complicated regulatory environment.[12]

Defense Mounted: Website Operators Say It Isn't Possible to Keep Track of All Tracking Tools, WALL ST. JOURNAL, Oct. 8, 2010.

[10] Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, Dec. 16, 2010, http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

[11] All comments that the Department received in response to the Green Paper are available at http://www.ntia.doc.gov/comments/101214614-0614-01/.

[12] For industry comments in support of legislation, *see, e.g.*, Intel Comment at 3 ("We disagree with the arguments some have advocated against the adoption of legislation, particularly that privacy legislation would stifle innovation and would hinder the growth of new technologies by small businesses. Instead, we believe that well-crafted legislation can actually enable small business e-commerce growth."); Google Comment at 2 (supporting "the development of a comprehensive privacy framework for commercial actors . . . that create[s] a baseline for privacy regulation that is flexible, scalable, and proportional"). For consumer groups and civil liberties' organizations comments in support of legislation, *see, e.g.*, Center for Democracy and Technology, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 2 ("CDT has long argued and continues to believe that the only way to implement a commercial data privacy framework that fully and effectively incorporates all the Fair Information Practice Principles is through baseline privacy legislation."); Center for Digital Democracy and USPIRG, Comment on Department of Commerce Privacy Green Paper, at 21 ("[W]e urge the adoption of

III. Strengthening Our Consumer Data Privacy Framework Through Baseline Protections.

To achieve the goals of promoting broader adoption of strong privacy in the commercial context and promoting an environment that encourages innovation, the Administration has recommended legislation with three main characteristics. First, it should establish baseline consumer data privacy protections that would apply in commercial contexts. Existing Federal privacy laws apply to some kinds of personal data in specific sectors, such as healthcare, financial services, and education; but they do not apply to much of the personal data that traverses the Internet. The protections in a baseline consumer data privacy law should be flexible, enforceable at law, and serve as the basis for both enforcement and development of enforceable codes of conduct that specify how the legislative principles apply in specific business contexts. Second, we have recommended that legislation provides appropriate incentives for stakeholders in the private sector to develop and adopt enforceable codes of conduct through a multi-stakeholder process. In our proposal, these codes would implement the baseline requirements of legislation in terms that make sense for a specific industry; but their adoption would be voluntary. Third, the Administration supports legislation that strengthens the FTC's consumer data privacy enforcement authority.

A. Enacting a Consumer Privacy Bill of Rights.

The Administration recommended that statutory baseline protections for consumer data privacy be enforceable by the FTC and based on a comprehensive set of Fair Information Practice Principles (FIPPs). In the Department of Commerce Green Paper, we drew from existing statements of FIPPs as a starting point for principles that should apply in the commercial context, in particular the original principles developed by the Department of Health, Education &

---

regulations that will ensure that consumer privacy online is protected. The foundation for such protection should be the implementation of Fair Information Practices for the digital marketing environment."); Consumers Union, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 2 ("Consumers Union supports the adoption of a privacy framework that will protect consumer data both online and offline. ... CU believes this comprehensive privacy framework should be grounded in statute ...."); Privacy Rights Clearinghouse, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 2 ("[N]oting that consumer trust is pivotal to commercial success online, and that it has diminished with industry self-regulatory practices, PRC advocates comprehensive federal FIPPs-based data privacy legislation.").

Welfare in 1973[13] and elaborations developed by the Organisation for Economic Co-operation and Development (OECD).[14] As we are developing in the Administration's forthcoming privacy White Paper, we seek to adapt these principles to the interactive and interconnected world of today in obligations that are enforceable against the organizations that collect, use, and disclose personal data. Transparency, security, accuracy, and accountability are fundamental to privacy protection, and the existing statements of FIPPs that we discussed in the Green Paper hold up well in the digital economy. But other dimensions of privacy protection may require a more dynamic and holistic approach. NTIA is working with our colleagues in the Department of Commerce and throughout the Administration to better address the complexity and dynamism of the digital economy while remaining consistent with existing statements of FIPPs.

One important question in this process is whether information technologies can expand individual control over personal information, and how any such capacity should be incorporated as an obligation in baseline consumer data privacy protections. A second area that we are considering was suggested by several commenters on the Commerce Department's Privacy Green Paper, who argued that FIPPs should be applied flexibly and in a manner that is appropriate to the contexts in which consumers use services in the digital economy.[15] We are examining how we might take this notion of context as a guide to applying other established elements of FIPPs principles, such as specifying the purposes for collecting personal data and limiting the uses of personal data to what is accords with those specified purposes in ways that continue to encourage and enable innovation. These are complex issues that are still under active discussion within the Administration. We look forward to working with Congress and

---

[13] *See* U.S. Dept. of Health, Education & Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems,* July 1973, http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

[14] *See* OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[15] *See, e.g.*, Ann Cavoukian, Comment on Department of Commerce Privacy Green Paper, Jan. 27, 2011, at 6 (emphasizing the importance of applying "practical privacy principles to particular contexts"); Centre for Information Policy Leadership, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 3-4 (arguing that FIPPs "should be applied within a contextual framework in which different principles carry more importance depending on the nature of the data, its sensitivity, or how it is used"); Facebook, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 6 ("[A]ny approach to privacy must give due regard to the context in which the information is collected or used, which necessarily shapes users' privacy expectations."); Google, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 6 (arguing that "FIPPs must be flexible enough to take account of the spectrum of identifiability, linkability, and sensitivity of various data in various contexts").

stakeholders to define these protections and enforcement authorities further and enact them into law.

B. Implementing Enforceable Codes of Conduct Developed Through Multi-Stakeholder Processes.

The second main element of the Administration's recommended approach to legislation is the development and adoption of legally enforceable codes of conduct developed through a multi-stakeholder process. The process should permit everyone who has a stake in privacy – companies, consumers, privacy advocates, academics, and others – to work together to take the statutory baseline privacy protections and expand them into legally enforceable best practices or codes of conduct. In such a process, the government is an active participant, a convener that brings together all participants and facilitates discussions, but does not prescribe the outcome. This process should be open to any person or organization that is willing to participate in the hard work of engaging with other stakeholders to resolve any substantive differences fairly and openly.

The Administration believes that a multi-stakeholder process can be flexible and could offer the most effective solution to the challenges posed by a rapidly changing technological, economic, and social environment. This recommendation reflects the Administration's view that government must support policy development processes that are nimble enough to respond quickly to consumer data privacy issues as they emerge and that incorporate the perspectives of all stakeholders to the greatest extent possible. A well-crafted multi-stakeholder process will allow stakeholders to address privacy issues in new technologies and business practices without the need for additional legislation, permit stakeholders to readily reexamine changing consumer expectations, and enable stakeholders to identify privacy risks early in the development of new products and services.

Multi-stakeholder processes can be well suited for illuminating the varying policy concerns inherent in such ideas as security breach notification, data security compliance, and Do-Not-Track. Starting with the commercialization of the Internet, the FTC has used a variety of stakeholder engagements to develop consumer data privacy policies. Its current work on Do-Not-Track carries on this history, and I applaud the leadership of Chairman Leibowitz,[16] as well

[16] *See* Statement of the Federal Trade Commission, before the Committee on Commerce, Science, and Transportation, United States Senate, Mar. 16, 2011, http://www.ftc.gov/os/testimony/110316consumerprivacysenate.pdf.

as Web browser developers, Internet companies, standards organizations, privacy advocates, and others to provide options for greater control over personal information that may be used for online tracking.[17] I encourage advertisers to work expeditiously with other stakeholders to implement Do Not Track capabilities based on the technical capabilities that have been added to Web browsers. The development of safe harbor programs is another task that can be addressed through the multi-stakeholder process recommended in the Commerce Green Paper.

C. Strengthening the FTC's Authority.

Bolstering the FTC's enforcement authority is the third key element of the Administration's proposed framework. In addition to its leadership in contributing to consumer data privacy policy, the FTC plays a vital role as the Nation's independent consumer privacy enforcement authority for non-regulated sectors. Granting the FTC explicit authority to enforce baseline privacy principles would strengthen its role in consumer data privacy policy and enforcement, resulting in better protection for consumers and evolving standards that can adapt to a rapidly evolving online marketplace.

D. Establishing Limiting Principles on Consumer Data Privacy Legislation.

As the Committee considers consumer data privacy legislation, I would like to reiterate the Administration's views on the limitations that Congress should observe in crafting privacy legislation. Legislation should not add duplicative or overly burdensome regulatory requirements to businesses that are already adhering to the principles in baseline consumer data privacy legislation. Legislation should be technology-neutral, so that firms have the flexibility to decide how to comply with its requirements and to adopt business models that are consistent with baseline principles but use personal data in ways that we have not yet contemplated. Furthermore, domestic privacy legislation should provide a basis for greater global cooperation on consumer privacy enforcement issues, as well as more streamlined cross-border data flows and reduced compliance burdens for U.S. businesses facing numerous foreign privacy laws.

IV. The Department of Commerce's Next Steps on Internet Privacy Policy.

A. Engaging with Stakeholders

---

[17] *See, e.g.*, W3C Workshop on Web Tracking and User Privacy, Apr. 28-29, http://www.w3.org/2011/track-privacy/ (collecting position papers and reporting on a workshop discussion of technical and policy approaches to limit web tracking).

As discussion of consumer privacy legislation moves forward, the Department of Commerce will continue to make consumer data privacy on the Internet a top priority. We will convene Internet stakeholders to discuss how best to encourage the development of enforceable codes of conduct, in order to provide greater certainty for businesses and necessary protections for consumers. The past 15 years have shown that self-regulation without government leadership can be sporadic and lack a sense of urgency. The Department received significant stakeholder support for the recommendation that it play a central role in convening stakeholders. A broad array of organizations, including consumer groups, companies, and industry groups, announced their support for the Department to help coordinate outreach to stakeholders to work together on enforceable codes of conduct.[18] This will be led by the National Telecommunications and Information Administration (NTIA) but would involve all relevant Commerce components, just as NTIA supports NIST's efforts to convene stakeholders to discuss privacy issues that may arise in the implementation of the National Strategy for Trusted Identities in Cyberspace (NSTIC),[19] and ITA administers efforts relating to the U.S.-EU Safe Harbor Agreement[20] and (in coordination with the State Department and other Federal agencies) the Asia-Pacific Economic Cooperation's (APEC) Cross-Border Data Privacy Rules.

B. Advancing Data Security

The Department will also continue to work with others in the Federal Government to develop the Administration policy on data security. The Nation's digital infrastructure is fundamental to our economy, critical to our national security and defense, and essential for open and transparent government. In addition, without sufficient data security, there can be no effective data privacy. To address these issues, the Administration in May submitted a legislative proposal to improve cybersecurity. Our proposal covers security breach reporting,

[18] *See, e.g.*, Center for Democracy and Technology, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 15; Consumers Union, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 2-3; Microsoft, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 6; Walmart, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 2; Intel, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 7; Google, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 5; Facebook, Comment to Department Privacy Green Paper, Jan. 28, 2011, on 13; and Yahoo!, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 11.

[19] National Strategy for Trusted Identities in Cyberspace (NSTIC), Apr. 15, 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[20] *See* Export.gov, Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks (last updated Mar. 31, 2011), http://www.export.gov/safeharbor/.

criminal penalties for computer crime, critical infrastructure cybersecurity, protecting Federal Government computers and networks, and protecting individuals' privacy and civil liberties.[21]

I would like to highlight the main elements of the security breach reporting proposal. State laws have helped consumers protect themselves against identity theft while also incentivizing businesses to have better cybersecurity, thus helping to stem the tide of identity theft. These laws require businesses that have suffered an intrusion to notify consumers if the intruder had access to the consumers' personal information. The Administration proposal would help businesses by simplifying and standardizing the existing patchwork of 47 state laws with a single, clear, nationwide requirement, and would help ensure that consumers receive notification, when appropriate standards are met, no matter where they live or where the business operates.

The Administration supports security breach notification legislation that addresses reasonable risks of harm to individuals, covers the types of personal data that are most likely to lead to these harms, and contains strong enforcement provisions. To achieve these ends, the Administration defines a set of "sensitive personally identifiable information" (SPII) to which notification requirements would apply and proposes to give the FTC the authority to add to this list. The reporting threshold in our proposal requires businesses to notify their customers of a breach unless there is no reasonable risk of harm to individuals. Businesses must also provide notice without unreasonable delay, presumed to be 60 days or less, subject to limitations for law enforcement and national security purposes. A "safe harbor" provision would exempt businesses from the reporting requirement when there is no reasonable risk of harm to individuals, as determined by applying criteria that are spelled out in the proposal, though businesses would be required to notify the FTC of their invocation of the safe harbor provision. Finally, the Administration's proposal contains strong enforcement provisions by authorizing the FTC to enforce the proposal's requirements. State Attorneys General are also authorized to bring civil actions in Federal district court, and they may obtain civil penalties through these enforcement actions. The Administration looks forward to working with this Committee and others in Congress on legislation in this area.

As a complement to the Administration's cybersecurity legislative package, the Department of Commerce has been developing a policy framework that is directed at increasing

[21] *See* Statement for the Record of Philip Reitinger, Deputy Under Secretary, National Protection and Programs Directorate, before the Senate Homeland Security and Governmental Affairs Committee: "Protecting Cyberspace: Assessing the White House Proposal", May 23, 2011.

security beyond core critical infrastructure. Last month the Department released a green paper entitled *Cybersecurity, Innovation, and the Internet Economy,* which addresses cybersecurity the dynamic Internet and information technology sectors.[22] We are currently soliciting comments from stakeholders to help us develop this critical strategy, with the goal of improving security at home and around the world so that Internet services can continue to provide a vital connection for trade and commerce, as well as for civic participation and social interaction.

C. Engaging with the Global Commercial Privacy Community

The Department will also support the Administration's efforts to encourage global interoperability by stepping up our engagement in international policymaking bodies. U.S. enterprises continue to incur substantial costs complying with disparate data privacy laws around the world. The need to comply with different privacy laws can lead to compartmentalization of data and privacy practices, can require a significant expenditure of time and resources, and can even prevent market access. Consistent with the National Export Initiative goal of decreasing regulatory barriers to trade and commerce, the Department will work with our allies and trading partners to facilitate cross-border data flows by increasing the global interoperability of privacy frameworks. Privacy laws across the globe are frequently based on similar values and a shared goal of protecting privacy while facilitating global trade and growth. The Department will work with our allies to find practical means of bridging any differences, which are often more a matter of form than substance. Specifically, the Department will work with other agencies to ensure that global privacy interoperability builds on accountability, mutual recognition and reciprocity, and enforcement cooperation principles pioneered in the Organisation for Economic Co-operation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC). The continued development of frameworks for cooperation with other privacy authorities around the world, coordinated with the State Department and other key actors in the Federal Government, could further reduce significant business global compliance costs.

Just two weeks ago, the United States and the 33 other countries that are members of the OECD issued principles for creating policies that will encourage continuing innovation and economic growth through the Internet.[23] One of these principles recognizes that "[s]trong

---

[22] Cybersecurity, Innovation and the Internet Economy, June 11, 2011, http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.

[23] OECD High Level Meeting on the Internet Economy, Communiqué on Principles for Internet Policy-Making, June 28-29, 2011, http://www.oecd.org/dataoecd/40/21/48289796.pdf.

privacy protection is critical to ensuring that the Internet fulfils its full social and economic potential" and calls for strengthening the "consistency and effectiveness in privacy protection at a global level" through mutual recognition of substantively similar privacy laws and increased cross-border enforcement cooperation.[24] The legislative approach in the Administration's overall framework, which preserves the flexibility that is one of the hallmarks of our current privacy framework, could advance the goal of mutual recognition and thus reduce the costs of doing business globally.

In addition, over the past two years, officials from Commerce and other parts of the Executive Branch have met frequently with European privacy officials. While we have much further to go in our discussions with Europe, and much remains uncertain about the final shape of the EU's revised Data Privacy Directive, we see encouraging signs of potential for interoperability from the other side of the Atlantic. U.S. enactment of legislation establishing comprehensive commercial data privacy protections will help to facilitate further development. Strong leadership in this area could form a model for our partners currently examining this issue, and prevent fragmentation of the world's privacy laws and its concomitant increase in compliance costs to our businesses that conduct international trade.

V. Conclusion.

Thank you again for the opportunity to provide our views on policies to protect consumer privacy and promote innovation in the 21st Century. We look forward to working with you, the FTC and other Federal agencies, the Executive Office of the President, and other stakeholders toward enactment of these consumer data privacy protections. I welcome any questions you have for me. Thank you.

[24] *Id.* at 5.

Mrs. BONO MACK. Thank you, Mr. Secretary. And thank you all for your unique insights. And I will recognize myself now for 5 minutes for questions.

And Chairman Genachowski, we have all seen the headlines about the phone hacking scandal in Britain. Are you satisfied that sufficient safeguards are in place to prevent similar privacy breaches here in the U.S., or should Americans be concerned?

And also, as mobile devices become integrated in our daily lives and consumers use them more and more for critical functions like banking, are we going to see an explosion of hacking incidents?

Mr. GENACHOWSKI. There are several laws in place that address hacking issues. There are Federal wiretapping laws that prevent unauthorized hacking. Hacking, I guess, by definition is unauthorized. There are provisions of the Communications Act that criminalize interception of information. There are state laws that prevent it. Any hacking of phones should be investigated. There are criminal provisions and they should be addressed very seriously.

There are also issues around the security of devices themselves. Several years ago, there was an effort to improve the security of phones, including voicemails, for example, by providing for password protection on voicemails. The state of play now is that many carriers automatically provide password protection for voicemails. Others give consumers the choice. There is no question that greater protection can be accomplished by using the password protections, and that is an area that should be looked at.

Mrs. BONO MACK. Thank you.

Commissioner Ramirez, the question of why a privacy regulation is needed is a policy question you must decide. If a regulation is needed, presumably there is harm or consumer injury and the regulation is seeking to prevent. Setting aside data security related to personally identifiable information, or PII, where we know the potential harm of identity theft and other unlawful conduct, what is the harm or consumer injury when we are discussing Internet privacy? Are you aware of specific cases or examples?

Ms. RAMIREZ. What I would say is that the fundamental issue that the FTC is trying to address is the issue that increasingly, information is being used in unexpected ways. Consumers simply do not know how the information that is being collected about them is—number one, what information is being collected, and number two, how that data is being used. So the framework that the staff has proposed in its initial report seeks to balance basic privacy protections for consumers against the needs of the business community. But the fundamental aim is to provide increased information to consumers and choice and control over the information that is being collected about them and how it is being used.

Mrs. BONO MACK. So we have heard from many stakeholders that we really don't know enough about what the average consumer thinks about privacy nor the use of his or her information in exchange for free content. We do know that opt-out rates are low even in those cases where people click through the pages that describe what information is gathered and shared. That is not necessarily conclusive evidence that consumers don't care about their information, but it must mean something. What is the Commission

doing to find out how consumers really feel about privacy and the use of their PII?

Ms. RAMIREZ. Well, we do know from public reports that there is survey after survey that shows that consumers are increasingly concerned about how their information is being used. They are increasingly concerned about privacy. We also know from public reports that there has been outcry by part of the public when certain companies have not provided basic privacy protections for them.

Furthermore, industry itself has recognized that there is a need for increased and greater consumer trust. The Digital Advertising Alliance has conducted a study and they themselves recognize that there is a greater need to have consumers have greater trust in the marketplace in order for the marketplace to continue to flourish and for innovation to be promoted.

Mrs. BONO MACK. The Federal Government hasn't done a study in, what, 10 years? Do you or any of the other agencies have plans to conduct another study soon to gather hard data?

Ms. RAMIREZ. What we have done is that, as the process laying the groundwork for the report that was issued by staff in December of last year, the Agency conducted a series of public roundtables soliciting input from all relevant stakeholders that included industry, consumers, academics, technologists. We have also solicited written comments and received approximately 450 written comments that are currently being analyzed by staff, and the Agency does intend to issue a final report later this year.

Mrs. BONO MACK. I thank the commissioner.

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

Mr. WAXMAN. Thank you very much for recognizing me.

The committee will soon be marking up a data security bill. That markup may involve defining what data must be secured. One approach might include requiring all data to have some minimum level of security if stored in the cloud or as it travels over a dump pipe. Under Section 222 of the Communications Act, customer proprietary network information, CPNI, must be protected. CPNI includes the time, date, duration, and destination number of each call, the type of network a consumer subscribes to, and any other information that appears on the consumer's telephone bill. Under the Cable Act, cable operators are supposed to secure personally identifiable information. Now, that term is not defined.

Under the chair's draft proposal, the term "personal information" means an individual's name or address or phone number in combination with an identifying number such as a Social Security number or driver's license number or financial account number, but only if there is the required security code or password. I agree with Commissioner Ramirez that this is a very narrow definition.

Mr. Strickling, we know what the administration thinks should be covered thanks to its draft proposal, so I won't need to ask you to answer this one, but I am going to run through a long list and I would like to hear from Chairman Genachowski and Commissioner Ramirez to tell me, answering yes or no, should the following types of data be required to be secured?

Whichever one of you—IP address? Mr. Genachowski?

Mr. GENACHOWSKI. Yes. And I think the CPNI rules that we have implemented at the FCC are a very good starting point, but yes.

Mr. WAXMAN. Ms. Ramirez?

Ms. RAMIREZ. Yes.

Mr. WAXMAN. OK. How about any unique persistent identifier such as a customer number, a unique pseudonym or user alias such as a Facebook user name and/or password. Ms. Ramirez?

Ms. RAMIREZ. Yes, it if could be linked to a specific individual or computer or device. Yes.

Mr. GENACHOWSKI. I would agree.

Mr. WAXMAN. How about medical history information, physical or mental condition, and information regarding the provision of healthcare to the individual?

Ms. RAMIREZ. Yes.

Mr. GENACHOWSKI. Yes, I would agree. And these are commonsense things that people would expect should be kept secured.

Mr. WAXMAN. Well, they are not in the bill now, so I am trying to get the record to indicate that you think they ought to be protected.

Race or ethnicity?

Ms. RAMIREZ. Yes.

Mr. GENACHOWSKI. I would assume so.

Mr. WAXMAN. Religious beliefs and affiliation, sexual orientation or sexual behavior, do you agree those ought to be covered?

Ms. RAMIREZ. I do.

Mr. GENACHOWSKI. Yes.

Mr. WAXMAN. Mother's maiden name?

Ms. RAMIREZ. Yes.

Mr. GENACHOWSKI. I would assume so. I haven't thought about that.

Mr. WAXMAN. Well, a lot of Web sites ask for your mother's maiden name.

Income, assets, liabilities, or financial records and other financial information associated with a financial account, including balances and other financial information?

Ms. RAMIREZ. Yes.

Mr. GENACHOWSKI. I agree.

Mr. WAXMAN. Precise geo-location information and any information about the individual's activities and relationships associated with such geo-location?

Ms. RAMIREZ. Yes.

Mr. GENACHOWSKI. Agree.

Mr. WAXMAN. Unique biometric data including a fingerprint or retina scan?

Ms. RAMIREZ. Yes.

Mr. GENACHOWSKI. Agree.

Mr. WAXMAN. Commissioner Ramirez, when you were here a few week ago to testify about the Republican's draft Data Security Bill, you mentioned that the Federal Trade Commission is concerned about the limited scope of personal information that would be subject to the bill's data security and breach notification requirements. In particular, you discussed health information collected from companies not covered by the HIPAA law. I agree that the FTC should

be concerned about this, but I have another concern. It is not clear to me what would happen when the company that is breached can argue that it does not know what type of information was breached.

Recently, we heard of an extensive breach at Dropbox. Dropbox is a popular cloud computing service that allows its 25 million users to store documents and other files on its servers. These users may store innocuous documents like a grocery list or pictures of nature or they may store sensitive information such as an application for a loan or compromising or embarrassing photos. Dropbox could argue that it is in a cloud provider of storage that doesn't know what its users put there and that those users expect it not to go snooping through their files to find out. Shouldn't Dropbox and companies like it be required to have a certain level of data security? And similarly, shouldn't Dropbox and companies like it be required to notify its customers of a breach even if it does not know what data it holds?

Ms. RAMIREZ. I am not in a position to comment on specific practices, but what I will say is that companies should provide reasonable security for personal information and private information of consumers. So depending on the nature of the specific facts and depending on the information that is being stored and the size of the company, a number of other factors, reasonable security measures ought to be provided, yes.

Mr. WAXMAN. Thank you very much.

Thank you, Madam Chair.

Mrs. BONO MACK. I thank the gentleman. And the chair is pleased to recognize Chairman Walden for 5 minutes.

Mr. WALDEN. I thank the chairwoman for that.

And I wonder if I might enter into a colloquy with the former Chairman. Could you just tell us what bill you were referencing? We were trying to figure that out over here.

Mr. WAXMAN. It is a draft that has not been introduced with a number, but we have a markup in the Consumer Affairs Committee next Wednesday, as I understand it.

Mr. WALDEN. OK. I am not on that committee, so we were just curious what it was.

Mr. WAXMAN. Yes. This is a joint hearing of the two subcommittees.

Mr. WALDEN. Right. Understood.

Mr. Strickling, I am kind of interested in some of the things that your colleagues there were able to comment on. Does the administration's position through your NTIA legislation, do you share those same positions as were articulated by the FCC and FTC?

Mr. STRICKLING. The administration put forward in May a proposal for data breach legislation that covered many—I can't say all—of the items that Congressman Waxman listed out for these folks.

Mr. WALDEN. Right.

Mr. STRICKLING. But many of them, such as the unique biometric data, unique account identifiers, those are all within the category of——

Mr. WALDEN. Right.

Mr. STRICKLING [continuing]. Sensitive personal information.

Mr. WALDEN. Were there any that were articulated here that you would disagree with?

Mr. STRICKLING. There might be some I would reserve judgment on but none I would disagree with listening to the list today.

Mr. WALDEN. OK. Thank you.

Chairman Genachowski and Commissioner Ramirez, I am concerned about the uneven competitive playing field given the convergence of communications out there in the marketplace. Do you think it is fair or competitively neutral to apply privacy protections to carriers but not, for example, operating system providers like Apple who have access to exactly the same consumer information?

Mr. GENACHOWSKI. The level playing field is a completely reasonable goal. How to achieve it is obviously a harder question and to the extent that different sectors come from different backgrounds, have different competitive frameworks, the exact regulatory scheme might be different, but at the end of the day, I agree on your principles on technological and competitive neutrality.

Mr. WALDEN. Commissioner?

Ms. RAMIREZ. I also agree that there should be a level playing field. From the FTC's perspective, it is important that consumers be provided with basic privacy protections irrespective of the entity that is providing the service. So the Agency does take the view that if there is legislation, the Agency ought to have jurisdiction over telecom common carriers.

Mr. WALDEN. Chairman Genachowski?

Mr. GENACHOWSKI. Well, there is a longstanding issue here. We disagree with our friends at the Federal Trade Commission on this point.

Mr. WALDEN. I wondered.

Mr. GENACHOWSKI. The FCC brings years of experience and expertise operating under congressional statutes with respect to networks wired and wireless——

Mr. WALDEN. Right.

Mr. GENACHOWSKI [continuing]. And privacy issues around them. That system has worked well. And any revisions to the statutory framework in my strong opinion should continue to recognize and take advantage of this long history of expertise. Now, our two agencies have worked very well together——

Mr. WALDEN. Right.

Mr. GENACHOWSKI [continuing]. Cooperatively and collaboratively.

Mr. WALDEN. I guess I think it is important there is some cop on the beat if you will allow me to use that, so I am kind of curious about the Commission's actions to enforce its CPNI rules and other consumer privacy protections. Can you just elaborate on that process for us?

Mr. GENACHOWSKI. Yes. First of all, there is an ongoing education process making sure that companies are certifying us as to their compliance and on a regular basis, our enforcement bureau issues notices of liabilities when companies are not doing that. Over the years, issues have emerged that the Commission is taking an action on. Some people may remember the pretexting discussion of a number of years ago where it was found that people were pos-

ing in order to gain access to records. The Commission at that point adopted some commonsense rules to make it clear——

Mr. WALDEN. Right.

Mr. GENACHOWSKI [continuing]. That that couldn't happen and to put in place opt-in requirements for third-party efforts to access data.

Mr. WALDEN. Ms. Ramirez?

Ms. RAMIREZ. If I may add, I did want to clarify that I was by no means suggesting that the FCC's role should be displaced here. All I was saying was that we do believe that the FTC has significant enforcement experience that ought to be brought to bear here.

Mr. WALDEN. Got it.

Mr. Strickling, do you want to comment on any of that?

Mr. STRICKLING. I was hoping to stay out of that actually, Mr. Chairman.

Mr. WALDEN. I figured as much. That is why I thought I would ask you to wade on in there.

Mr. STRICKLING. I think what I will say is that the framework we are proposing, which would apply to all of industry, does not intend by the proposal we are making to displace sector-specific regulation if there is a need for that. And I think we could all agree that there are certain industries such as the financial services and healthcare industry where I think additional protections are absolutely justified.

Mr. WALDEN. Indeed. Well, we appreciate your testimony today and working with you as we go forward to deal with this issue that we are all affected by and want to do the right thing on.

Thank you, Madam Chair.

Mrs. BONO MACK. Thank you, Chairman Walden. And recognize now the gentlelady from California, Ms. Eshoo, for 5 minutes.

Ms. ESHOO. Thank you again, Madam Chairwoman.

Thank you to each of you for your testimony and for the work that you have done on this.

I mentioned in my opening statement that we need a unified approach. And while I really respect and appreciate the work that you have been doing, each Agency is taking on what they are taking on. It is the same subject matter but it is very difficult for me to see how this is all stitched together so that there is a comprehensive policy for the country. I think we can draw from the work that you are doing but I think that the Congress really either needs to update some of the laws that are on the books or do something that is overarching that is going to protect innovation but also speak to, what, the second decade of the 21st Century that we are already in. That is what my sense of what I have heard.

To Chairman Genachowski, under current law, does the FCC have authority over ISPs to ensure that the proprietary network information of Internet customers is not being sold to third parties or used for the ISPs on marketing efforts?

Mr. GENACHOWSKI. Well, that is an area where clarification of the Communications Act would be helpful. There is uncertainty and unpredictability about that now. And in thinking about a level playing field, looking at Telco's cable satellite where there is clear jurisdiction of VoIP, telephony, voice-over-Internet telephone service where the FCC has acted as well. This is an area where clari-

fication would be very helpful. And in the absence of it, there is a gap.

Ms. ESHOO. You do need legislative clarification?

Mr. GENACHOWSKI. Yes.

Ms. ESHOO. I hope all the members heard that because there——

Mr. GENACHOWSKI. Legislative clarification would be beneficial——

Ms. ESHOO. OK.

Mr. GENACHOWSKI [continuing]. And would eliminate uncertainty and unpredictability.

Ms. ESHOO. Each word counts. Each word counts.

Help me with this and whomever wants to lean in on this. We are all concerned about children. And I think if there were to be a starting place, you know, I think that we could develop consensus around that because I think consensus already exists on it. Children, no matter what, are always the most vulnerable, no matter what the category is that we speak of. I think just about across the board that applies.

Now, if we are talking about children versus those that are a little older but they are still teenagers, who is going to tell the truth about their age when they are online? You know, I mean if it is an 11-year-old who is probably more adept at, you know, traveling all of these lanes than someone that is 32 years old, but there is a restriction because of their age, why would they tell the truth? So it seems to me that, you know, this is something we need to figure out. I don't know how we protect children if, in fact, we start out with that as an approach to this issue of privacy and all that is attached to it. Have any of the agencies given thought to this? And if so, what is it?

Ms. RAMIREZ. I will take the lead, if I may.

Ms. ESHOO. Sure. You are brave.

Ms. RAMIREZ. The FTC has certainly thought about these issues and you certainly raised some very important practical concerns. The Agency is currently undergoing a review of the rules——

Ms. ESHOO. Um-hum.

Ms. RAMIREZ [continuing]. And staff is analyzing comments on the——

Ms. ESHOO. When are you going to finish that?

Ms. RAMIREZ. We are moving forward with that and expect to be coming out with recommendations shortly.

Ms. ESHOO. But does it cover this issue?

Ms. RAMIREZ. Well, I can't comment on the specific recommendations that will ultimately be made, but I will tell you that——

Ms. ESHOO. No, I am not asking you what your recommendation is going to be. I am asking you if you are examining this specific issue and when you are going to be finished.

Ms. RAMIREZ. We are examining the practical difficulties that do apply when applying that statute, yes. And in particular, the issue has frankly become of greater concern when one speaks about teenagers who may raise even more significant concerns along those lines. And that is an issue that we are also seeking comment on and will be addressing in our final——

Ms. ESHOO. My time is running out.

Mr. Chairman?

Mr. GENACHOWSKI. I agree that a focus on children as a starting point is something that should be strongly looked at. Part of the reason is it is an area where there is the widest consensus——

Ms. ESHOO. Um-hum.

Mr. GENACHOWSKI [continuing]. That as a parent that we want to make sure that we know how to basically protect our children and that the Internet is a safe place for them as well as a place that they can learn——

Ms. ESHOO. Are you looking at this?

Mr. GENACHOWSKI. We are looking at it with respect to communications networks, and we have been working with innovators in the area——

Ms. ESHOO. Um-hum.

Mr. GENACHOWSKI [continuing]. Encouraging them to develop tools. And I was in your district a couple of months ago and at the Computer History Museum we organize a showcase of tools and technologies that were being developed to help parents exactly with these issues online——

Ms. ESHOO. Well, a lot of companies are becoming that much more sensitive about—well, I think my time has run out but I think that this hearing is most helpful to move this issue along. Thank you.

Mrs. BONO MACK. I thank the gentlelady and know recognize the vice chair of the subcommittee, Ms. Blackburn, for 5 minutes.

Mrs. BLACKBURN. Thank you, Madam Chairman. Thank you all for your patience.

Ms. Ramirez, I want to go back. In your testimony you stated that you thought the harm was lack of choice or lack of knowledge of how their information is being used and your comments about the public. So what I am wanting to know from you is do you think that is justification for implementing Do Not Track? Are you going to come forward and identify some real harms so that you are articulating what the bad practices or the bad actions are that would require Do Not Track addressing, and are you planning to do any market analysis and market impact of any steps that you come forward with?

Ms. RAMIREZ. Let me first emphasize that the Commission is not advocating legislation in the privacy arena at this time. What we have done is to put out a broad framework of best practices that we recommend to industry and also a framework that policymakers can consider should Congress decide to pursue legislation in this arena.

As to your specific question regarding Do Not Track, that is just simply one element and one aspect of the recommendations that relates solely to behavioral advertising——

Mrs. BLACKBURN. So you are not wedded to that as a template?

Ms. RAMIREZ. So what we have stated—and the majority of those of us on the Commission do advocate—is a universal Do Not Track mechanism. We have identified several elements that we think are important to——

Mrs. BLACKBURN. OK. Are you separating the online advertising from some of the aggressive social media networking as you do that analysis? Are you separating those two transactions?

Ms. RAMIREZ. Again, online advertising, the majority of us do believe that there should be a Do Not Track mechanism that gives consumers greater choice about what information about them is collected and how that information is——

Mrs. BLACKBURN. OK. Let me move on with you then. The Supreme Court case, Sorrell v. IMS Health Incorporated, the Court struck down Vermont's Prescription Confidentiality Act. And Vermont's law restricted the ability of the pharmacist and drug manufacturers from using previous prescription data for marketing. Legal experts have claimed that this case will have implications for existing and proposed privacy laws. So yes or no, do you agree with the Supreme Court's ruling that restrictions on the collection and use of data must first pass the First Amendment's scrutiny?

Ms. RAMIREZ. I do believe that if there is legislation enacted in this arena, there need to be considerations that were identified by the Supreme Court in that particular case.

Mrs. BLACKBURN. OK. Do you believe the government must defer to less-restrictive alternatives in remedying privacy harms as the Court found in the recent Sorrell case?

Ms. RAMIREZ. Again, I think the applicable standards of First Amendment principles apply.

Mrs. BLACKBURN. OK. All right. Let me move on with you, then. Has anybody asked about Google+ and what you all are doing?

Ms. RAMIREZ. No.

Mrs. BLACKBURN. No one has? OK. What is the FTC doing—I will come to you in just a minute, Chairman Genachowski. What is the FTC doing now to oversee Google+ and the new service that apparently there are some problems with? If you will very quickly.

Ms. RAMIREZ. The FTC entered into a settlement with Google with regard to its rollout of its Google Buzz service, which was a social network service that it provided. The proposed order, which is yet to become final, contains a few key elements. One, it bars misrepresentations on the part of Google with regard to data practices. It requires Google to provide a comprehensive data privacy program and also to conduct privacy audits.

Mrs. BLACKBURN. OK. And what is the FTC doing in regard to Facebook and the facial recognition technology? Do you think that poses a threat to privacy?

Ms. RAMIREZ. I am afraid that I can't comment on specific practices or specific companies. What I will tell you is that the Agency is looking very closely at the social networking arena as evidenced by the Google Buzz case that we just discussed.

Mrs. BLACKBURN. OK. Thank you.

Chairman Genachowski, back to who has the jurisdiction here. How do you square this? How do you think that overseeing the issue of privacy fits into the FCC's mission? Because I see it more closely aligned with the FTC. So just 30 seconds on that.

Mr. GENACHOWSKI. Congress is assigned the Federal Communications Commission force since at least 1984 the responsibility for protecting CPNI or PII, various personal information on communications networks. And we have developed expertise around the engineering of those networks, the business practices of those networks that continues to be important even as we move forward

into this new area. And so it is the reason that we collaborate so closely with the Federal Trade Commission. We have a joint task force where we look together at some of these issues of overlap and we bring different experiences and expertise to the table that I think on a net basis is very beneficial in the area. We have an obligation to make sure that anything we do together or any areas of overlap and jurisdiction are communicated clearly and that the public and industry has clear guidance about what the landscape is and what they are supposed to——

Mrs. BLACKBURN. OK. I am over time. So thank you so much.

Mr. Strickling, you are off scot-free.

Mrs. BONO MACK. If the gentlelady would just yield for 10 seconds to Commissioner Ramirez. I thought I heard Ms. Blackburn ask about Google+ and your answer was not Google+. I was wondering if——

Ms. RAMIREZ. I believe the reference was to the Google Buzz matter.

Mrs. BLACKBURN. No, ma'am. I said Google+.

Ms. RAMIREZ. OK. Again, I can't comment on nonpublic matters, so my response was in reference to a recent——

Mrs. BLACKBURN. To Google Buzz.

Ms. RAMIREZ [continuing]. Commission order on Google Buzz that relates to social networking.

Mrs. BONO MACK. Thank you just for the clarification.

Mrs. BLACKBURN. Thank you, Madam Chairman.

Mrs. BONO MACK. And the chair is happy to recognize Mr. Butterfield for 5 minutes.

Mr. BUTTERFIELD. Thank you very much, Madam Chairman.

Right now, we are grappling with how a data security bill should treat activities regulated under Gramm, Leach, Bliley. We are all weary of duplicative regulation. On the other hand, we don't want gaps in consumer protection. Both CNN and NPR have reported that banks—which aren't within the FTC's jurisdiction—are selling information that they collect from credit and debit purchases. That is they are selling their consumers entire purchase histories to retailers. All calls for privacy legislation may be pointless if such legislation is limited to a select group of data collectors.

For example, if privacy legislation is limited to companies within the FTC's jurisdiction, as are many of current proposals in the House and the Senate, retailers such as Amazon would be limited in collecting and selling data about a consumer's shopping habits, but Citibank would be totally free to collect and sell that same information to Amazon. Do any of you have any concerns about such a scenario?

Ms. RAMIREZ. I can address the question and I will do it in reference to the draft bill that was discussed earlier, the Safe Data Act, where the Agency does have a concern that it drafted—there is a carve-out with regard to data security and breach notification. There is a carve-out for entities that would be subject to the FTC's jurisdiction. So we do have a concern about that gap.

Mr. BUTTERFIELD. Some have suggested that any data security legislation or privacy legislation we draft should be written very narrowly because there are sector-specific laws on the books already. Others want it broad enough to ensure that all gaps are cov-

ered. FTC has experienced sharing jurisdiction in other areas. Do you support data security or privacy legislation that could overlap with existing sector-specific regulation? Ms. Ramirez? Yes?

Ms. RAMIREZ. With regard to data security we do support legislation, again, keeping in mind that gap that I talked about. That is a concern. We do have limited jurisdiction in certain other respects. We do not have jurisdiction over banks, for instance, but we do support general data security legislation.

Mr. BUTTERFIELD. All right. And to the Chairman, Mr. Chairman, as you may know, the Internet service providers argue that they should not be subject to the requirements of any data security bill that this committee might consider. We have heard two basic arguments from them. One is that ISPs are just so-called dump pipes and they don't know what information is being passed to and from their customers. The ISPs have also argued that the FTC regulation would be duplicative because FCC regulates telecommunication service providers through the CPNI rules that include breach notification requirements for CPNI. Should those who provide dump pipes—and I just heard that word for the first time the other day—should those who provide dump pipes that sometimes carry innocuous documents and that sometimes carry sensitive documents also be subject to some minimum security requirements for the data that moves along those pipes?

Mr. GENACHOWSKI. Well, one way to look at it is from the perspective of consumer and outcomes. I think consumers just want to know that their private information that is put out on networks—and they don't know all the different details about what is this, what is that—that there are effective data security policies in place that they can rely on. And we want that as a country because not having that will hinder broadband adoption and the economic benefits of broadband. So I think we need to find a way to make sure that consumers have confidence in the safety and security of the Internet and the services that ISPs provide.

Mr. BUTTERFIELD. CPNI is the data collected by telecommunications companies about a consumer's telephone calls. It includes the time, the date, duration and destination number of each call, the type of network a consumer subscribes to, and any other information that appears on the consumer's telephone bill. That is pretty vast. Does FCC under these rules protect data breaches of content? For example, if I subscribe to the service of one of the traditional telecom carriers and I receive a voicemail which is content stored by that carrier, does that voicemail information have to be secured?

Mr. GENACHOWSKI. So there are two issues. I think from the perspective of the FCC rules and obligations on telephone companies, they have an obligation to provide security. From the perspective of third parties who might seek to hack in and get that information, that is a criminal violation that would be prosecuted by the appropriate authorities.

Mr. BUTTERFIELD. Well, what about if I subscribe to voice over IP service? I understand that voice over IP can transcribe a subscriber's voicemail message into email and text messages so that voicemail, email, and text will exist as content to the extent—and

Madam Chairman, I didn't realize my time had expired. I will save it for the next round. Thank you.

Mrs. BONO MACK. I would allow the gentleman to answer the question, though.

Mr. BUTTERFIELD. Yes. All right.

Mr. GENACHOWSKI. Well, I would say that the FCC has applied Section 222, the CPNI provisions, to voice over the Internet. We are viewing whether there are gaps as technology evolves, and that is something that we would look forward to work with the committee on.

Mr. BUTTERFIELD. All right. Thank you.

Mrs. BONO MACK. I thank the gentleman. And the chair now recognizes the chairman emeritus of the full committee, Mr. Barton, for 5 minutes.

Mr. BARTON. Thank you, Madam Chairwoman.

I think the questions that the committee members have been asking point out a fundamental issue that at some point in time we have to deal with. What information is personal and what information is private and who controls it? We get the same question in a different format from every member of the committee. And hopefully, in this Congress in conjunction with our agencies we can put in the statute in the regulation the answers to that question.

My first question is pretty straightforward to the witnesses here before us. Congressman Markey and I have introduced a bill, H.R. 1895, which is the Do Not Track Kids Act privacy protection of 2011. Do your agencies have a position on that bill yet, and if so, what is it?

Mr. STRICKLING. I will start. The administration has not yet taken a position on that or any other Do Not Track legislation at this point in time. I think, though, it is clear and will emerge from the work we are doing now that the idea of providing more protection for children and for adolescents is one that we think ought to be incorporated in the Fair Information Principles that we will be proposing.

Mr. GENACHOWSKI. And at the Federal Communications Commission, the Agency hasn't taken a position. Speaking for myself, the focus on children and the unique issues that are raised by children in the context of new technologies I think is appropriate.

Mr. BARTON. Thank you.

Ms. RAMIREZ. And the FTC also has not taken a position on the legislation but, as I have indicated earlier, the Commission does support the adoption and implementation of a Do Not Track universal system.

Mr. BARTON. Thank you.

This question is for Commissioner Ramirez at the FTC. Several years ago a company called Google used a technique called street mapping. This street-mapping service amassed quite a bit of data of very private and personal information. Google testified before this subcommittee—or at least one of these subcommittees—about it and promised that it was done unaware at the corporate level and they were going to make changes. They also, in response to an inquiry by the FTC, made fairly significant verbal assurances that they would improve their behavior and do certain things. But apparently that is all they did. They really didn't change their busi-

ness model and it appears to me that Google has adopted a model of saying one thing in Washington and doing another thing in their business practices. We might need to drop the G from Google and just call them Oogle because of what they appear to be doing. I am not saying that are doing it intentionally.

So my question to you, Commissioner Ramirez, when you have a company like Google that doesn't appear to really follow up and doesn't appear to change their business practice, what should a regulatory agency like yours do to insist that they change business practices, and do you feel that you have the adequate statutory authority to make that happen or do we need to pass legislation to give you that authority?

Ms. RAMIREZ. Let me just say that I don't want to focus on a particular company but the Agency is——

Mr. BARTON. My question is on that particular company.

Ms. RAMIREZ. What I can say is that the Agency is very vigilant when it comes to the issues about protecting personal information of consumers. With regard to Google, I did mention a recent proposed order that is soon to become final with regard to Google Buzz. In the situation that identified, that investigation was closed and I do believe that it highlights the limits of the FTC's jurisdiction in the following way. The Agency has done quite a bit with its Section 5 authority, but there are limits. If a company has not engaged in a misrepresentation, the Agency would not be able to use its deception authority to pursue an enforcement action, and that was the case in the Wi-Fi matter that you identified.

Mr. BARTON. So you think the Congress needs to give additional statutory authority to enforce that type of an action?

Ms. RAMIREZ. The FTC is not taking a position as to whether legislation is needed, but what I will say is that there are limits to the Agency's Section 5 authority, and in my personal view, there does need to be more work in order for consumers to have basic privacy——

Mr. BARTON. Under current law, your authority is limited?

Ms. RAMIREZ. That is right. Our Section 5 authority will not reach all practices that can cause concern in this area.

Mr. BARTON. OK. My time has expired, Madam Chairwoman, but I would just point out for thoughtful purposes, if this Congress or one of these regulatory agencies attempted to either pass a law or pass a statute that required every citizen to wear a transponder and keep it active so that everywhere we went, any place we shopped would be automatically recorded not just by the Federal Government but would be available to the private sector for use, our voters and citizens would come unglued. And yet if you go on the Internet without your permission, that is the basic status quo. And I believe we need to take steps to put privacy back into the personal realm and take it out of the consumer marketing opportunity realm and hopefully, on a bipartisan basis, we can begin to do that in this Congress and in this committee.

And with that I want to thank my two subcommittee chairmen and women for doing this hearing and the ranking members of those two subcommittees for participating. Thank you.

Mrs. BONO MACK. I thank the gentleman and now recognize Mr. Markey for 5 minutes.

Mr. MARKEY. Thank you. Thank you, Madam Chair.

I am just going to be following up upon the same line of inquiry that the gentleman from Texas and his son Jack were engaging in. Right now you can see his interest in child online privacy sitting up there. He is waving to you in thanks for the work that you are going to do to protect children online. That is Jack Barton over there.

So you heard this concern about an eraser button, you know, that can be used to just say that children and minors, what were they thinking going to that site? What were they thinking putting that picture up? What were they thinking when they were 13, 14. And in anticipation, now, of their Senate confirmation hearing where someone has now gone and pulled it all up or the admissions office at State U has now got someone kind of checking out what the kid did at age 12, 13, 14, 15. And there is a whole bunch of really young people going I know a lot of things about a lot of these candidates. That is not a good thing. There should be a way in which that information is erased. And it would be the parents, of course, who will want to erase it and that they have a right to do so and the technology makes it possible for them to do so.

And again, this is not big brother. This is just big mother and big father saying, you know, they were only 12, they were only 13, they were only 14 to the company. We want to be able to erase it. Do you think, Ms. Ramirez, that that makes sense, that that be a right that parents have to be able to have that technology available to them and that they can erase it not just on a discretionary basis but it is their right to see it mandated to the company that they have to delete it for a minor, for a child?

Ms. RAMIREZ. I do believe that that is an interesting idea that is deserving of exploration and we are happy to work with you in addressing that.

Mr. MARKEY. So you are not sure if it should be a right yet?

Ms. RAMIREZ. I would like to think about it further.

Mr. MARKEY. OK, good.

Chairman Genachowski?

Mr. GENACHOWSKI. Well, two points. One is the concerns about children are very real, very serious; and the second is empowering parents to do what they want to do when it comes to educating, protecting their kids is also extremely important; number three, technology as you have indicated can help solve this. Technology can provide these tools. And so I think this is a direction that makes sense.

Mr. MARKEY. OK. Mr. Strickling?

Mr. STRICKLING. The principle no one can disagree with. But here is, I think, the caution I would urge everyone to keep in mind, which is for the legislature or for the regulator to be dictating technological solutions I think is something we need to approach with caution. We need to establish the principles, and that is important——

Mr. MARKEY. OK. The principle would be that the parents have a right technologically to have the information erased and then it is up to the company to figure out what the technology is. Would that be oK with you? The principle is that parents should be able to get it erased. Do you agree with that principle?

Mr. STRICKLING. There is no way to disagree with that principle——

Mr. MARKEY. OK, thank you.

Mr. STRICKLING [continuing]. But I still would urge some restraint in terms of setting down in regulation something that could inadvertently and unintendedly lead to a loss of innovation on the Internet.

Mr. MARKEY. No, I appreciate that. We would depend upon smart people to make sure that we didn't invoke the law of unintended consequences.

Mr. STRICKLING. Right.

Mr. MARKEY. We would mandate to you to do it, to protect children and give parents the right to do it and to make sure that we don't invoke the law of unintended consequences. Do you think you could do that?

Mr. STRICKLING. So, yes, our model would say set the principle and then bring the stakeholders together to find the ways to do it.

Mr. MARKEY. Good. So is the same thing true on geo-location that you shouldn't have a tracking device on a 12-, 13-, 14-year-old, you know, that the parent should be able to have that shut off? Do you agree with that as well? Yes? I only have a minute left. Could you say yes, please?

Mr. STRICKLING. Sure.

Mr. MARKEY. OK, good. Thank you.

Chairman Genachowski, it is not a good idea for a 12-, 13-, 14-year-old to have all this tracking information? Do you agree with that?

Mr. GENACHOWSKI. So very quickly, I think there is a balance here that has to be done right——

Mr. MARKEY. Yes, I get it.

Mr. GENACHOWSKI. I have a 17-year-old. I want him to have a device where——

Mr. MARKEY. How about a 12-year-old, a 13-year-old?

Mr. GENACHOWSKI. Whatever the right age is, but at some age, for emergency purposes, a parent might want to make the decision.

Mr. MARKEY. OK. I got you.

Mr. GENACHOWSKI. The parental control is a powerful principle.

Mr. MARKEY. OK. But the technology is there to shut it off for all other purposes other than a parent. That is what I am saying, big mother and big father. Do you agree with that, Ms. Ramirez?

Ms. RAMIREZ. I do believe that parents should be able to have control over that.

Mr. MARKEY. OK. Good. And finally, on the targeting of marketing, you know, by these companies to children and minors, do you agree that there should be a prohibition on targeting minors? We don't let people advertise on children's programming, you know, the kind of products we don't think should be there with little kids. Do you agree as well that we should have prohibitions on the targeting of minors when it comes to, you know, these Internet- and Web-based services that are out there? Ms. Ramirez?

Ms. RAMIREZ. I believe that, again, parents should have control over it and should be able to provide——

Mr. MARKEY. And there should be a technology that makes it possible?

Ms. RAMIREZ. That is right.

Mr. MARKEY. Yes. Good. Mr. Genachowski?

Mr. GENACHOWSKI. Basically, yes. There is a long history, as you know, in the television area and I think borrowing from what we have learned that that has worked makes sense.

Mr. MARKEY. OK. Thank you. Mr. Strickling?

Mr. STRICKLING. I would agree with the comments already expressed.

Mr. MARKEY. Thank you. Thank you, Madam Chair.

Mrs. BONO MACK. Thank you. The gentleman's time has expired. The chair recognizes Mr. Latta for 5 minutes.

Mr. LATTA. Well, thank you very much, Madam Chair, and to our panel, thanks very much for being here to discuss this issue with us today.

And Mr. Strickling, if I could start, on page 1 of your testimony, you noted that the Department of Commerce has been working with the Internet Policy Task Force and the White House to conduct a broad assessment of how well our current consumer data privacy policy framework serves the consumers, businesses, and other participants in the Internet community. Can you talk a little bit about how the recently announced National Strategy for Trusted Identities in Cyberspace fits in with that assessment?

Mr. STRICKLING. Certainly. That is an effort, again, a voluntary effort to allow industry to develop ways that people can operate in the Internet environment with a trusted identity that can replace passwords and otherwise improve the security any individual might have transacting business on the Internet. Totally voluntary, the goal is to have industry develop these tools with government serving as a facilitator or convener. It is very much part of our overall multi-stakeholder approach to how to deal with these Internet policy issues.

Mr. LATTA. OK. And just to follow up on that because as we have been talking—you know, the whole discussion is with the privacy and if individuals are to participate in the identity management system, what protections would be in place to ensure the privacy of the information that they turn over to their credential provider.

Mr. STRICKLING. Well, keep in mind that our role in this will be to work with industry to have them develop these sort of trusted identify mechanisms. It is not a program that we are going out to the public with to get people in the public to sign up for these. The idea, though, is to create what the market and what consumers would find to be a preferred approach to operating and transacting business on the Internet than the current system, the passwords, which in many ways is quite insecure for people.

Mr. LATTA. Well, have you in your discussions with the folks out there that might be developing this, have they given you any indication how it might work then and to protect that?

Mr. STRICKLING. This effort is actually headed up by NIST at the Department of Commerce, so I have not had any of those conversations with industry about how they would go about this. But the folks at NIST are leading this effort.

Mr. LATTA. If I could, could I ask if you might be able to ask them if they could provide us with information of what they might have at this time on that? That would be greatly appreciated.

Mr. STRICKLING. Certainly.

Mr. LATTA. And if I could go on, I have heard there are certain allegations out there that certain foreign nations have more onerous privacy laws on the books than we have here in the United States, but they seem to apply those laws mainly only to American businesses. What is the administration doing to ensure that privacy protections aren't being used as a means of preventing American companies from competing in the global market?

Mr. STRICKLING. I will take that one. We are involved in a lot of discussions internationally with the goal of trying to reach some interoperability of privacy rules around the world. We think it is absolutely critical for American business to be able to operate in other countries. And while those countries certainly have valid and legitimate interests in protecting the privacy of their citizens, we think it is in everyone's interest to find a regime or set of regimes that are interoperable with each other.

I would mention that our emphasis on the creation of these codes of conduct by industry working with other stakeholders may be a way to bridge some of those differences between the privacy protections in our country as compared to those that might be employed in other countries, the idea being that if we can get the various of these other countries to recognize codes of conduct as an appropriate response to the privacy imperatives of that nation or set of nations, that gives industry an opportunity to create one operating approach that meets the obligations of many different countries.

So very specifically, in Europe, they are in the process of rewriting the European Union Privacy Directive, and we have had a number of conversations with the folks at the EU to talk to them about making sure that they have a role for codes of conduct as a way to meet these obligations. We see that as a fast way to achieve the interoperability our businesses need to be able to thrive internationally.

Mr. GENACHOWSKI. If I could just echo the—this is a very important effort. The threat to American businesses, our economy if this doesn't succeed is very significant. And the opportunity to make progress internationally on a set of principles that can be complied with across multiple jurisdictions is a window that is closing because if many countries go ahead and adopt inconsistent regulations, ones that make it extremely difficult, expensive, impossible for American companies to comply with, reversing that will be much more difficult than working now, as the Commerce Department is doing—we are and others—to establish a level playing field internationally from the start of this very important growing industry.

Mr. LATTA. Thank you very much. And Madam Chair, I see my time has expired. I yield back.

Mrs. BONO MACK. I thank the gentleman and now recognize the gentlelady from California, Ms. Matsui, for her 5 minutes.

Ms. MATSUI. Thank you very much, Madam Chair.

As I have said previously, in today's economy, information is everything to everyone even though we might think our personal information is not that important on various things. We might throw things away but it is important to somebody. And with ever-changing technologies and applications emerging, it is essential that we

properly protect the private and personal information of consumers. We must do it in such a way that doesn't stifle innovation. And as I said before, I know this is a delicate balance. But how do we find that delicate balance to ensure consumers are aware of what information is being collected and the scope of it while not stifling innovation?

Why don't you start off, Ms. Ramirez?

Ms. RAMIREZ. Yes. The approach that the FTC has taken has been precisely to solicit input on these complicated questions to ensure that we do undertake a balanced approach. And the framework that has been proposed preliminarily in staff's report issued last December is precisely an approach that we believe balances the need for consumer protection here as well as the needs of industry.

Mr. GENACHOWSKI. And I would answer that. The process that our various agencies have undergone and the process that Congress has undergone through the hearings on this topic, they actually led to growing consensus around some core ideas: focusing on consumer choice, transparency, and real data security. Obviously, there are a lot of issues in implementation, but I think where we are now collectively as compared to where we were a year ago reflects real progress. Obviously, now, the difficult task of converting that into rules where necessary at agencies—or not because I think to the point Mr. Strickling made before, industry-led efforts here can have particular benefits if they move and if they put those measures in place.

Ms. MATSUI. Do you have anything further to add, Mr. Strickling?

Mr. STRICKLING. Certainly. I will make it easy for you. Pass legislation along the lines of what we recommend. Baseline principles allow industry working with all stakeholders to develop codes of conduct and give the FTC the enforcement power it needs to enforce the baseline principles. I think that is exactly the balance we want to have. It gives industry the flexibility to craft specific rules of behavior that meet their needs and allow them to continue to innovate, but at the same time, it is based on a bedrock set of a bill of rights of privacy that ensure that everyone gets a basic amount of protection.

Ms. MATSUI. OK. Thank you.

And as you know, OMB is implementing a cloud computing initiative to improve government efficiency while saving taxpayers money. And I do support an initiative like this.

Now, Chairman Genachowski, do you support cloud initiatives and what kind of impact do you think it will have on our economy? And how can we ensure any potential privacy concerns with a cloud are properly met?

Mr. GENACHOWSKI. I strongly support these cloud initiatives. On the part of both government, large businesses, small business, they are efficiency-enhancing, productivity-enhancing, they will save money. They are new areas of tremendous growth for our economy. It is an example of a new technology that has extraordinary opportunities that also presents challenges. And there is no question that data security and privacy are some of the challenges. I would not tackle that by slowing down cloud computing. I would tackle

that by working diligently hard with industry to make sure that security is fully protected and taking advantage of the extraordinary technological expertise that we have in this country to make sure that that happens.

Ms. MATSUI. OK. Thank you.

As we all know, often these policies that we are talking about are drafted in complicated legal language. And more importantly, even if a consumer is able to understand a privacy policy of one company, the policies can't easily be compared from company to company. Thus, there is no means for consumers to comparison shop for privacy in any meaningful way. What can industry to do to improve privacy policies and set some standards so that privacy practices can be compared from company to company? Ms. Ramirez?

Ms. RAMIREZ. I first want to say that I agree that privacy policies—the way they have developed poses significant challenges. This is particularly acute in the mobile arena when you have a very small screen and sometimes you have to scroll through 100 screens to read a single privacy policy. So one of the key elements of what the FTC has proposed in its framework is that there be simplified consumer notice and choice. And that is an essential feature of the framework that we are proposing.

Ms. MATSUI. OK. I see my time is running out. Can you two just comment quickly on this, too?

Mr. GENACHOWSKI. I agree. I think the importance of industry-led efforts to ensure compliance with these principles that I think there is broad agreement on choice, transparency, real security is an important part of what we all need to be going forward.

Ms. MATSUI. Thank you. And Mr. Strickling?

Mr. STRICKLING. We totally subscribe to transparency and more simplicity.

Ms. MATSUI. OK. Thank you.

Thank you very much, Madam Chair.

Mrs. BONO MACK. Thank you. The chair recognizes Mr. Scalise for 5 minutes.

Mr. SCALISE. Thank you, Madam Chair.

And I know as we are all struggling with the balance between protecting privacy while also making sure that as people use the Internet, one of the great things about the Internet is that for the most part there are so many things you can do free where there are services that are provided but at the same time in many cases you are not necessarily paying for some of those services. And of course the hook comes in is that in many cases the things that you are doing on the Internet, there is some tracking that goes on and ultimately it is sold to advertisers, and the advertising money that those companies make allows them to provide the service for free. So you have got to weigh that balance and make sure that we can protect privacy and then also allow for that ability for consumers who do want to participate in that transaction to be able to still have those services offered if they so choose. And I guess that is where we really get into the policy side is how best to make sure that framework gives the consumer, the online user the choice.

I want to first just get your take on something. There was an article I read. It was called "You're Not Google's Customer—You're the Product." And it kind of lays out an interesting scenario of who

is the product, who is the customer. And in many cases you are a customer if you walk into a store and you pay for something, you are the customer. And it seems like in some cases some of these companies—not just Google but all of the companies that have this kind of business model—are you really the customer if you are really not paying for anything but in fact your actions on their Web site is what is used for them to then go and sell advertising and in essence would then the advertiser be the customer and not you? And then how does that relationship all come down to how you as regulators treat those various entities? And so if I could just get each of your takes on that, that business model and how you really view—where is the user of the service in that transaction?

Mr. STRICKLING. I will give my first impression. I haven't seen the article so I am not sure exactly the context in which——

Mr. SCALISE. I ask unanimous consent to enter this into the record and make it available to the witnesses as well.

Mrs. BONO MACK. No objection.

[The information follows:]

You're Not Google's Customer -- You're the Product: Antitrust in a Web 2.0 World
By Nathan Newman
March 29, 2011
http://www.huffingtonpost.com/nathan-newman/youre-not-googles-custome_b_841599.html

You think Google's search engine is great. Gmail is easy to use. YouTube gives you instant access to funny pictures of dogs and music videos. And Google maps helps you find where you are and the nearest pizza place. And it's all free.

So you're a happy customer and don't understand why anyone would think antitrust action is needed against Google. Or why government officials from Europe to the U.S. Congress and, just last week, U.S. state governments are bringing antitrust investigations against Google.

Except remember -- it's free! Google doesn't make a dime of profit from you, so you aren't the customer. In fact, all those cool products are just bait to get your information in the Google ecosystem so your attention and eyeballs can be sold to Google's advertisers.

The pleasant experience of using Google products is little different (in any economic analysis) from the pleasant massage administered to Kobe beef cattle in Japan; each is just a tool to increase the quality of the product delivered up to the real customers.

What is Google's Market in a Web 2.0 World? So here's the key place to start in understanding proper technology policy for Google: there is **no market** for search engines; there is **no market** for online geolocation mapping software; there is **no market** for online video.

Google, by making these products free, has destroyed those markets in favor of an alternative economic model of selling individual attention and precise information about those users to advertisers. You are the product, not the customer. That market between Google and its advertisers is where antitrust authorities ultimately have to look to understand what public policy is needed.

As law professor Siva Vaidhyanathan describes in his just-published *The Googlization of Everything (and Why We Should Worry)*, "Google's method of generating and selling advertisement placement is brilliant." Through user queries and searches, as well as personal information about those users, Google can deliver a product to advertisers tailored to their exact needs -- people looking for shoes are delivered to shoe sellers, people located in a certain town are delivered to local restaurants, and so on.

And while individual users may think the brilliance of Google is in the technical design of its search engines, as a company, its profit is driven by its brilliance in nearly monopolizing the online search marketplace serving these advertising companies.

And what profits! With revenue coming overwhelmingly from its advertising monopoly, in 2010, Google's net income was $8.51bn, up 30 percent from 2009 on total revenue that grew 24 percent to $29.32bn. And to understand Google's dominance, look at this chart of data from E-marketer, which shows Google's overwhelming dominance over its competitors in delivering search advertising:

US Search Ad Revenues at Top 4 Search Sites as a % of US Total Search Ad Spending

	2009	2010	2011	2012
Google	70.5%	71.4%	75.2%	76.6%
Microsoft	8.9%	10.2%	10.8%	11.1%
Yahoo!	15.7%	10.4%	8.1%	6.5%
AOL	3.0%	2.3%	1.9%	1.5%

Data: E-Marketer

Note that Google's dominance is growing and is projected to grow more. In mobile phone advertising, Google has established a phenomenal 97 percent of paid mobile search advertising, which by itself is projected to be worth $1.1 billion by the end of 2011 and is likely to skyrocket as a percentage of advertising.

And this dominance cannot easily be overcome by some alternative upstart website, even by well-capitalized competitors, since underlying Google's enterprise is, in Vaidhyanathan's words, a "monumental collection of physical sites such as research labs, server farms, data networks and sales offices." Given the interplay of different Google services and customization of results based on having so many users involved in its ecosystem, there are so-called "network effects" from being dominant that any competitor has too large a challenge in displacing Google.

So what are all the cool new Google products like Android, Chrome and Apps for? First, they are more ways to collect the personal information to target advertising to individuals (and new threats to personal privacy as described below).

But they also serve a sinister role from an antitrust perspective. They help destroy any alternative economic base for a competitor to challenge Google's dominance of online search advertising. Citing Warren Buffet's observation that strong businesses are "economic castles" protected by "moats," analyst Bill Gurley describes these free products as moats to drown any competitor who "stands between the user and Google":

Android, as well as Chrome and Chrome OS for that matter, are not "products" in the classic business sense. They have no plan to become their own "economic castles." Rather they are very expensive and very aggressive "moats," funded by the height and magnitude of Google's castle... Google is also scorching the earth for 250 miles around the outside of the castle to ensure no one can approach it.

To understand how this plays out in antitrust analysis, look at a top current focus of the Justice Department's Antitrust division, namely Google's proposed acquisition of travel software provider ITA Software. ITA provides the underlying technology used by online travel agents, travel websites and airline websites. Now, some analysts worry that Google could use its position to unfairly price access to the database to potential competitors in the travel search market or skew search results to favor key partners.

But if it just destroys the business model for competing travel agents and websites by absorbing the service into its overall search system, it will undermine a whole set of potential competitors for advertising dollars. Tim Wu, a law professor and author of the book *The Master Switch*, argues of such a deal, "In the longer term, however, the risk is that this deal could give Google such an advantage that travel search becomes like other forms of search, dominated by one engine, which could eventually stifle innovation." (And of course, Google may just flat out skew results in travel, given complaints across a wide range of areas by businesses involved in its search and advertising market, as I detailed in my post, The Case for Antitrust Action Against Google.)

How Privacy is Threatened by Google's Business Model: So why should individual users care about any of this if they are still getting the goodies for free?

The reason this is not a dry economic issue of whether Google is cutting into the profits of a few competitors or deciding a few winners and losers desperate for a higher ranking in its search results is that Google is not giving anything away for free. Google's whole business model is based on systematically stripping away user's privacy to trade Google's knowledge about you to advertisers.

A former Federal Trade Commissioner, Pamela Jones Harbour, highlighted the problem of this model for both privacy and antitrust policy in the American Bar Association's *Antitrust Law Journal*. Harbour, who served at the FTC from 2003 to 2009, dissented from the FTC decision to allow Google to take over the online ad display company, Doubleclick. If you understood that the relevant market was "data used for behavioral marketing," the merger brought together two companies already controlling large amounts of personal data, so the merger left Google even more dominant in this sector.

Harbour emphasizes the point made above that you miss the ball if you look at "search engine markets" or "map software markets", but instead you have to understand that the product is aggregated personal data where:

...[revenue] derives from the accumulation of data, which can then be put to myriad commercial uses... The sites are subsidized, in effect, by trading on the value of accumulated data. In many instances, the data come from individual consumers, who may or may not realize that they are paying for "free" information or services by disclosing their personal information.

Companies like Google with the most specific personal data can better target ads and thus dominate these advertising markets. What this also means is that non-price factors, such as privacy decisions by consumers, can easily be distorted in a non-competitive online environment. If companies' real constituencies are advertisers, they then have a strong incentive to violate privacy if it serves their behavioral targeting goals. Thus you end up with Google continually breaching consumer privacy, even going as far as the wi-fi spying through their Street View project, without too much worry about losing consumer support.

Some neoliberal doubters of the need for antitrust and other regulatory action on Google might argue that market competition will protect privacy, but if you understand that the relevant customers are the advertisers -- and it's the advertisers who want privacy violated to better target advertising -- you'll understand that the "market", such as it is, is driving the destruction of personal privacy online.

There may be a "market" for convincing customers that companies are trying to protect individual privacy, but, to return to the Kobe beef metaphor, that's the same incentive for hiding the slaughterhouse from the cattle. It's only a cosmetic change in a business model driving to the same result.

Why Active Regulation is Needed: What's clear is that "the market" is not going to solve either the antitrust or the privacy problems from Google or comparable actors in other sectors of the online world. A Web 2.0 world requires new tools and analyses, where a company like Google with such dominance needs to be treated a bit more like a public utility -- delivering important public benefits but also requiring public accountability to protect the public interest.

Mergers by Google deserve more skepticism -- and the privacy and antitrust implications of its actions need sharper scrutiny (something the judge who blocked the Google Books settlement this past week thankfully engaged in).

But that's just the first step. More active regulation is needed to protect privacy and keep competition alive to maintain pressure for innovation on even as dominant a player as Google. One flip side of understanding how critical violations of privacy are to Google's economic model is that enacting stronger privacy protection also will, in former FTC Commissioner Harbour's words "directly influence how much competition is able to emerge in related technology markets." Harbour points to strengthening the ability of consumers to port data from one service to another as an example. While it looks like a consumer protection practice, it also service competition policy as well:

Imagine that a given legal regime were to encourage greater consumer control over data (e.g., through open standards), such that a market emerged to accommodate the porting of data relatively easily among applications. In that entry-friendly environment, if consumers were unhappy with the level of privacy protection offered by a popular application or service, consumers would be better able to "vote with their feet" (or, more accurately, their data) and switch to competing providers, without losing the accrued value of their personal datasets.

Still, even data portability is not enough in a world where users often don't know how companies are misusing their data. Analyst and Seton Hall Professor Frank Pasquale argues that data portability and other market-based regulations will fail: "privacy regulators' monitoring of oligopolistic online entities will be more effective than waiting for the elusive concept of 'privacy competition.'"

That's one reason I do think U.S. policymakers need to look at policy innovations in Europe that are demanding specific rights for consumers and even promoting key technologies that bypass the privacy-destroying process of many current online practices. They are moving towards policies that give individuals the right to remove personal data from online databases, require transparency in what data has been collected, and require explicit consent to collect personal data in the first place. Germany, for example, is requiring new central online sites where individuals can track exactly what data is being collected on them -- and be able to remove it -- and even promoting alternative online mapping software that eliminates the requirement by consumers to share their location to access it.

Beyond Neoliberal Economics Online: Whatever the salience of the neoliberal economic argument that regulation is not needed and markets will protect consumers -- and the bloody financial meltdown should make anyone question the general doctrine -- what's clear is that the Web 2.0 world has its own dynamics that make even the basic assumptions of neoliberal economics invalid.

Markets online are odd multi-party affairs, where individuals (often unknowingly) trade off their private information to intermediaries like Google, which in turn market that information to advertisers, who in turn try to market products or services often from other companies back to individuals. Individual interests in privacy are at war with the interests of advertisers in obliterating that privacy and "network effects" allow a company like Google to attain greater and greater dominance, even as it uses giving away free products to undermine the business model of potential competitors.

Waving the magic "market" wand seems a very weak and uncertain tool in achieving what we want as a society. Instead, what is needed are clearer mandates on all online companies to deliver what is promised -- whether products, searches or social connections -- while severely limiting how those companies can resell or market based on personal data without explicit consent.

People deserve to be back in control of their online experience, not merely a data point in a product marketed to advertisers.

Mr. STRICKLING. That would be great, but I think I can answer your question, which is that what is key here is if you are collecting information about people, so I think there is nothing to be gained by a distinction between a customer and a non-customer or a product or whatever. The issue is information about you being collected by this particular entity when you go online to their Web site. And it needs to be made very transparent and in clear language, you know, to you in whatever capacity you are coming to that Web site, what that information is and how it is going to be used. But I don't think the distinction is important. The question really is are you collecting information about this individual when they visit your Web site?

Mr. SCALISE. Chairman Genachowski?

Mr. GENACHOWSKI. I would add this. We are in a period now in this country of tremendous and technological and business model innovation and that is a really good thing. It is part of what makes our country great. It is part of what will ultimately make our economy sound and strong. And we wouldn't want to be seeing this happen in other countries and not here. Now, new technologies, new business models gives rise to new concerns, and it is appropriate that we are having this discussion, this debate involving industry, involving agencies, involving Congress to identify core principles that should be protected even as we encourage world-leading business model and technological innovation. And so it is what I keep coming back to and I think Mr. Strickling—we all do—core principles that can help provide guidance even as we make sure we are encouraging world-leading innovation and technology in business models.

Mr. SCALISE. Thanks. Commissioner Ramirez?

Ms. RAMIREZ. We also recognize that consumer information is becoming a commodity. We do believe that you can craft standards that take into account the benefits provided to consumers while at the same time providing protection. And to me, the core issue is, again, providing transparency, providing information to consumers so that they can exercise choice. And let me just use the example of the Do Not Track mechanism that I believe should be implemented. I believe there can be an intermediate approach that can be used where consumers can select what type of advertising they are willing to receive and what type of information about them can be collected so that in that fashion advertising would continue. But, for instance, if a consumer doesn't want to receive advertising relating to health information, that would not be done, but they could receive advertising——

Mr. SCALISE. OK. Thanks. And I have got just a few seconds. One last—Chairman Genachowski, in relation to a question that I think Congresswoman Blackburn had asked, I am not sure if you implied it, but it seemed like you might have been referring to the Internet as a telecommunications service. I mean, I wouldn't consider it a telecommunications service in that sense. Was that your intention or——

Mr. GENACHOWSKI. I am not sure I used that phrase. I may have referred to it as a communications network and I think it clearly is.

Mr. SCALISE. But not a telecommunications service because that would in terms of classification——

Mr. GENACHOWSKI. Which I didn't intend to raise.

Mr. SCALISE. Great. No, I appreciate it. Well, thank you all for your answers and I yield back.

Mrs. BONO MACK. I thank the gentleman and recognize Mr. Rush for 5 minutes.

Mr. RUSH. Thank you, Madam Chair. And Madam Chair, I certainly want to thank you and all the other very important people who have put together this hearing. And I want to thank all of the witnesses for appearing before us today. I know they are quite busy but to come over and share with us their opinions and their conclusions.

Commissioner Ramirez stated correctly, I believe, that individuals can and do have varying privacy tolerance thresholds, and these thresholds can and do turn on several variables, including who has their personal information and what that information—which is personal in nature—what it represents. And I introduced a bill in the last Congress and reintroduced it in this Congress. It is called the Best Practices Act, H.R. 611, which would require covered entities to obtain express consent from consumers for collection, use, or disclosure of particularly sensitive information or comprehensive online data collection. Among other things, it would give the FTC APA rulemaking authority to further modify the definition of "sensitive information." Given how complex a person's decision-making process and all the dependencies that are involved, I would like to ask each of the witnesses today—and especially you, Commissioner Ramirez—your opinion on whether such a grant of authority is prudent and would it make for a good public policy?

Ms. RAMIREZ. Again, let me just say that the FTC has not taken a formal position on legislation but I will note that in the privacy report that was issued in December, the staff does recommend that sensitive information be provided, both additional data security protections and that consumers be given an opportunity to provide express affirmative consent for the use of that information. I also do believe that if legislation were to be enacted, it would be beneficial to accord the agency APA rulemaking authority to make modifications should that prove necessary with regard to the types of sensitive information that would be protected.

Mr. RUSH. Chairman Genachowski?

Mr. GENACHOWSKI. Let me just add that the less clear and more confusing disclosures are about how information is being used, the stronger the argument for an opt-in requirement. The more clear, easy-to-understand, transparent disclosures are, the weaker the argument is. And so it is an area where the industry can step up, provide disclosures about how they are using information, what they are collecting that are so clear that make it so easy for consumers to choose that there would be no need to have an opt-in/opt-out debate. If the industry doesn't do that and the disclosures are less clear/more confusing, I imagine we will continue to hear from consumers saying we don't understand this. We need some defaults.

Mr. RUSH. Mr. Strickling?

Mr. STRICKLING. I guess I would like to take your question up just one level because it could be raised about any number of things and again point out, you know, our concern about getting too detailed and too regulatory in terms of specific prohibitions and the mechanisms that are used to implement them. What is important we can all agree is that there be meaningful consent. None of us can predict today what technology might be available in 2 or 3 years by which meaningful consent could be obtained from a consumer. And therefore, we are quite concerned about incorporating into legislative language or in rulemakings that by themselves will take quite some time to conduct, you know, very specific approaches. To preserve the ability for business to innovate, we think this is a perfect example of where you set the principle and then ask industry working with all stakeholders, civil society and other folks that are interested in this to devise the rules of behavior that would actually be engaged in and which can be changed on a regular basis to accommodate——

Mr. RUSH. I want to move on. Commissioner Ramirez also stated that some consumers may be more predisposed than others to be taken advantage of, including consumers who are put on marketing sucker lists based on their past behavior. This may beg additional question as to what could be deemed to be sensitive information. Along that line of logic, how sensitive would you say other forms of compulsive disorder-related personal information about consumers such as drugs, sex, gambling addiction, for example? How sensitive would those particular areas and other areas be to you?

Ms. RAMIREZ. And again, I will turn to the recommendations that were made in our privacy report to identify certain categories such as health information, financial information, geo-location information. So those I would classify as being sensitive.

Mr. RUSH. Commissioner?

Mr. GENACHOWSKI. I would agree with that.

Mr. STRICKLING. In our legislative proposal on data breach in May, we provided a list of what the administration would believe to be sensitive personal information. And I would refer to that list.

Mr. RUSH. I yield back.

Mrs. BONO MACK. I thank the gentleman and recognize Dr. Cassidy for 5 minutes.

Mr. CASSIDY. Commissioner Ramirez, you helped me last time understand what HIPAA applies to and what it does not. Now, your opening statement was kind of like a good Hemingway story. That first sentence kind of grabbed me and took me off with you. So when I go to CVS and I buy my Advil for my bad knee, is that HIPAA-protected that I just purchased Advil over the counter or can CVS integrate that with other bits of data so now I start getting advertisements for Advil or other non-steroidals on my side bar as I do the net.

Ms. RAMIREZ. If you go to a retailer, that would not be protected under HIPAA. HIPAA only covers things like hospitals, medical providers. So retailers would be able to use that information.

Mr. CASSIDY. Well, I buy glucosamine chondroitin just to tell you more about myself than you care to know.

Ms. RAMIREZ. I am sorry. Say that one——

Mr. CASSIDY. I buy something for osteoarthritis and it is non-protected. It is over-the-counter. And they can integrate that with other things known about me since I have a little kind of rewards card, and that can go into this database that says here is Bill Cassidy. Let us tag the son of a gun.

Ms. RAMIREZ. That can be done, yes.

Mr. CASSIDY. Now, what if it is a prescription medication?

Ms. RAMIREZ. Prescription medication would have other protections, but again if, for example, one does research online, it is conceivable that certain personal health information could then be part of a profile that is compiled digitally.

Mr. CASSIDY. Well, I go to PubMed, the National Institute of Health Web site—I am a physician—regarding medical information. I may look up anything I want to there. I am a physician. So I look up hepatitis. Now, that I don't see things on the sidebar about hepatitis. So clearly it is possible to keep that even if I start off—but let me ask you if I go to Google and just put in hepatitis and I come up with Wikipedia and I come up with PubMed and I go to PubMed, the very fact that I put it into Google means that now Google knows I am interested in hepatitis, correct?

Ms. RAMIREZ. Correct.

Mr. CASSIDY. But what about my credit card company? If my credit card company I am purchasing airplane tickets to come to Washington, D.C., does American Express or U.S. Air or Visa integrate that into my overall profile?

Ms. RAMIREZ. I would note that the Agency doesn't have jurisdiction over banks so there are certain safeguards that apply to financial information that might be more strict. So there is a difference there.

Mr. CASSIDY. Got you. The other thing I am noticing that is in my inbox now, I will get an email from somebody suggesting that I have requested information from them and I happen to know that I have not. It is almost a form of phishing. Is this something that is common now that some bank will say you need to update your records? We see there has been a recent change and so our—not a bank because you don't have banks but some other company that basically entices me to go to their Web site to update my records even though I haven't used that service?

Ms. RAMIREZ. There are a number of scams that we are aware of where fraudulent operators may try to get confidential information from consumers——

Mr. CASSIDY. I see. So that may be the company or that may be a scam?

Ms. RAMIREZ. So consumers need to be careful about that, certainly.

Mr. CASSIDY. Yes, I got you. And now the children's aspect of this, Commissioner—and I guess it is you—I have a daughter who is 9 and she just kind of whizzes past. She accepts everything, oK? I am struck that some of these do-you-accept are so long that unless you are an obsessive compulsive attorney you are just never going to read it. So is it possible to surely make me fully aware of this but I am not fully aware of it because it is somewhere on line 47 of paragraph 42? Do you follow where I am going with that? To put it differently, when we ask someone to opt in or opt out, an

effective technique would be to bury it within long contract language. Is there currently any rule that would make the companies say listen, if you are going to have them opt in/opt out or agree to a certain type of advertising, it has to be understandable and not buried deep within a contract? Does that make sense? You are looking at me blankly so was I——

Ms. RAMIREZ. I am sorry. I wasn't sure if you were speaking to——

Mr. CASSIDY. To whoever is the person——

Ms. RAMIREZ. I will take this. Again, we do have concerns about long privacy policies. One of the key elements of the FTC's recommendations is that notice and choice be provided in a simple, understandable manner. There is no current requirement that that be done, but we believe as a best practice, companies ought to do that.

Mr. CASSIDY. Got you. OK. I yield back. Thank you.

Mrs. BONO MACK. Thank you, Dr. Cassidy. And the chair recognizes Mr. Harper for 5 minutes.

Mr. HARPER. Thank you, Chairman Bono Mack.

Commissioner Ramirez, I want to follow up on some questions or an area that Mrs. Bono Mack had done regarding harm to consumers. And does the Commission or can the Commission provide specific examples of actual harm or we talking more of hypotheticals?

Ms. RAMIREZ. The harms that we are concerned about are not speculation. We have heard public reports of activities along the lines of the hypothetical that I used in my opening statement as actually happening. Insurance companies, for instance, today are developing models by which they can assemble information that is available to them through this aggregation of data that we have been discussing as a means of substituting what formerly would be more complicated underwriting analyses. So the potential is clearly there. There are public reports that these things are happening today.

Mr. HARPER. Are you able to provide to us evidence or documentation of those specific harms?

Ms. RAMIREZ. The FTC, we are certainly happy to work with you to provide more details and information about those harms.

Mr. HARPER. All right. As we look at this, before we look at additional regulations or we look at information, should the Federal Government be required to show what significant consumer harm exists to justify the type of additional costs that we could be talking about when it comes to market regulation on privacy or Do Not Track legislation that that might impose upon businesses?

Ms. RAMIREZ. I believe that if Congress decides to move forward with legislation, certainly, one has to take into account the implications for all relevant stakeholders, yes.

Mr. HARPER. Have you done any analysis of that potential cost, the cost to businesses for that?

Ms. RAMIREZ. Again, we have solicited comments and have received over 450 comments from industry, consumers, and other stakeholders. We do have a Bureau of Economics that is involved in our review and we will be putting out recommendations later this year.

Mr. HARPER. OK. And do you have a time frame? Later this year——

Ms. RAMIREZ. Later this year.

Mr. HARPER [continuing]. When you think that might be?

Ms. RAMIREZ. I am afraid I can't be more specific.

Mr. HARPER. OK. We will give you that much wiggle room.

Ms. RAMIREZ. I appreciate it.

Mr. HARPER. Can you tell me how much we know about what information Internet sites collect about users and how much do we know about the sharing of that information? I know we have covered that some in this hearing, but can you enlighten us?

Ms. RAMIREZ. I am afraid that I can't quantify the scope. What I can tell you is that there is clearly a need for the principles that we are advocating. There is clearly a need for greater transparency. There is a greater need for companies to take into account privacy protections when they provide services and products to consumers and a greater need for simplified choice.

Mr. HARPER. You know, some critics have expressed concern that self-regulatory schemes could constitute a barrier to entry, perhaps erected by, you know, more powerful market participants against smaller and newer companies. How do we guard against such a result as that?

Ms. RAMIREZ. I do think it is a concern and that one has to take into consideration the impact on small- and medium-sized businesses. It is an issue that the Agency is looking at very closely and we do intend to address the issue in our final report.

Mr. HARPER. And what would be the best alternative to self-regulation? Is that going to work?

Ms. RAMIREZ. Well, that is an issue that I think you will have to ultimately decide as to whether or not legislation is needed. But if one is to rely on self-regulation, what I will say is that is very important that there be an enforcement element. There has to be accountability, and I think the FTC ought to play a role in enforcement.

Mr. HARPER. Thank you, Madam Chairman. I yield back.

Mrs. BONO MACK. Thank you. The chair recognizes Mr. Olson for 5 minutes.

Mr. OLSON. I thank the chair. I would like to welcome the witnesses again and thank you all for coming and giving us your expertise and your time.

And my first questions are for you, Commissioner Ramirez. I want to kind of follow up on the line of questioning from my colleague from Mississippi, Mr. Harper, was pursuing.

In December of 2010, the FTC issued a preliminary staff privacy report to open up discussion on consumer privacy issues and in that report advanced the concept of Do Not Track. This concept has been compared by the FTC and others to the national Do Not Call Registry already managed by the Commission, but in reality, they are very different. Do Not Call, as you know, was created because people being bothered by unsolicited telemarketing calls particularly during their dinner hours. But online advertising is not invasive in that way the way telemarketing calls are, and consumers can simply ignore ads online when they come up. You know, in my experience, none of my friends has slammed their

computer on the floor for online advertising, but I have seen many of them slam the phones on the floor because of repeated calls from telemarketers.

And so there are many benefits to targeted ads online such as giving consumers information about products and services they might actually be interested in. This type of advertising also has great value to consumers because this advertising revenue funds the free online content and service consumers enjoy. But I ask you, do you concur that Do Not Track is analogous to the Do Not Call Registry?

Ms. RAMIREZ. I do not. I agree with you that there are significant differences. First of all, the Do Not Track system would not call for the creation of any kind of national registry. It is also not something that has to be implemented necessarily by government. So what the Agency has advocated is we have put out a description of various elements that we feel would be important, but again, the key feature of it would be that it is a universal mechanism to allow the consumers that do have a concern about online collection and use of information to have greater choice and control over how their data is being used.

Mr. OLSON. Is Do Not Track feasible now, ma'am?

Ms. RAMIREZ. Yes, it is. We have a distinguished team of technologists at the FTC and a number of companies do agree, there is consensus that it is feasible.

Mr. OLSON. You can kind of take in my colleague from Mississippi's line of questioning. Since you say it is feasible, have you performed any economic analysis of adopting a Do Not Track on our businesses?

Ms. RAMIREZ. No, we have not. And again, what we have done so far is to simply identify the elements that we think are important to a Do Not Track system but we are not advocated a particular mechanism.

Mr. OLSON. Are you planning on doing those?

Ms. RAMIREZ. We will be issuing final recommendations at the end of the year.

Mr. OLSON. And those will include the impacts of the economic impact?

Ms. RAMIREZ. I can't comment on the details but what I can tell you, as I mentioned before, is that we certainly understand the importance of taking into account the impact on business and we think that a carefully crafted standard can be adopted that will both help restore confidence in the online marketplace and I think businesses themselves recognize that consumer trust is vital.

Mr. OLSON. Yes, ma'am. And I have heard from some companies that legislation is needed to create an online privacy framework that is technologically neutral based on industry self-regulation and enforced exclusively by the FTC. And with respect to technological neutrality, is it true today that the FTC and FCC would have jurisdiction over the download of a video on demand from a cable company but only the FTC would have jurisdiction over the download of a video from an over-the-top provider like Netflix? Anybody can chime in there. You are the experts.

Mr. GENACHOWSKI. I think that is probably a correct description of the current framework.

Mr. OLSON. So can we come up with a proposition where we can have some common system where there is one regulator?

Mr. GENACHOWSKI. I am not sure that that is the answer. The FCC and the FTC have worked very well together over more than 20 years in areas of complementary jurisdiction to make sure that the expertise and experience that are different that each agency brings to the table informs solutions that get the balance right between taking in the account of impact on our economy and protecting basic values like privacy.

Mr. OLSON. OK. Thank you. And again, with respect to industry self-regulation—and this is mainly for you, Commissioner Ramirez—can you please advise the committee whether the FTC uses industry self-regulation in other contexts to protect consumers and what role the FTC believes industry self-regulation should have in protecting customers' online privacy?

Ms. RAMIREZ. Yes. We believe that self-regulation can play a key role. In fact, the FTC alone cannot undertake the effort that is necessary here to ensure that consumers have basic protections. So we think self-regulation is vital but again provided that there is an accountability mechanism, an enforcement mechanism and we believe that the FTC ought to provide that.

Mr. OLSON. Thanks to the answers to the questions. I see that the clock is going up and that means I will yield back the balance of my time.

Mrs. BONO MACK. Thank you, Mr. Olson. The chair recognizes Mr. Kinzinger for 5 minutes.

Mr. KINZINGER. Thank you. And thank you, Madam Chairman, and thank you——

Mrs. BONO MACK. Excuse me. Can you check your microphone?

Mr. KINZINGER. Yes, it is on.

Mrs. BONO MACK. Probably the one next—yes. Thank you.

Mr. KINZINGER. Well, thank you. Thank you for coming out. I appreciate it.

The explosive expansion we have seen in online marketing and tracking over the past few years has been unprecedented. From 2010 to 2014, the industry is projected to grow to about $2.6 billion from $1.3 billion in 2010. As a consumer who uses free services that have been made available by the Internet, I understand the value of behavior advertising and the effect it is having on this country's economic growth and job creation. Any privacy legislation that this committee considers must fully contend with the implications of what slower growth will have on both our economy and the services provided to the consumer.

It is estimated that privacy legislation could cost the industry as much as $623 million in growth if the legislation imposes limits on online tracking. I am also keenly aware that the decisions we make in this committee will profoundly impact the question of whether or not privacy is still a right in this country. The accelerated accumulation of aggregated data over the past few years is troubling for many consumers. I believe one important action this committee should take is determine what type of information is aggregated. Do a few companies control both sensitive health information and my shoe size? And as a consumer, am I allowed to know what in-

formation is stored about me? These are all important issues that I believe we need to consider when drafting privacy legislation.

So while some of these may have been asked in a different way, I will ask the first question to Commissioner Ramirez. What impact do you think Do Not Track legislation will have specifically on free Internet service itself?

Ms. RAMIREZ. Well, I think it all depends on how a Do Not Track mechanism is implemented. And of course, that is the key question. What the FTC has done is to outline what it considers to be the core elements that any such mechanism ought to have in order to assure basic protections for consumers and to allow them to have choice. And again, the emphasis here is on choice. I personally believe that a mechanism can be constructed that I would call an intermediate option that would allow consumers to have granular choice about what type of advertising to receive. And I think such a system would benefit both consumers and industry.

Mr. KINZINGER. OK. And I guess to all three of you, do you believe consumers have a right to know as far as what information is obtained and—on them both in the online and in the offline space and how do we determine what information is private and what is not? Again, this may have been addressed but I am curious as to—you know, do consumers have the right to know? And then also how do we determine what should be private and what should not, just generally? Mr. Strickling, go ahead.

Mr. STRICKLING. Yes, we think one of the fair information practices should incorporate this notion of the consumers knowing what is being collected about them and how it is going to be used. As a broader point, though, I would just say that the specific regulation about how that be done is not something we propose either Congress or a regulatory agency do. Again, we see the benefits. And this goes to your question about the costs that legislation and regulation impose on businesses. We think it is vitally important that we give industry the opportunity to take the principles and then create the voluntary codes of conduct that they will commit to live by without sacrificing innovation, without costing them the dollars that perhaps a less-well-crafted regulation might impose on them.

Mr. KINZINGER. OK. Sir?

Mr. GENACHOWSKI. I agree.

Mr. KINZINGER. We are all in agreement? Great. That is easy. Those are easy questions. No, I am kidding.

All right. Do we know the amount of data that companies are collecting specifically and do we know how that is being collected, bought, and sold? I know that is pretty basic, too.

Ms. RAMIREZ. I am sorry. Could you again—I didn't quite hear——

Mr. KINZINGER. Yes, do we know the amount of data that companies are actually collecting on consumers and do we know how that is bought and sold?

Ms. RAMIREZ. As I mentioned before, I can't quantify exactly what is taking place. What we do know is that information is being compiled and that there are very significant concerns. Again, the hypothetical that I used in my opening statement highlights how

this information can be used. And again, this is not speculation. That is happening today.

Mr. KINZINGER. Sure. Well, I appreciate everybody's patience and everybody coming in and spending some time with us, and I look forward to continuing to tackle this problem.

And I yield back.

Mrs. BONO MACK. Thank you very much.

And Mr. Rush has asked for a second round of a single question and the ranking member and I have agreed to allow Mr. Rush to ask one more question before we conclude.

Mr. RUSH. I really want to thank you, Madam Chair, and the ranking member for your kind indulgence. I also thank the witnesses.

This morning and this afternoon, you have been asked over and over what is the harm if a consumer Web site, social network, or supermarket knows about my personal habits and my private life? And today's testimony references have been made to broadband's possible effects on job creation and productivity. Assuming Americans are unemployed and searching for work, are there some issues that we may be overlooking regarding privacy safeguards that may be making it more difficult for Americans to obtain employment? Specifically, Commissioner Ramirez, has the FTC heard complaints from the public suggesting that their efforts to obtain jobs have somehow been hampered or harmed due to any privacy-related abuses?

Ms. RAMIREZ. Yes. And I think a number of the enforcement matters that the Agency has brought, I think it shows that there is a failing sometimes with regard to basic privacy protections. And those are highlighted in the written testimony that I have submitted.

But in addition to that, there is survey after survey that shows that consumers increasingly are very concerned about how their information is being used. So I think there is evidence that supports the idea that additional privacy protection is needed.

Mr. RUSH. Mr. Genachowski, do you want to comment on this particular matter?

Mr. GENACHOWSKI. I think that the relationship between what happens in the privacy arena and achieving the economic and job-creation potential of the Internet really are related. And so being very thoughtful about that is important. I mentioned in my opening statement the relationship between trust of the Internet and increases in broadband adoption in a world where almost all job postings are online. So I think you are raising a very important set of sensitivities that need to be very carefully considered in this area.

Mr. RUSH. Thank you. I yield back.

Mrs. BONO MACK. I thank the gentleman. And on his point I want to again reiterate that his question was a terrific one while we are here and the extensive deliberations and thought we need to put into all of this as we move forward. And as you know, this is a first in a series of privacy hearings that we will be holding this year, and I look forward to our continued discussions and our work together on how we can best balance these needs that everybody has brought up today. And it is clear to me anyway that personal data truly is a gold rush of our time.

And I would like to say Commissioner Ramirez, in her written testimony, referred to a statement by her fellow Commissioner Rosch with his separate views on Internet privacy and it has been shared with minority staff. And with unanimous consent, it will be included in the record. And without objection, so ordered.

[The information follows:]

Statement of Commissioner J. Thomas Rosch, Dissenting in Part
Internet Privacy: The Views of the FTC, FCC, and NTIA
Testimony before the
House Subcommittee on Commerce, Manufacturing, and Trade
and
House Subcommittee on Communications and Technology
of the House Committee on Energy and Commerce
July 14, 2011

INTRODUCTION

In December 2010, the Commission issued a preliminary staff privacy report ("Report") in order to continue the dialogue on issues related to consumer privacy and to solicit comment on a proposed new framework for how companies should protect consumers' privacy. Although I concurred in the decision to issue the Report and seek critical comment on the issues it raised, I have serious reservations about some of the proposals advanced in the Report, including the concept of "Do Not Track."

As a guide to Congress about what privacy protection law should look like,[1] the Report is flawed. First, insofar as the Report suggests that a new framework for consumer privacy should replace "notice" (or "harm") as the basis for Commission challenges relating to consumer privacy protection, that is unnecessary. A privacy notice that is opaque or fails to disclose material facts (such as the fact that consumer information may be shared with third parties) is deceptive under Section 5. That is particularly true if the sharing of the information may cause tangible harm. Moreover, Section 5 liability could not be avoided by eschewing a privacy notice

[1] The Report acknowledges that it is intended to "inform policymakers, including Congress, as they develop solutions, policies, and potential laws governing privacy." *See* Report at i, 2.

altogether both because that would generally be competitive suicide and because that course would be deceptive in that it would entail a failure to disclose material facts.[2]

Second, insofar as the Report suggests that "notice and choice" has ever been a basis for law enforcement at the Commission (*see* Report at iii, 8-11), that suggestion is unfounded. Although the Commission has on several occasions challenged privacy notices that it considered deceptive, it has never challenged a firm's failure to offer a particular kind of "choice." For example, the Commission has never challenged an opt-out mechanism on the ground that it should have been an opt-in mechanism. Indeed, if the notice has been adequate, consumers have generally not had any choice other than to "take or leave it," and that choice has never been considered to be a Section 5 violation unless what was represented in the notice was different than what was actually done in practice.[3]

In short, to the extent that privacy notices have been buried, incomplete, or otherwise ineffective – and they have been – the answer is to enhance efforts to enforce the "notice" model, not to replace it with a new framework.

---

[2] The duty to disclose "material" facts would be triggered when the information was collected, used, or shared in a manner that "is likely to affect the consumer's conduct or decision with regard to a product or service." *See* FTC Policy Statement on Deception, *appended to Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174, 175 (1984). In some cases, disclosure would not have to be express. For example, using consumer information to provide order fulfillment would be disclosed by virtue of the transaction itself. *See also* Report at vi, 41, 52-53.

[3] The Report mentions "access" and "security" as aspirational privacy goals. *See* Report at 7. However, with the possible exceptions of the Children's Online Privacy Protection Act and the Fair Credit Reporting Act, the Report does not suggest that Congress has ever enacted a special statute mandating "access," and the Report does not cite any instance in which "lack of access" has been a basis for a Commission law enforcement action. Moreover, except for the special statutes identified, the Report does not identify any special statute enacted by Congress that mandates "security" as such. The Commission has brought cases under the "unfairness" prong of Section 5 for failure to have reasonable security measures in place, but there was financial harm threatened in those cases.

As a hortatory exercise, the Report is less problematic.[4] Many, if not all, of the "best practices" suggested are desirable. However, I disagree with the Report insofar as it suggests that even when the privacy notice is inadequate, the defect may be cured if consumers are offered some "meaningful choice" mechanism – whether it be opt in or opt out. *See* Report at 41, 52, 56-68. If firms are offered that alternative, that might disincentivize them from adopting acceptable privacy notices in the first place. That would be undesirable. Moreover, the Report takes no position as to whether the choice mechanism should be an opt-in or opt-out mechanism. *Id.* Because that question is left open, the Report can be read to portend that the final Report will suggest an opt-in option. More fundamentally, the self-regulation that is championed in this area (*see* Report at 8) may constitute a way for a powerful, well-entrenched competitor to raise the bar so as to create an entry barrier to a rival that may constrain the exercise of undue power. *See* Report at 48 (respecting self-regulation as applicable to a "legacy system"). That possibility may be blunted by insuring that smaller rivals participate in the adoption of self-regulatory rules, but that may not be practical.

ANALYSIS

The Report repeatedly acknowledges that the increasing flow of information provides important benefits to consumers and businesses.[5] Report at i, iv, 21, 33-35. Yet, despite the

---

[4] The Report asserts that there are a number of "best practices" that private firms should adopt from the get-go in order to protect privacy. *See* Report at v, 39, 40-41, 43-52. Most of these practices are desirable in the abstract. But that does not mean that firms should be mandated *de jure* (*i.e.*, by legislation) to adopt them or that firms should be required to do so *de facto* (*i.e.*, that large, well-entrenched firms engaging in "self-regulation" should dictate what the privacy practices of their competitors should be).

[5] "In particular, [workshop] panelists discussed benefits specific to business models such as online search, online behavioral advertising, social networking, cloud computing, mobile technologies, and health services. Participants noted that search engines provide customers with

acknowledgment of these benefits, the Report, as written, leaves room in any final report for a prohibition against dissemination to third parties of non-sensitive information generally, and of information collected through behavioral tracking specifically.

First, based on testimony by some workshop participants, the Report asserts that the use being made of online and offline consumer information is contrary to consumer understanding. *See* Report at 25-26, 29. The Report also alleges that "consumer surveys have shown that a majority of consumers are uncomfortable with being tracked online." *Id.* at 29. Although some consumers may hold that view (which would be sufficient to make the practice of behavioral tracking a "material" fact), as the Report itself acknowledges it is inaccurate to assert that consumer surveys establish that "a majority of consumers" feel that way. *Id.* at 29 n.72. As others have observed, consumer surveys vary considerably in this respect. Of course, many consumers do not opt in to behavioral tracking when asked. But an even higher percentage do not opt out when given the chance to do so (and there is no solid evidence that this is because they have not been able to make an informed choice).[6]

Second, the Report asserts that the "notice" model that the Commission has used in the past no longer works (*see* Report at iii, 19-20) and that the Commission should instead adopt the

---

instant access to tremendous amounts of information at no charge to the consumer. Online advertising helps to support much of the content available to consumers online and allows personalized advertising that many consumers value. Social networking services permit users to connect with friends and share experiences online, in real time. These platforms also facilitate broader types of civic engagement on political and social issues." *See* Report at 33-34.

[6] *See, e.g.*, Thomas M. Lenhard and Paul H. Rubin, *Privacy and the Commercial Use of Personal Information: The Case of Customer Proprietary Network Information*, Progress on Point, at 6 (Aug. 2007)("[I]n testimony before the FTC on the experience of one firm, a witness indicated that, when the default was opt-in, 85 percent of consumers chose not to provide their data. In contrast, 95 percent chose to provide their data when the default was opt-out"), *available at* http://www.pff.org/issues-pubs/pops/pop14.15lenardrubinCPNIprivacy.pdf.

new framework proposed in the Report. Although the Report repeatedly asserts that this new framework "builds upon" the traditional Commission law enforcement model (*see* Report at v, 38-39, 40), it in fact would replace that model. To be sure, many, if not most, privacy policy disclosures are prolix and incomprehensible. But the appropriate remedy for opacity is to require notices to be clear, conspicuous and effective. If a consumer is provided with clear and conspicuous notice prior to the collection of information, there is no basis for concluding that a consumer cannot generally make an informed choice.[7] In addition, to the extent that the Commission has used a "harm" model based on the potential for physical or financial harm, or intangible harm constituting a violation of a special statute, that model may be a useful and legitimate framework.[8] However, the Commission could overstep its bounds if it were to begin considering "reputational harm" or "the fear of being monitored" or "other intangible privacy interests" (*see* Report at iii, 20, 31), generally when analyzing consumer injury. The Commission has specifically advised Congress that absent deception, it will not ordinarily enforce Section 5 against alleged intangible harm.[9]

---

[7] The Report asserts there has been an "enormous growth in data processing and storage capabilities" (*see* Report at 24), and that there has been a proliferation of affiliates, information brokers and other information aggregators. *See* Report at 21, 23-24, 45-46, 68. But the Report does not explain how or why this phenomenon cannot be addressed by clear and conspicuous disclosures to consumers that their information may be aggregated in that fashion.

[8] The Commission has challenged practices threatening physical harm under Section 5 of the FTC Act. *See Int'l Harvester Co.*, 104 F.T.C. 949 (1984). Moreover, it has challenged practices threatening intangible harm under special statutes enacted by Congress, specifically the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act, and the Do Not Call amendments to the Telemarketing Sales Rule. *See* Report at 10-12. However, the Commission has not challenged practices threatening intangible harm under Section 5.

[9] Letter from the Federal Trade Commission to Hon. Wendell Ford and Hon. John Danforth, Committee on Commerce, Science and Transportation, United States Senate,

Third, as stated, the Report takes the position that an opt-in requirement may be triggered whenever there is a "material" change in the handling of the "other" information, including the sharing of non-sensitive information like behavioral tracking information, with third parties. *See* Report at 75-76. The Report is ambiguous as to whether this requirement would apply no matter how clear and conspicuous the disclosure of the prospect of material change was. *Compare* Report at 15, 75-76 *with* Report at 39, 76. Arguably, there is no warrant for requiring more than an opt-out requirement if that was what was initially required, when the disclosure of the material change and the ability to opt out is made clearly and conspicuously and the consumer actually receives the disclosure.

Fourth, insofar as the Report could be read as suggesting a ban on "take it or leave it" options (*see* Report at 60), again, clear and conspicuous disclosure is the most appropriate way to deal with such an option. I question whether such a ban would be constitutional and am also concerned about the impact of a ban on innovation.

Finally, if the traditional "notice" law enforcement model is to be augmented by some "choice" mechanism, I continue to have many questions about the proper implemantation of a Do Not Track concept. The root problem with the concept of "Do Not Track" is that we, and with respect, the Congress, do not know enough about most tracking to determine how to achieve the five attributes identified in today's Commission testimony, or even whether those attributes can be achieved.[10] Considered in a vacuum, the proposed Do Not Track attributes set

---

Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction, *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

[10] As described in today's and prior testimony, the five attributes are:

First, any Do Not Track system should be implemented universally, so that consumers do not

forth in today's testimony can be considered innocuous, indeed even beneficial. However, the concept of Do Not Track cannot be considered in a vacuum. The promulgation of five attributes, standing alone, untethered to actual business practices and consumer preferences, and not evaluated in light of their impact upon innovation or the Internet economy, is irresponsible. I therefore respectfully dissent to the portions of the testimony that discuss and describe certain conclusions about the concept of Do Not Track.[11]

It is easy to attack practices that threaten data security. There is a consensus in both the United States and Europe that those practices are pernicious, and the Commission has successfully challenged them.[12] It is also easy to attack practices that compromise certain personally identifiable information ("PII") like one's social security number, confidential

---

have to repeatedly opt out of tracking on different sites. Second, the choice mechanism should be easy to find, easy to understand, and easy to use. Third, any choices offered should be persistent and should not be deleted if, for example, consumers clear their cookies or update their browsers. Fourth, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes. Finally, an effective Do Not Track system would go beyond simply opting consumers out of receiving targeted advertisements; it would opt them out of collection of behavioral data for all purposes other than product and service fulfillment and other commonly accepted practices.

[11] The concept of Do Not Track was presented in the preliminary Staff Privacy Report, issued in December 2010. *See* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. At that time, the Commission requested public comment on the issues raised in that preliminary report.

[12] *See, e.g., Lookout Servs., Inc.*, FTC File No. 1023076 (June 15, 2011) (consent order) (alleging failure to reasonably and appropriately secure employees' and customers' personal information, collected and maintained in an online database); *CVS Caremark Corp.*, FTC File No. 0723119 (June 18, 2009) (consent order) (alleging failure to implement reasonable policies and procedures for secure disposal of personal information); *BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005) (consent order) (alleging failure to take reasonable and appropriate security measures to protect sensitive consumer financial information with respect to credit and debit card purchases); *Eli Lilly and Co.*, FTC File No. 0123214 (May 8, 2002) (consent order) (alleging failure to provide appropriate training for employees regarding consumer privacy and information security).

financial or health data, or other sensitive information, such as that respecting children. The consensus about those practices in the United States is reflected in federal statutes like the Health Insurance Portability and Accountability Act ("HIPAA"), the Gramm-Leach-Bliley Act ("GLBA"), and the Children's Online Privacy Protection Act ("COPPA"), and the Commission has likewise successfully challenged practices that violate those statutes.[13] On the other hand, some of the "tracking" that occurs routinely is benign, such as tracking to ensure against advertisement repetition and other tracking activities that are essential to ensuring the smooth operation of websites and internet browsing. But we do not know enough about other kinds of "tracking" – or what consumers think about it – to reach any conclusions about whether most consumers consider it good, bad or are indifferent.

More specifically, it is premature to endorse any particular browser's Do Not Track mechanism. One type of browser mechanism proposed to implement Do Not Track involves the use of "white lists" and "black lists" to allow consumers to pick and choose which advertising networks they will allow to track them.[14] These lists are furnished by interested third parties in order to prevent the types of tracking that consumers supposedly do not want.[15] It is clear from

---

[13] *Rite Aid Corp.*, FTC File No. 0723121 (Nov. 12, 2010) (consent order) (in conjunction with HHS; alleging failure to establish policies and procedures for the secure disposal of consumers' sensitive health information) (HIPAA); *SettlementOne Credit Corp.*, FTC File No. 0823208 (Feb 9, 2011) (proposed consent agreement) (alleging that credit report reseller failed to implement reasonable safeguards to control risks to sensitive consumer information) (GLBA); *United States v. Playdom, Inc.*, Case No. SACV 11-0724-AG(ANx) (C.D. Cal. May 24, 2011) (consent order) (alleging failure to provide notice and obtain consent from parents before collecting, using, and disclosing children's personal information) (COPPA).

[14] Many, if not all, browsers currently allow consumers to customize their browser to prevent the installation of, or delete already installed, cookies that are used for tracking.

[15] Some Tracking Protection Lists (TPLs) allow any criterion to be used to decide which sites go on a TPL and which do not. In some cases, consumers may have the option to create

these "lists" what the interested third parties think about the tracking on the lists (or not on the lists). However, it is not clear whether most consumers share those views, or even understand the basis upon which the "list" was created. Another proposed browser Do Not Track mechanism operates by sending a Do Not Track header as consumers surf the Internet. This mechanism would only eliminate tracking to the extent that the entities receiving the Do Not Track header understand and respect that choice. Theoretically at least, this mechanism could block all tracking if it does not offer customization and preserve the ability to customize.[16] This is important because there may be some tracking that consumers find beneficial and wish to retain.

Beyond that, consumers (including consumers that are surveyed by interested third parties) are generally not fully informed about the consequences – both bad and good – of subscribing to a Do Not Track mechanism.[17] They are not always told, for example, that they may lose content (including advertising) that is most pertinent and relevant to them. Neither are they told that they may lose free content (that is paid for by advertising). Nor are they told that subscribing to a Do Not Track mechanism may result in more obtrusive advertising or in the loss of the chance to "sell" the history of their internet activity to interested third parties. Indeed,

---

their own TPL. However, as discussed below, neither the FTC, nor consumer advocates, nor consumers themselves, know enough about the tracking, collection, retention and sharing practices of online entities.

[16] In addition, it is not clear how the "recipient" of the Do Not Track header would respond to such a request when the consumer has otherwise indicated that he or she wishes to have the recipient customize the consumer's experience.

[17] That is not to say that current technology cannot facilitate these disclosures. However, it is critical that advertisers and publishers take the opportunity to explain to consumers what their practices are and why they might be beneficial.

they are not even generally told what kinds of tracking are going to be eliminated. On the other hand, consumers are not told that tracking may facilitate the compilation of a consumer "profile" through the aggregation of information by third parties to whom it is sold or with whom it is shared (such as insurance companies engaged in "rating" consumers). One reason that consumers are not told about the latter consequence is that we do not know enough about what information is being collected and sold to third parties to know the extent to which such aggregation is occurring.

One thing is certain though: consumers cannot expect simply to "register" for a Do Not Track mechanism as they now register for "Do Not Call."[18] That is because a consumer registering for Do Not Call needs to furnish only his or her phone number. In the context of the Do Not Call program, each telephone already has a unique identifier in the form of a telephone number. In contrast, there is no such persistent identifier for computers. For example, Internet Protocol ("IP") addresses can and do change frequently. In this context, creating a persistent identifier, and then submitting it to a centralized database, would raise significant privacy issues.[19] Thus, information respecting the particular computer involved is essential, and that kind of information cannot be furnished without compromising the very confidential information that consumers supposedly do not want to share. In addition, multiple users of the same

---

[18] *See* Prepared Statement of the Federal Trade Commission on Do Not Track Before the House Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection, Dec. 2, 2010, *available at* http://www.ftc.gov/os/testimony/101202donottrack.pdf.

[19] A new identifier would be yet another piece of PII that companies could use to gather data about individual consumers.

computer or device may have different preferences, and tying a broad Do Not Track mechanism to a particular computer or device does not take that into consideration.

This is not to say that a Do Not Track mechanism is not feasible. It is to say that we must gather competent and reliable evidence about what kind of tracking is occurring before we embrace any particular mechanism. We must also gather reliable evidence about the practices most consumers are concerned about. Nor is it to say that it is impossible to gather that evidence. The Commission currently knows the identities of several hundred ad networks representing more than 90 percent of those entities engaged in the gathering and sharing of tracking information. It is possible to serve those networks with compulsory process, which means that the questions about their information practices (collection, tracking, retention and sharing) must be answered under oath. That would enable the Commission to determine and report the kinds of information practices that are most frequently occurring. Consumers could then access more complete and reliable information about the consequences of information collection, tracking, retention and sharing. Additionally, the Commission could either furnish, or, depending on technical changes that may occur, facilitate the furnishing of, more complete and accurate "lists" and consumers would then have the ability to make informed choices about the collection, tracking, retention and sharing practices they would or would not permit.

This course is not perfect. For one thing, it would take time to gather this information. For another thing, it would involve some expense and burden for responding parties (though no more than that to which food and alcohol advertisers who currently must answer such questionnaires are exposed). Consumers would also be obliged to avail themselves of the information provided by the Commission. But I respectfully submit that this course is superior to acting blindly, which is what I fear we are doing now.

CONCLUSION

To the extent we have exercised our authority under Section 5, the "notice" model for privacy law enforcement has served this Commission long and well. Not only is there no warrant for discarding it now in favor of a proposed new framework that is as yet theoretical and untested, but in my judgment it would also be bad public policy to do so. To the contrary, if there is anything wrong with the "notice" model, it is that we do not enforce it stringently enough. Moreover, as the Bureau of Consumer Protection concedes, there are many benefits to the sharing of non-sensitive consumer information, and they may be endangered by the aspirational proposals advanced in the Report, however hortatory they may be.

Mrs. BONO MACK. And I would like to thank my colleagues for their participation today. I would like to thank the ranking members on both subcommittees as well as Chairman Walden. I would like to wish Joe Barton good luck tonight in the congressional baseball game and remind you all to attend if you are interested and remind members that they have 10 business days to submit questions for the record. I ask witnesses to please respond promptly to any questions they receive. And again, I thank our panelists very much for your time today. And the hearing is now adjourned.

[Whereupon, at 1:33 p.m., the subcommittees were adjourned.]

[Material submitted for inclusion in the record follows:]

Statement of Rep. Ed Towns (NY-10)
Before the US House of Representatives
Energy and Commerce Committee
Joint Hearing

"Internet Privacy: The Views of the FTC, the FCC, and NTIA"

Thursday July 14th, 2011

I want to thank Chairman Walden and Chairman Bono-Mack along with Ranking Members Eshoo and Butterfield for holding this hearing today on "Internet Privacy" which has become a growing concern among many Americans. The issue of internet privacy has become a top priority for many Americans who engage in online social networking and e-commerce. Over the past several years data brokers have collected a vast amount of information about consumers for commercial use. While I understand that most businesses use reasonable collection methods to obtain consumer information, questions still remain about individual privacy safeguards.

It is my hope that this hearing will shed light on what initiatives the Federal Government has undertaken to protect the privacy of children and other consumers from potential fraudulent activity. I am very interested in hearing how each respective agency with jurisdiction over internet privacy is handling this growing concern among American consumers.

This committee must commit itself to providing consumers more transparency on how companies are using the information they obtain. We must also examine whether current regulations are sufficient enough to safeguard individual privacy on the internet and whether industry officials are properly self regulating to protect consumer information.

Since the advent of the internet the FTC, FCC and NTIA have been tasked with the regulation of internet policy. Under the FTC's leadership several steps have been taken to address the issue of internet policy through roundtable discussions, educational workshops and reports that highlight the need for increased consumer privacy in

an era that has undergone rapid change. Consumers and Industry are both seeking a coordinated policy that reflects both the desire to offer new and exciting options for customers while respecting basic expectations of privacy and transparency. This hearing is an important first step in making sure that congress and the relevant agencies work together to craft a framework that takes all viewpoints into account.

Thank you, I yield back my time.

Responses to Questions for the Record to Commissioner Ramirez
July 14, 2011 "Internet Privacy: The Views of the FTC, the FCC, and NTIA" Hearing

Responses to Questions for the Record from Ranking Member G.K. Butterfield

1. **Section 5(9) of H.R. 2577, the Secure and Fortify Electronic Data Act ("SAFE Data Act"), defines a "service provider" as "a person that provides electronic data transmission, routing, intermediate and transient storage, or connections to its system or network, where the person providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and does not differentiate personal information from other information that such person transmits, routes, or stores, or for which such person provides connections."**

   Section 2(c) exempts a "service provider" from the data security requirements in the bill. Section 3(b)(2) requires a "service provider" that becomes aware of a breach of security of data in electronic form containing personal information that is owned or possessed by another person engaged in interstate commerce that connects to or uses the service provider's system or network to transmit, route or intermediately or transiently store that data in connection with that commercial activity to notify: (1) law enforcement, and (2) the person that initiated the connection, transmission, routing, or storage, if that person can reasonably be identified.

   a. **Do you believe that a direct-to-consumer cloud provider could argue that it is a "service provider," and therefore not obligated to meet the data security requirements in the bill? Please explain why or why not.**

      A direct-to-consumer cloud provider might argue that it is a "service provider," as currently defined in the bill, and, as such, that it is exempt from the bill's data security requirements. For example, a cloud-based email provider may contend that it provides electronic data transmission, does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and does not differentiate personal information from other information that it transmits. At the same time, a strong counter-argument could be made that a direct-to-consumer cloud provider does not fall within the service provider exemption because it: (1) is actually providing permanent rather than "intermediate and transient storage," and (2) is not providing the service to a "third party" but rather to the very individual who engaged the provider for such service. Direct-to-consumer cloud providers, such as e-mail providers, often have highly sensitive information including passwords and financial information. In addition, technology is evolving in such a way that increasing amounts of personal information are stored in the cloud. It is therefore critical to ensure that cloud-based providers are covered by the bill.

   b. **Do you believe the definition of "service provider," as drafted, is overly broad? If so, what types of direct-to-consumer Internet services, cloud or otherwise, could exploit the definition to skirt the bill's data security requirements? In addition,**

please provide any comments, guidance or legislative language that would narrow the definition to what you believe is a more appropriate scope.

Yes, I am concerned that many existing types of cloud-based providers might argue that they satisfy the definition of "service provider," including, for example, email providers and storage providers that enable consumers to store documents, photos, and other content in the cloud. As more companies move to the cloud, they may argue that the exception applies to new types of cloud models that may develop. Other Internet-based businesses, such as email providers that transmit but do not store information, may make similar arguments. To avoid any potential ambiguity about the scope of protection afforded to consumers, the bill should explicitly cover direct-to-consumer cloud providers.

c. Assuming that a direct-to-consumer cloud provider is NOT a "service provider":

i. Do you believe such a provider could nonetheless argue that it is not obligated to meet the data security or breach notification requirements in the bill because the provider generally does not know the contents of data in its custody, and in particular whether that data contains "personal information," as defined in the bill? Please explain.

Direct-to-consumer cloud providers may well argue in an investigation or litigation that, because they do not know the specific content of the information put in the cloud, they cannot be held responsible for "owning or possessing" personal information under the bill. Moreover, they may claim that, without knowing whether the cloud contains personal information or its nature, they cannot develop reasonable data security procedures tailored to the nature of that information. Given consumers' increasing use of cloud providers to store information, including sensitive data, it is important that cloud providers take reasonable measures to secure consumer data and inform them if there is a breach, regardless of whether the provider knows which types of data have been accessed. To foreclose such arguments, the bill could include a presumption that entities that provide data storage services to individuals own or possess data containing personal information and are therefore subject to the bill's requirements.

ii. Do you believe such a provider could argue that it does not "own or possess" the data containing personal information as required for the bill to apply? Please explain.

Under the bill as currently drafted, direct-to-consumer cloud providers may argue they are not subject to the bill's data security requirements regardless of whether they know that the information that consumers put in the cloud contains personal information. This is because the bill applies to entities engaged in commerce that own or possess data containing personal information "related to that commercial activity." Cloud providers might argue that the information placed in the cloud by

consumers is not "related to that commercial activity" of providing the cloud service itself. To avoid potential ambiguity about the scope of protection afforded to consumers, the bill should explicitly cover direct-to-consumer cloud providers.

d. Do you believe direct-to-consumer cloud providers should be more clearly brought within the scope of the bill, regardless of their awareness of the contents of the data in their custody? Please explain why or why not. If so, please also provide comments, guidance or legislative language to bring such services within the bill's reach.

Yes. I believe that all companies that hold sensitive consumer data – including direct-to-consumer cloud providers – should be required to take reasonable measures to safeguard such information. If cloud providers fail to maintain reasonable security, consumers could lose trust in the electronic marketplace. As noted above, one way to ensure that cloud providers are covered by the scope of the bill is to include a provision stating that if any person provides data storage services to individuals, there shall be a presumption that such person owns or possesses data containing personal information and they are subject to the bill.

2. I understand that the FTC has brought enforcement actions against 36 companies under its Federal Trade Commission Act (FTCA) authority to prevent "unfair or deceptive acts or practices in or affecting commerce" for their failure to adequately secure consumers' personal information. H.R. 2577 would provide FTC with a specific grant of authority to pursue data security cases and to seek civil penalties.

Among the types of personal information these 36 companies failed to adequately protect were: payroll information, employer histories, health information, mortgage information, email addresses, income histories, book and music purchase histories, and tax returns. H.R. 2577 only requires that businesses secure an individual's name, or address, or phone number, *IN COMBINATION WITH* an identifying number such as Social Security number or driver's license number; or a financial account number *WITH* any required security code or password.

a. Do you believe that FTC's authority to bring some of these 36 cases would have been limited had H.R. 2577 - as reported by the Subcommittee on Commerce, Manufacturing, and Trade on July 20, 2011 - been law? If so, how many of these cases and/or claims within cases would FTC have been prevented from pursuing? Please briefly describe those cases and why FTC would have been unable to pursue and bring them to a close. Also, please discuss why you believe those were important cases for FTC to be able to pursue.

The majority of the FTC's 36 data security enforcement actions involved types of personal information that would fall, or arguably fall, outside the bill as currently drafted. Although the bill does not explicitly limit the FTC Act's applicability to data security, and the FTC would continue to bring cases under Section 5 of the FTC Act, I am concerned that a court might interpret the bill as implicitly limiting the FTC Act's scope

due to the bill's narrow definition of "personal information." Twenty-two of the Commission's data security cases involved some types of information that would not be covered under the bill's current definition of personal information. While some of these cases involved financial information such as Social Security numbers ("SSNs") that are included in the definition of personal information, such information was not always kept in databases together with identifying information and thus would not be covered under the personal information definition. SSNs or account numbers alone can be used for identity theft and fraud, even when not combined with other information. In addition, a number of our data security cases involved "consumer reports," as defined in the Fair Credit Reporting Act. While some consumer reports, particularly credit reports, contain SSNs and thus would be considered personal information if not truncated, other types of consumer reports such as check cashing reports, landlord rental histories, and the like may not contain SSNs or account numbers and would not be deemed personal information under the bill's current definition.

The definition of "personal information" also does not include health information, even though breaches of health information can cause harm. In both the *CVS* and the *Rite Aid* cases (*available at* http://www.ftc.gov/os/caselist/0723119/index.shtm and http://www.ftc.gov/os/caselist/0723121/index.shtm), the Commission charged that pill bottles and other prescription information were left in open dumpsters, potentially revealing consumers' sensitive medical conditions and prescriptions. One of the Commission's very first data security cases was against Eli Lilly and Company (*available at* http://www.ftc.gov/os/caselist/0123214/0123214.shtm). In that case, the Commission charged that the company failed to train its employees, one of whom sent a blast email revealing the names of people who were on Prozac. I think many consumers would find these types of breaches of their medications and medical conditions harmful and would want this data to be protected from exposure.

There are also other types of sensitive data not included in the bill's definition of "personal information" that should be protected. The definition, for instance, does not include geolocation data or information such as user name and password that can be used to access an account. Account access information such as user name and password is sensitive information and should be protected, especially since passwords are frequently reused across many websites. Breach of location information can result in physical harm.

Accordingly, in order to ensure that sensitive consumer data is appropriately protected, I recommend that the definition of "personal information" include the following information that is sensitive in nature:

(i) Social Security number.

(ii) Driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity.

(iii) Financial account number, credit or debit card number, or any required security code, access code, or password that is necessary to permit access to an individual's financial account.

(iv) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation.

(v) Information that could be used to access an individual's account, such as user name and password or email address and password.

(vi) An individual's first and last name, first initial and last name, or other unique identifier in combination with:

(1) the individual's month, day, and year of birth or mother's maiden name.

(2) the individual's precise geolocation.

(3) information that relates to the individual's past, present or future physical or mental health or condition, or to the provision of health care to the individual.

(4) the individual's non-public communications or other user-created content such as emails or photographs.

b. Given the choice between continuing to pursue data security cases under its current FTCA authority or under H.R. 2577, as reported by the Subcommittee on July 20, which would be more preferable to FTC and why?

In prior testimony, the Commission has announced its support for legislation requiring all companies that hold sensitive consumer data – not just companies within the FTC's jurisdiction – to take reasonable measures to safeguard it and to notify consumers when the security of their information is breached. Under current federal law, many businesses outside FTC jurisdiction have no obligation to secure the consumer information they maintain, and the vast majority of businesses are not required to give notice of a breach. Legislation would also give the Commission authority to seek civil penalties in data security cases, which would increase the deterrent value of our orders, as equitable remedies such as disgorgement and redress are often inadequate in these cases. However, the Commission already has a robust data security program, requiring companies to implement reasonable and appropriate measures to protect sensitive consumer data. In my view, it is critical that new legislation not potentially narrow the scope of the Commission's existing program, either expressly or by implication. In particular I am concerned that the definition of "personal information" does not include sensitive data, such as SSNs and financial account numbers alone, health information, and geolocation data, emails or user names and passwords, the release of which could result in significant consumer harm. In order to ensure that sensitive consumer data is appropriately

protected both under this legislation and the FTC Act, I believe the scope of this definition should be expanded to include the types of information discussed above. I look forward to working with members of Congress on this and other issues.

Responses to Questions for the Record from Rep. Joe Barton

1. **I'm troubled by the fact that the FTC - the principal federal agency charged with protecting consumers - accepted nothing more than verbal assurances of improved behavior from a company with a very spotty track record of protecting consumer privacy. When it comes to protecting privacy, I don't think verbal reassurances cut it, especially when there's a clearly established pattern of violating privacy.**

   Of course I'm referring to the manner in which the FTC handled the unprecedented privacy breach that resulted when Google utilized its Street View mapping service to amass an unthinkable volume of private, personal information about consumers. This debacle became known as SpyFi.

   On June 19, 2009, Nicole Wong, Deputy General Counsel for Google, testified before this committee and stated "Because user trust is so critical to us, we've ensured that privacy considerations are deeply embedded in our culture ... For example, our team ... works ... from the beginning of product development to ensure that our products protect our users' privacy." I ask to enter into the hearing record her testimony from that June 19, 2009.

   Yet, in May 2010, almost 12 months after Mrs. Wong testified to our Committee that privacy is "deeply embedded" into Google's culture, it became clear that SpyFi was occurring at the same time she testified. Her verbal reassurances to this Committee were clearly inadequate. Moreover, one thing that is not tolerated by our Committee - regardless of which party occupies the chairman's seat - is being deceived by the witnesses that we call to testify. Now, I'm not saying that Ms. Wong deliberately misled us when she testified here in 2009, but one thing is clear: her testimony has since been directly contradicted by internal actions her company was taking at the time she testified.

   For these reasons, I want to know why you settled only for Google's verbal assurances that it would hire another director of privacy, provide privacy training for engineers, and add a privacy review process for products. I request that the FTC's letter dated October 27, 2010, which outlines the FTC's bases for closing its SpyFi investigation, also be entered into the record.

   Google's data collection through its Street View vehicles involved the invisible and massive collection of consumer data without consent – including data that was personally identifiable. I am unquestionably concerned about the collection of private consumer information without consent.

In light of what transpired, Commission staff conducted a thorough investigation of Google's conduct to determine whether Google violated any law enforced by the FTC and specifically Section 5 of the FTC Act, our principal statutory authority, which prohibits deceptive or unfair acts or practices in or affecting commerce. Under Section 5, a representation or omission is deceptive if it contains a misrepresentation or omission that is likely to mislead consumers acting reasonably under the circumstances to their detriment. Deceptive claims or omissions are actionable if they are material, *i.e.*, they would affect a consumer's decision or conduct with respect to a product or service. An act or practice is unfair if it causes or is likely to cause substantial consumer injury that is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition.

Following our review of the evidence obtained in our investigation into this matter and after receiving a commitment from Google that there would be no recurrence of this episode, we determined to close the investigation. As noted in a letter from Bureau Director David Vladeck sent to Google on October 27, 2010, which is available on the FTC's website (*available at* http://www.ftc.gov/os/closings/101027googleletter.pdf), Google confirmed that it had not used the payload data (*i.e.*, contents of communications over unsecured wireless networks) obtained from its Street View cars in any Google product or service. In addition, FTC staff received significant commitments from Google that it would not do so in the future and would delete the data as soon as possible. Moreover, at our urging, Google implemented a number of measures to prevent privacy violations in the future. Many of these measures build privacy into product development and ensure that Google engineers and managers receive core privacy training. These measures are summarized in Mr. Vladeck's letter.

Although I cannot provide any more detail concerning the investigation of Google Street View, I would like to note that in March the Commission announced a major enforcement action against Google arising from the February 2010 launch of its Buzz social network (*available at* http://www.ftc.gov/os/caselist/1023136/index.shtm). The proposed Google Buzz order, among other things, prohibits Google from misrepresenting the extent to which it maintains and protects the privacy and confidentiality of information from or about consumers. The order also requires the company to institute a comprehensive privacy program for all information Google collects from or about an individual in connection with any of Google's many products or services – including the types of WiFi communications collected by its Street View vehicles – and to obtain independent audits of that privacy program on a biennial basis for 20 years. I believe that, as a result of the Google Buzz order, Google is required to provide meaningful privacy protection for all consumers from whom it collects information.

2. **I recently introduced H.R. 1895, the Do Not Track Kids Act of 2011 with Mr. Markey. Has your agency taken a position on this bill? If so, what is your position?**

Although the Commission has not taken a position on general privacy or Do Not

Track legislation, in my view legislation introduced to date, including the Do Not Track Kids Act of 2011, represents significant progress in addressing important privacy concerns while ensuring continued robust development and growth of new services. I support the fundamental goal of this piece of legislation – to provide privacy protections for children and teens.

FEDERAL COMMUNICATIONS COMMISSION

JULIUS GENACHOWSKI
CHAIRMAN

September 15, 2011

The Honorable Mary Bono Mack
Chairwoman
Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairwoman Bono Mack:

Attached please find my responses to the additional post-hearing questions from my appearance before the Committee on July 14, 2011. Please let me know if I can be of further assistance.

Sincerely,

Julius Genachowski

The Honorable Joe Barton

1. **I recently introduced H.R. 1895, the Do Not Track Kids Act of 2011 with Mr. Markey. Has your agency taken a position on this bill? If so, what is your position?**

   Response: Although the FCC has not taken a position on H.R. 1895 specifically, the FCC in general supports efforts to educate children about safe behaviors while online and to protect them from the potential misuse of their online profiles. A recent example of the FCC's efforts in this area is the *Back to School in the Digital World* forum hosted by the agency on September 8, 2011, to discuss the opportunities and challenges around technology use by adolescents.

The Honorable G.K. Butterfield

1. **Section 631(c)(1) of the Communications Act of 1934 requires that cable operators "take such actions as are necessary to prevent unauthorized access to [personally identifiable information concerning any subscriber] by a person other than the subscriber or cable operator." This provision is generally understood to create an obligation on cable operators to secure the personally identifiable information ("PII") of their subscribers. Given that the term "personally identifiable information" is not defined in the Act, I would like you to clarify the data security protection requirements that apply to cable operators.**

   a. **Please list (and to the extent it might be helpful, describe) the types of PII that cable operators are expected to protect.**

      Response: As your question indicates, the Communications Act does not provide a specific definition of the term "personally identifiable information" under Section 631, nor has the FCC had occasion to define the scope of that term in a proceeding. In an Attachment to this submission, I have included an analysis from the FCC's General Counsel regarding the meaning of that phrase in the context of the Communications Act.

   b. **I understand that the FCC has not provided any guidance or issued any rules regarding the meaning of PII. Is it your understanding or belief that cable operators know they are obligated to protect each type of PII listed in response to the above question and that they are in fact doing so? What is the basis for this understanding or belief?**

      Response: Section 631 of the Communications Act has been in effect for more than two decades, during which time cable operators have had the opportunity to develop an understanding of their responsibilities to protect personally identifiable information and to monitor and update their data security practices to protect such information. The paucity of complaints to the FCC about the privacy practices of cable operators and the

dearth of court cases enforcing subscribers' private right of action under Section 631(f) support the notion that cable operators in general are meeting their statutory obligations.

The FCC is committed to remaining vigilant in ensuring that cable subscribers' privacy is protected. The FCC has an internal privacy working group that has met with cable operators and other industry participants over the last year to discuss the industry's privacy and data security practices. Cable operators have informed staff that they have implemented data security practices designed to protect the personally identifiable information of their subscribers as required by Section 631 of the Communications Act.

c. H.R. 2577, the Secure and Fortify Electronic Data Act ("SAFE Data Act"), requires that businesses secure an individual's name, or address, or phone number, *IN COMBINATION WITH* an identifying number such as Social Security number or driver's license number; or a financial account number *WITH* any required security code or password.

i. Please compare the list of personal information that must be secured under H.R. 2577 with the list of PII that must be secured under Section 631(c)(1) of the Communications Act and briefly describe the differences.

Response: The categories of personal information protected under the SAFE Data Act appear to be narrower that the personally identifiable information cable operators are required to protect pursuant to Section 631(c)(1) of the Communications Act. As discussed in the attachment, the statute and legislative history of Section 631 demonstrate that in enacting Section 631, Congress was focused on protecting information about subscribers' viewing habits or patterns and transactions conducted by subscribers over the cable system, information that is uniquely available to cable operators by virtue of their operation of the network. The SAFE Data Act's definition of personal information does not include types of personally identifiable information that Congress sought to protect under Section 631, such as when the subscriber used the services provided by the cable operator and for how long, any pay-per-view or premium purchases made by the subscriber over the cable system, and information about other transactions made by the subscriber over the cable system. The bill also would not protect information about customers' Internet usage.

ii. H.R. 2577 deletes Section 631(c)(1) from the Communications Act, with the anticipated effect of bringing cable operators under the jurisdiction of the FTC for the purposes of data security and breach notification requirements. Please describe any concerns you may have regarding gaps in the types of information that would be required to be protected if H.R. 2577 were to be enacted into law, compared to what is required to be protected under current law.

Response: As discussed above, the definition of personal information in H.R. 2577 does not include information that is uniquely available to cable operators by virtue of their operation of the network, such as information about subscribers' viewing habits or

patterns and transactions conducted by the subscriber over the cable system. Because cable operators understand that such data is included within the scope of personally identifiable information protected by Section 631(c)(1) of the Communications Act, H.R. 2577's elimination of that paragraph would create a new gap, leaving unprotected some types of private information that now is protected by law.

iii. Would you have any other concerns about putting cable operators under the jurisdiction of the FTC for the purpose of enforcing data security and breach notification requirements and eliminating the FCC's authority in this area? Please explain.

Response: The FCC and the FTC both play important roles in the protection of consumer privacy. While the FTC has authority to protect consumers from unfair and deceptive acts and practices, including in the area of privacy and data security, the FCC is uniquely qualified to monitor and oversee the privacy and information security practices of communications providers, including cable operators in the operation of their networks. The FCC is the expert agency responsible for the communications sector, and in that capacity has developed experience and expertise in the operations of communications networks that it brings to bear in monitoring privacy and data security practices on those networks. If the FCC's authority were eliminated in this area of growing concern, consumers would lose the benefit of the FCC's expertise in the communications sector.

2. **Under Section 222 of the Communications Act of 1934, customer proprietary network information (CPNI) must be protected. CPNI includes the time, date, duration, and destination number of each call, the type of network a consumer subscribes to, and any other information that appears on the consumer's telephone bill.**

   a. **H.R. 2577 deletes Section 631(c)(1) of the Communications Act, which requires cable operators "to prevent unauthorized access to [personally identifiable information] by a person other than the subscriber or cable operator." Cable operators would instead have to comply with H.R. 2577's security requirements. Please discuss whether and how data security requirements would be different for telecommunications carriers (as covered under Section 222 of the Communications Act of 1934) and for cable operators (if covered under H.R. 2577).**

   Response: Section 222 of the Communications Act, 47 U.S.C. § 222, and the FCC's rules implementing that section, 47 C.F.R. §§ 64.2001-2011 (the "CPNI rules"), require telecommunications carriers to protect customer proprietary network information (CPNI). CPNI includes "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by a customer of a telecommunications service, and that is made available to the carrier solely by virtue of the carrier-customer relationship" and information contained in customers' telephone bills except for subscriber list information. *See* 47 U.S.C. § 222(h)(1). Under Section 222 of the Communications Act and the FCC's CPNI rules, telecommunications carriers and interconnected Voice over Internet Protocol (VoIP) providers are required to protect and secure such data.

If cable operators are subject to the data security provisions of H.R. 2577, and are not subject to any other data security requirements, then cable operators' obligation to protect personal information would extend only to the information covered by H.R. 2577. As the bill is currently drafted, this includes only an individual's first name or initial and last name, or address, or phone number, in combination with that individual's Social Security number; driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity; or financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account.

b. Cable operators and telecommunications carriers are seen as competitors; both can provide network connections for telephone or voice, Internet, and television. Should cable operators and telecommunications carriers be required to comply with the same data security requirements?

Response: Legislative enactments over the last several decades have opened communications networks to competition and encouraged regulatory parity. Congress sought to open video markets to competition in the Cable Television Consumer Protection and Competition Act of 1992, and later sought to open telecommunications markets to competition in the Telecommunications Act of 1996. Congress thus created a regulatory regime that encouraged competition among communications providers while recognizing the different methodologies for delivering services to consumers and allowed for flexibility to account for these differences. One result has been an interconnected system of obligations on communications providers depending on the type of service provided. Thus, if cable operators provide telecommunications or interconnected VoIP services, Section 222 of the Act applies, and if telecommunications operators provide cable services, Section 631 of the Act applies. In this case, the same data security requirements apply to all providers.

3. Section 2(c) of H.R. 2577 exempts a "service provider" from data security requirements in the bill. Section 5(9) defines a "service provider" as "a person that provides electronic data transmission, routing, intermediate and transient storage, or connections to its system or network, where the person providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and does not differentiate personal information from other information that such person transmits, routes, or stores, or for which such person provides connections."

This "service provider" exemption was written to remove internet service providers (ISPs) from the bill's data security requirements.

a. At the hearing, when asked whether "the FCC has authority over ISPs to ensure proprietary network information of Internet customers is not being sold to third

parties," you responded that "this is an area where clarification would be very helpful, and in the absence of it, there is a gap."

i. Does this also mean that the FCC does not currently have clear authority to enforce data security requirements for ISPs? If this authority does not exist, do you support H.R. 2577 covering ISPs? Please explain why or why not.

Response: I believe that the best reading of Section 631 of the Communications Act is that the Internet access services offered over cable networks are covered by the requirements of that section. *See Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d)*, 157 F. Supp. 2d 286, 291 (S.D.N.Y. 2001). Likewise, to the extent that telecommunications carriers offer Internet access services on a common carrier basis, those services are covered by Section 222. However, to the extent that ISPs are not entities covered by those sections of the Communications Act, the data security requirements contained therein would not be applicable to those ISPs, and the FCC would been severely limited in its ability to enforce data security requirements against those entities. ISPs have access to the personal information of their subscribers, and therefore should be under some statutory obligation to provide protection to that information.

ii. If you do not support covering ISPs in H.R. 2577, please provide any comments, guidance or legislative language to ensure that ISPs are required to meet some minimum data security requirements.

Response: See above.

b. Do cable operators currently have a general obligation (e.g. when acting as a "dumb pipe") to secure and protect their transmission lines against unauthorized access? If so, what is the basis for this obligation? For example, is Section 631(c)(1) of the Communications Act the basis for this obligation?

Response: Cable operators are obligated pursuant to the language of Section 631(c)(1) of the Communications Act to "take such actions as are necessary to prevent unauthorized access to" the personally identifiable information of its subscribers, including the obligation to protect such information as it travels over the cable operators' transmission lines. Likewise, cable operators' telecommunications and interconnected VoIP services are covered by Section 222 of the Communications Act, which imposes obligations to protect subscribers' CPNI.

Furthermore, the Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001-1010 ("CALEA"), appears to impose obligations on all providers of broadband Internet access service to ensure that customers' communications cannot be intercepted illegally. *See* 47 U.S.C. § 1004; *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, First Report and Order and Further Notice of Proposed Rulemaking, FCC 05-153 (Sept. 23, 2005) (ruling that CALEA is applicable to

providers of broadband Internet access services), *aff'd American Council on Educ. v. FCC*, 451 F.3d 226 (D.C. Cir. 2006).

c. If cable operators have a general obligation (e.g. when acting as a "dumb pipe") to secure and protect their transmission lines against unauthorized access, do you believe the service provider exemption in H.R. 2577, combined with the provision deleting Section 631(c)(1) from the Communications Act, would completely eliminate this obligation for cable operators?

Response: As currently drafted, H.R. 2577 would eliminate the data security provision of Section 631(c)(1) of the Communications Act. Therefore, except to the extent their telecommunications and interconnected VoIP services are covered by Section 222 of the Communications Act, cable operators would not be subject to the current obligation to protect the security of the personally identifiable information of their subscribers. This would create a gap in the obligations of cable operators to protect personally identifiable information even if the service provider exemption in H.R. 2577 did not apply. If the service provider exemption in H.R. 2577 was found to apply to cable operators, an additional gap would be created in that cable operators would not be subject to the data protection obligations for personal information in H.R. 2577. H.R. 2577 would not affect the security obligations in CALEA, 47 U.S.C. § 1004, to secure their networks against unauthorized interceptions.

d. Do telecommunications carriers have a general obligation (e.g. when acting as a "dumb pipe") to secure and protect their transmission lines against authorized access? If so, what is the basis for this obligation?

Response: Telecommunications carriers are obligated pursuant to Section 222 of the Communications Act and the CPNI rules to secure and protect CPNI, including the obligation to protect such information as it is transmitted over the carrier's network. Furthermore, a telecommunications carrier is obligated by CALEA to "ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission." 47 U.S.C. § 1004.

e. Given that H.R. 2577 makes no changes to the Communications Act with respect to the obligations of telecommunications carriers in this area, would the authority of the FCC over them remain unchanged? Does this mean that H.R. 2577 would set up a regime where the "dumb pipes" of telecommunications carriers would be treated differently than those of cable operators? Would this concern you? Please explain.

Response: As currently drafted, H.R. 2577 does not change the FCC's authority over telecommunications carriers when they provide telecommunications services. H.R. 2577 would eliminate the portion of Section 631(c)(1) of the Communications Act that provides the FCC with authority over the data security practices of cable operators. This

would result in a gap in the FCC's authority over cable operators that does not exist under current law.

f. **Do you believe the definition of "service provider" as drafted is overly broad? If so, what types of direct-to-consumer Internet services, cloud or otherwise, could exploit the definition to skirt the bill's data security requirements? In addition, please provide any comments, guidance or legislative language to narrow the definition to what you believe is a more appropriate scope.**

Response: Congress has utilized a service provider exception in the past to protect an entity with no editorial control over the content that passes through its network from liability related to issues with the content itself. For example, the Digital Millennium Copyright Act (DMCA) creates a scheme for providing immunity to online service providers that meet certain criteria from copyright infringement liability for actions by a third party in which a service provider's network or system is utilized. *See* 17 U.S.C. § 512. Under the provisions of the DMCA, knowledge of the illegality of the content is not imputed to the online service provider just by virtue of the fact that the online service provider's network is involved in the transmission. Similarly, Section 230 of the Communications Decency Act immunizes providers of interactive computer services from liability from content created by third parties using the providers' service. *See* 47 U.S.C. § 230. In both of these statutes, Congress sought to protect providers acting essentially as passive conduits of information from liability when the information itself was problematic in some manner.

The same considerations do not support exempting service providers from all obligations to provide a basic level of security for personal information that is collected or held by an operator or is transmitted over its network. If there is a security problem with the network itself that is within the control of the network operator, the network operator should maintain responsibility.

4. **Do sections 222 and 631 of the Communications Act require telecommunications carriers and cable operators, respectively, to protect content generated when providing any of their services to subscribers, including access to television, telephone or Internet? For example, if I subscribe to the service of one of the traditional telecommunications carriers and I receive a voicemail – which is content stored by that carrier – does that information have to be secured?**

Response: As discussed above, Section 222 of the Communications Act and the CPNI rules require telecommunications carriers to protect CPNI. CPNI includes "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by a customer of a telecommunications service, and that is made available to the carrier solely by virtue of the carrier-customer relationship" and information contained in customers' telephone bills except for subscriber list information. *See* 47 U.S.C. § 222(h)(1). Congress did not include content in its definition of CPNI.

When telecommunications providers offer Internet access on a non-common carrier basis, subscriber information relating to their Internet access services is not covered by Section 222 of the Communications Act or the CPNI rules. It is important to protect consumers' privacy when it comes to Internet access services, and this gap is one of the reasons that in my oral testimony before your Committee I encouraged some updating of the Communications Act's network-oriented privacy regime to account for the advances of the digital age.

As discussed above, Section 631 of the Communications Act does not provide a comprehensive definition of personally identifiable information, nor has the FCC defined that term by rulemaking. In the Attachment, the FCC's General Counsel provides an analysis of the phrase "personally identifiable information" based on the context of the statute, the legislative history and court decisions. The General Counsel explains that there is no indication from these sources that content would be included in the definition of personally identifiable information under Section 631.

Apart from the Communications Act, the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-2522, 2701-2712, 3121-3127, provides some protection for the content of electronic communications and for subscriber information. Telephone companies and Internet service providers are considered to be providers of electronic communications services covered by ECPA. As discussed above, CALEA also provides some protections against unauthorized interception by requiring providers of telecommunications service and broadband Internet access service to secure their networks to prevent unauthorized interceptions.

5. **I understand that Voice over Internet Protocol (VoIP) services can transcribe a subscriber's voicemail messages into email and text messages, so that voicemail, email, and text message exist as written content.**

   a. **To the extent that these messages exist on a VoIP service's systems, does that information have to be secured? If so, under what statute or regulations must that information be secured?**

      Response: Providers of interconnected VoIP services are covered by the FCC's CPNI rules under Section 222.[1] Under the CPNI rules, interconnected VoIP providers have the same obligation to protect CPNI as providers of traditional telecommunications service. As discussed above, content of communications is not specifically CPNI, but to the extent a voice mail message includes call detail information such as the date, time, call duration and the phone number of the calling party that left the message, the CPNI rules cover that information.

[1] As defined in Section 9.3 of the FCC's rules, 47 C.F.R. § 9.3, an interconnected VoIP service is a service that: (1) enables real-time, two-way voice communications; (2) requires a broadband connection from the user's location; (3) requires Internet protocol-compatible customer premises equipment (CPE); and (4) permits users generally to receive calls that originate on the public switched telephone network and to terminate calls to the public switched telephone network.

Email and text messages have not traditionally received the same regulatory treatment as voice services. Email is generally considered to be an information service not covered by Section 222 of the Communications Act. The FCC has not ruled on whether text messaging is a common carrier service.

Apart from the Communications Act, the Electronic Communications Privacy Act provides some protection for the content of email and text messages, and for subscriber information relating to email and text message services.

b. Is there a difference in the level of protection required from a traditional carrier compared to that required from a VoIP provider?

Response: The FCC's CPNI rules under Section 222 require interconnected VoIP providers to provide their subscribers with the same level of protection as traditional common carriers.

ATTACHMENT: GENERAL COUNSEL'S ANALYSIS

The phrase "personally identifiable information" in Section 631 of the Communications Act is not defined in the statute. The meaning of that term in this context can, however, be inferred from the language of the statute, its legislative history, and court decisions.

The context of the statute indicates that "names and addresses of subscribers to any cable service or other service," the "extent of any viewing or other use by the subscriber of a cable service or other service provided by the cable operator," and "the nature of any transaction made by the subscriber over the cable system of the cable operator" are included in the definition of personally identifiable information because they are explicitly protected under Section 631(c)(2)(C). Conversely, "any record of aggregate data which does not identify particular persons" is excluded from the definition of personally identifiable information by Section 631(a)(2)(A).

By including Section 631 in the Cable Communications Policy Act of 1984, Congress expressed its intent that the section apply to "all individually identifiable information collected by a cable operator over a cable system regarding its subscribers." *See* H.R. Rep. No. 934, 98th Cong., 2d Sess. (1984), *reprinted in* 1984 U.S.C.C.A.N. 4655, 4713. The legislative history of Section 631 further illuminates the scope of protected personally identifiable information by specifically including "when the subscriber used the services and for how long" within the phrase "extent of any viewing or other use by the subscriber" as used in Section 631(c)(2). *Id.* at 4715. The legislative history also suggests that "particular selections of the subscribers" and "details of a particular transaction conducted over the cable system (such as a bank-at-home or shop-at-home transaction)" were intended to fall within the personally identifiable information that must be protected under the statute. *Id.*

Court decisions further support interpreting the term personally identifiable information under Section 631 of the Communications Act as including "subscriber viewing habits or the nature of transactions made by the subscriber over the cable system." *See, e.g., Scofield v. Telecable of Overland Park, Inc.*, 973 F.2d 874, 876 (10th Cir. 1992); *see also Metrovision of Livonia, Inc. v. Wood*, 864 F. Supp. 675, 681 n.3 (E.D. Mich. 1994) (providing as an example of personally identifiable information whether "a particular subscriber watched three hours of the Playboy Channel every night followed by two hours of a pay-per-view Wrestlemania contest"). Courts have relied on the legislative history to observe that Congress intended Section 631 to protect "details about bank transactions, shopping habits, political contributions, viewing habits and other significant personal decisions" of subscribers that the cable operator had in its possession by virtue of its operation of the network over which this information was transmitted. H.R. Rep. No. 934 at 29, *cited in Metrovision of Livonia*, 864 F. Supp. at 681. The "principal potential problem" that Congress intended Section 631 to address was the "opportunity to monitor subscriber viewing habits and then disclose such personally identifiable information without prior consent." S. Rep. No. 67, 98th Cong., 1st Sess. 28 (1983), *quoted in Metrovision of Livonia*, 864 F. Supp. at 681.

UNITED STATES DEPARTMENT OF COMMERCE
The Assistant Secretary for Communications and Information
Washington, D.C. 20230

SEP 8 2011

The Honorable Mary Bono Mack
Chairwoman
Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
House of Representatives
Washington, DC 20515

The Honorable Greg Walden
Chairman
Subcommittee on Communications and Technology
Committee on Energy and Commerce
House of Representatives
Washington, DC 20515

Dear Chairwoman Bono Mack and Chairman Walden:

Thank you for the opportunity to testify on July 14, 2011 before the Subcommittee on Commerce, Manufacturing, and Trade and the Subcommittee on Communications and Technology at the hearing entitled "Internet Privacy: The Views of the FTC, the FCC, and NTIA." I appreciate your forwarding an additional question for the record to me on August 16, 2011.

My response to the question is enclosed. If you or your staff have any additional questions, please do not hesitate to contact me or James Wasilewski, NTIA's Director of Congressional Affairs, at (202) 482-1551.

Sincerely,

Lawrence E. Strickling

Responses to Questions from Honorable Joe Barton

1. **I recently introduced H.R. 1895, the Do Not Track Kids Act of 2011 with Mr. Markey. Has your agency taken a position on this bill? If so, what is your position?**

At this time, the Administration has not taken a position on H.R. 1895, although we do support the goal of creating a safe online environment for all Internet users—children, teenagers, and adults—including the adoption of appropriate privacy protections. Protecting children's and teenagers' privacy interests may require approaches that take into the account the unique characteristics of these age groups.

In NTIA's view, the framework that the Obama Administration has proposed for consumer data privacy is appropriate for protecting children and teenagers. At the center of this framework is a "consumer privacy bill of rights" that is based on a general, flexible, and actionable set of privacy principles. Our recommended framework also includes an open, transparent multistakeholder process to develop enforceable codes of conduct that implement the consumer privacy bill of rights in specific contexts, as well as specific authority for the Federal Trade Commission (FTC) to enforce the consumer privacy bill of rights. A major benefit of this approach is that we will minimize the likelihood of legislative or regulatory requirements being imposed that will become outmoded quickly, hampering innovation, preventing law enforcement from ensuring public safety, and otherwise failing to meet the needs of Internet users in this fast-changing industry.

Under our proposal, the characteristics of an online business' customers, such as whether they include children or teenagers, are key elements in determining the appropriate privacy protections a business needs to implement. In environments that involve children, for example, businesses may need to comply with the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. § 6501 *et seq.*) and the Children's Online Protection Rule (16 C.F.R. Part 312), but they may also adopt codes of conduct based on the consumer privacy bill of rights that are more comprehensive and stringent than COPPA requires. Our framework should provide meaningful privacy protections for children and teenagers while sustaining an environment that promotes innovation.

We look forward to working with you, other members of Congress, privacy and consumer advocates, industry, and the FTC on this important issue.

○