S. HRG. 112–791

THE NEED FOR PRIVACY PROTECTIONS: PERSPECTIVES FROM THE ADMINISTRATION AND THE FEDERAL TRADE COMMISSION

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

MAY 9, 2012

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

81–793 PDF WASHINGTON : 2013

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

DANIEL K. INOUYE, Hawaii	KAY BAILEY HUTCHISON, Texas, *Ranking*
JOHN F. KERRY, Massachusetts	OLYMPIA J. SNOWE, Maine
BARBARA BOXER, California	JIM DEMINT, South Carolina
BILL NELSON, Florida	JOHN THUNE, South Dakota
MARIA CANTWELL, Washington	ROGER F. WICKER, Mississippi
FRANK R. LAUTENBERG, New Jersey	JOHNNY ISAKSON, Georgia
MARK PRYOR, Arkansas	ROY BLUNT, Missouri
CLAIRE MCCASKILL, Missouri	JOHN BOOZMAN, Arkansas
AMY KLOBUCHAR, Minnesota	PATRICK J. TOOMEY, Pennsylvania
TOM UDALL, New Mexico	MARCO RUBIO, Florida
MARK WARNER, Virginia	KELLY AYOTTE, New Hampshire
MARK BEGICH, Alaska	DEAN HELLER, Nevada

ELLEN L. DONESKI, *Staff Director*
JAMES REID, *Deputy Staff Director*
JOHN WILLIAMS, *General Counsel*
RICHARD M. RUSSELL, *Republican Staff Director*
DAVID QUINALTY, *Republican Deputy Staff Director*
REBECCA SEIDEL, *Republican General Counsel and Chief Investigator*

CONTENTS

WITNESSES

APPENDIX

THE NEED FOR PRIVACY PROTECTIONS: PERSPECTIVES FROM THE ADMINISTRATION AND THE FEDERAL TRADE COMMISSION

WEDNESDAY, MAY 9, 2012

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 2:35 p.m. in room SR–253, Russell Senate Office Building, Hon. John D. Rockefeller IV, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

The CHAIRMAN. Good afternoon, and I apologize for being 5 minutes late.

Every day, tens of millions of Americans go online to search for information. They want to shop. They want to pay their bills, or they're accessing social networking. To state the obvious, the Internet has fundamentally transformed every aspect of our lives.

What is less obvious is the level of information that is collected about us each time we visit a website or watch a video or send an e-mail or make a purchase.

Now consumers have had no choice but to place an enormous amount of trust in the online world, trust that their information is safe, that it will be secure, and it will be used appropriately, whatever that means.

But the incentive to misuse consumers' information is very great. A consumer's personal information is the currency, in fact, of the web.

The value of this data has created untold riches for those who have successfully harnessed it. This is not necessarily bad, as it enables an enormous amount of content to be accessed for free and allows companies to offer a number of services for free.

But unfettered collection of consumers' online data poses, to me, very significant risks.

Right now, consumers have little or no choice in managing how their online information is collected and how it is used. Whatever limited choices they do have are often too difficult to use and muddled by complicated, wordy, privacy policies. It's, again, your classic health insurance comparison—tiny writing.

Protecting consumer privacy is critical for companies, and I understand that. People need to trust the websites that they are visiting. But online companies are conflicted. They need to protect

consumers' information, but they also need to be able to monetize their users' data.

I am afraid that in the hypercompetitive online marketplace, the need to monetize consumers' data and profits will win out, probably almost every time, over privacy concerns.

The administration and the Federal Trade Commission have both recently issued reports on the need for industry to do more, to protect consumer data, and give consumers control over how their personal information is used. They have worked to bring about industry consensus on voluntary actions. This is an interesting subject, which we will discuss further at another hearing.

The administration's and the industry's actions are to be commended, with this respect. But I've learned over many years that self-regulation is inherently one-sided in many industries, in many times, in many eras, it's inherently one-sided, and that consumers' rights always seem to lose out to the industry's needs.

I believe consumers need strong legal protections. They need simple and easy-to-understand rules about how, what, and when their information can be collected and used. They need easy-to-understand privacy policies rather than pages of incomprehensible legalese.

We should take up strong, consumer-focused privacy legislation this year. I do not believe that significant consensus exists yet on what that legislation should look like, but I will continue to work with my colleagues on legislation.

As Chairman of this Committee, I will continue to work with the administration and the FTC, both represented here, to push the industry to develop and adhere to strong consumer privacy protections.

I will continue to hold oversight hearings to make sure that the trust Americans have placed in these companies is being respected.

I call now on the Ranking Member, my next-door neighbor.

STATEMENT OF HON. PATRICK J. TOOMEY,
U.S. SENATOR FROM PENNSYLVANIA

Senator TOOMEY. Thank you very much, Mr. Chairman. And thank you for holding another hearing on the topic of privacy. It is a very important topic.

As I have said in this committee in the past, I still remain skeptical of the need for Congress to pass privacy legislation, or, for that matter, for the FTC to have increased authority to enforce new privacy rules, regulations, or principles on the private sector.

It seems to me that neither this committee nor the FTC nor the Commerce Department fully understands what consumers' expectations are when it comes to their online privacy. Consumer expectations of privacy can vary based on a particular application they're using or by the general privacy preference of any given individual consumer.

It's important that companies have maximum flexibility to work with their customers to ensure their customers' needs and preferences are met, and that the application or service functions as consumers expect.

As the recent FTC report correctly points out, companies are already currently competing on privacy and are promoting services

as having stronger privacy protections than what is being offered by marketplace rivals, for instance. This is a sign of a healthy, functioning, and competitive market. This type of competition is something that we should be encouraging.

Overly restrictive privacy rules and regulations handed down from Washington may threaten this innovation by shifting the incentives to compliance over competition. I don't think anyone desires such a result, which is why I caution my colleagues and the administration to proceed with caution.

Proponents of Federal privacy legislation and of granting the FTC authority to regulate online activity really should clearly demonstrate the market failure and consumer harm that they seek to address.

The benefits of online tracking and data collection are very clear. Facebook is free. Gmail is free. Google Maps is free. There are thousands of mobile device applications that are free.

It's often said that information is the currency of the Internet. A detailed, cost-benefit analysis of a Do Not Track regulation or other new privacy rules would better inform our discussion. But to my knowledge, one has not been completed.

We need to fully understand the impact these proposals will have on the marketplace and on the many online services consumers have come to expect for free or at a minimal cost.

Less information available is very likely to result in fewer, free online services and an increase in pay walls. I think it's irresponsible for the Federal Government to require companies to radically alter a successful business model that has provided many consumer benefits without knowing all the facts first.

I also question whether specific consumer harms currently occurring in the marketplace cannot be addressed under the FTC's current statutory authority. Section 5 of the FTC Act grants the Commission broad authority to investigate unfair or deceptive acts or practices, and the Commission has brought enforcement actions using this authority.

In fact, the Commission highlights a number of these enforcement actions in the beginning of its recently released report.

When the Commission sees what it believes to be unfair or deceptive practices, it has acted. Just yesterday, it was reported that the FTC and MySpace reached a privacy settlement that will subject the company to biennial privacy assessments for the next 20 years.

In addition, Google and Facebook recently entered into consent decrees that subject the companies to outside audits for two decades. I have not yet heard a persuasive argument as to why the FTC needs even greater authority.

And last, I find it interesting that the Commission seems very concerned about consumer trust in the private sector. Consumer trust is very, very important. But there's no one for whom it's more important than the company that's hoping to attract and maintain customers. So I think trust in the marketplace is something that the marketplace tends to sort out pretty well.

Companies in all sectors of the economy have a powerful interest in building a strong, trusting relationship with their customers. If

consumers don't trust company A, they quickly flee to company B. In the online space, this incentive is even stronger.

The Internet has made leaving one company or service provider for another very easy. It can often be done at little or no cost. As one major online company likes to say, the Internet is where "competition is one click away."

While this is an important topic and certainly worthy of our consideration, I do think it's premature to begin discussing specific legislative fixes or increased FTC authority when we don't fully know whether or not and to what extent the problem exists.

I look forward to hearing from our witnesses today. I thank them for coming, and I thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much, Senator Toomey.

And I call now on the Chairman of the Subcommittee that works this, and that is Senator John Kerry.

STATEMENT OF HON. JOHN F. KERRY,
U.S. SENATOR FROM MASSACHUSETTS

Senator KERRY. Thank you very much, Mr. Chairman. I appreciate it. And I certainly appreciate this hearing.

And I think this hearing can help, as a couple of prior hearings have.

I think the record is already fairly clear, Senator Toomey, if I may say, that a lot of the questions you've raised have actually been addressed in those hearings. And I think there's been a pretty powerful showing with respect to both the ability to have a privacy standard as well as the need for the privacy standard, without affecting those applications and the free access and all the other things you're talking about. And I think the record will reflect that.

I'm delighted that we have the Chair of the Federal Trade Commission and one of the commissioners from the Commission here with us today.

And obviously, I'm delighted to welcome my own brother, who carries either the burden or privilege of being so. But I'm glad that he's here today representing the Commerce Department. He's been working on this under two different secretaries now, as have many of us here on the Committee.

So I know that in his capacity as the General Counsel, together with the Chair, they are going to set out today the final findings of both the Commerce Department and the Federal Trade Commission with respect to this question.

It is not unimportant, I think, that both the Commerce Department and the Federal Trade Commission, frankly, together with most of the privacy experts in the country, have all come to the conclusion that we need to have a privacy law with respect to providing protection to individuals in commerce.

And I think that the distinction, Senator Toomey, is that the privacy experts have all come to that conclusion. Obviously, some of the companies have not and don't share it. And the reason for that is very simple. In the information economy, the more that a company knows about you, the more valuable you are to them, whether you have consented to that or not. And they are collecting more than simply the information that you type in. And a lot of Americans aren't necessarily aware of that.

These companies watch your behavior, and they measure your behavior—how long you linger on a site, your specific searches. A lot of people think they're just going in and searching privately. Somebody's watching you. Somebody's tracking you.

You know, you wouldn't feel particularly good if you had a private investigator trailing you through the mall, looking at every single receipt that you get and everything you peruse and look at and ask for. That's essentially what's happening here.

You don't have privacy. They analyze and enhance that data, and then they reach a conclusion about you.

Using that information, these data scientists, are creating enormous wealth, often producing innovative products, we agree, and services. But there is nothing to stop them from doing the creation of those products and services with the consent of people who want to be part of that, or without necessarily the detail of those who do not.

So what's the harm? Senator Toomey sort of asked the question today: what's the harm of what can happen to you without your knowledge, consent, or active participation, and where there are no limits to what can be collected and where you have no right to access what is being collected about you?

It seems to me the more conservative position here is, frankly, to protect the individual in America, not to protect the right of people to invade your space without your knowing it.

So if it's not properly secured, that information can actually harm you, number one, through identity theft. And even if it is properly secured, it can be used to categorize you inaccurately or in ways that you don't wish to be categorized, exposing you to either reputational harm or to unwanted targeting.

For example, by analyzing your buying habits, a retailer may know that you're pregnant before you even tell anyone, may begin to send you advertising based on medical status, or on your ethnicity or on your age. And corresponding behavior can then be used to target you in different ways than other populations may be targeted, and maybe you don't want to be targeted or analyzed in that particular way.

Or as in the case of the Google Wi-Fi collection, your private communications, including sensitive conversations, can be easily captured exposing aspects of your life to companies that are simply nobody's business.

But when information collected about you is used to make your buying experience better or serve you better, you'll find a majority of the people have absolutely no problem consenting to that kind of use.

But the collector ought to have the right to make that judgment, the value proposition with respect to the consumer.

Most Americans don't have any awareness that there's no general law of privacy in commerce in the U.S. today governing these transactions. And when it's brought to their attention, they say they want one. Our largest trading partners have such laws built on the European standard.

But I believe it's important for us to set our own standard, something that could, in fact, be more flexible and more stakeholder-

driven and less punitive than what exists in Europe today, but just as capable of delivering strong privacy protections.

So in keeping with the spirit that the United States normally doesn't wait for someone else to set the standard and then borrow it, we ought to be setting our own standard. The final agency reports that have been issued recently agree that we ought to lay out a blueprint of privacy principles for legislation.

Senator John McCain and I have agreed on one approach. And I introduced that approach with him more than a year ago. It reflects each of the principles that are being put forward in the analyses today, as well as the concept of a safe harbor for a flexible application of the code of conduct to different kinds of businesses.

I think all of us know that consumers in the United States are very smart. They'll consent to reasonable and useful data collection and use practices, particularly if they think it enhances their buying and life experience.

But the most important principle we want to reinforce here is that the individual consumer has the right to make that decision.

So can we get there? I think it's up to the members of this committee on both sides of the Committee. The bipartisan proposal that Senator McCain and I offered up is, as I said, it's not the only way to approach this. We're ready to negotiate. And I think we ought to compromise in this effort to reach sort of a fair standard.

But we need to get down to that discussion, because we really can't afford another year of delay, which may in the end wind up putting America into a default position on this, which would be far less flexible, thoughtful, and sensitive to our own business interests.

And I think that Americans ought to know that Congress believes that, in the digital age, every individual American has a right to an expectation of privacy.

I hope we can find that way forward, Mr. Chairman.

The CHAIRMAN. Thank you very much, Senator Kerry.

I want to proceed now to our witnesses, and we'll have ample time for questioning, and other members will be coming and leaving.

My preference of order would be to start with the Hon. John Leibowitz, who is the Chairman of the Federal Trade Commission. Then Hon. Ohlhausen, I'm going to skip over you to the guy who is General Counsel to the Department of Commerce, who is somehow related to Senator Kerry. And then come back to you as a cleanup. Is that all right?

Ms. OHLHAUSEN. Certainly.

The CHAIRMAN. So let's start with Chairman Leibowitz.

STATEMENT OF HON. JON D. LEIBOWITZ, CHAIRMAN, FEDERAL TRADE COMMISSION

Mr. LEIBOWITZ. Thank you, Chairman Rockefeller, Senator Toomey, Senator Kerry, Senator Pryor, Senator Klobuchar, and Senator Ayotte. I appreciate the opportunity to present the Commission's testimony on consumer privacy, alongside our newest Commissioner, Maureen Ohlhausen, as well as my friend Cam Kerry.

The Commission commends the recent privacy efforts by the Department of Commerce, as well as the bipartisan leadership your committee has shown on consumer privacy issues. Though most of my remarks today will concern privacy policy and especially Do Not Track, the FTC is primarily an enforcement agency, and Commissioner Ohlhausen will describe our recent enforcement efforts.

Mr. Chairman, imagine a cash-strapped college student working part-time to keep up with tuition payments. To make ends meet, she applies online for a loan and obtains it at a favorable rate. But she also goes online because her father suffers from depression, so she wants to research symptoms and potential treatments.

Soon after, in the mail, she receives another loan offer, this time from a payday lender at a much higher rate. In the evening, she spends time relaxing by catching up with friends' posts on a social network. While online, she notices she's receiving ads for medication for stress and depression, as well as more loan offers.

Could the lender have sold the information about her need for money to payday lenders, who are now offering her loans? Could the fact that she researched depression be sold to or shared with potential employers or insurers? Can these exchanges of information occur without the consumers' consent or even awareness?

The answer to all these questions is yes.

Of course, the college student benefits from quick responses to loan applications, free access to health information, and an easy way to keep up with her friends and family.

But as Senator Kerry noted in his opening statement, the vast majority of Americans simply have no knowledge that their financial, health, and other personal information may be sold to data brokers, lead generators, lenders, insurance companies, potential employers, and, really, just about anybody else. Most consumers are entirely unaware of the vast amounts data about them being collected, sold, and used both online and offline.

Now, we at the Commission applaud—applaud—the Internet innovation that has created enormous benefits for consumers and the advertising ecosystem that has provided free content and services, the ones that we have all come to expect and enjoy. But as the Nation's privacy protection agency, we are also concerned that some practices by some companies may adversely affect Americans and their critical rights to privacy.

At the FTC, we have been thinking about this issue for more than a decade. We recently released our final privacy report that sets forth what we in the public and private sectors should do to make sure that the right to privacy remains robust for all Americans.

The short answer is the consumer should have more choice and more control. And to ensure that control, our report lays out three simple but powerful principles for companies to follow in handling personal data.

This is guidance. It is not a regulation.

First, incorporate privacy protections into products as they are developed. That is privacy by design. Second, offer consumers choice and control over how their data is collected and used. And third, provide more transparency; that is, better explanations to consumers about how their data is handled by companies.

The final report also recommends that Congress consider enacting general privacy legislation, as well as specific statutes addressing data security and data brokers. Data brokers often hold a wealth of information about consumers but remain utterly invisible to them.

In addition, our report calls for a Do Not Track mechanism, one that is easy to use and persistent, to enable consumers to control the collection of information about their activities across websites. And it's worth emphasizing here that your computer is your property.

And as the first chairman I served with, Republican Deborah Majoras, used to say, "people shouldn't be putting things in your computer without your consent." And I think that is fundamentally, a conservative notion.

In the last year, industry has made strides toward finalizing a meaningful Do Not Track system, as you know, Mr. Chairman. Indeed, at this point, we are no longer asking whether Do Not Track will exist, but only how it will be implemented. We're optimistic that, with the encouragement of this committee and especially you, Mr. Chairman, a Do Not Track mechanism that allows consumers to control the collection of their browsing information, with limited exceptions—for example, to prevent fraud—will be in place by the end of the year.

And just going back to the discussion between Senator Toomey and Senator Kerry, Do Not Track, of course, will be run by industry. It won't be run like the Government runs Do Not Call.

Of course, vigorous enforcement remains a top priority for our agency, as Commissioner Ohlhausen will describe in more detail. Just this week, we announced a case against the social network MySpace. The FTC complaint alleged that MySpace shared personal user information with advertisers after promising that it would not. The proposed settlement order prohibits MySpace from making any privacy misrepresentations and requires it to create a comprehensive privacy program, and undergo third party audits. Simply put, this case, as well as others that we brought, stands for the proposition that we will hold companies accountable for their privacy commitments.

We appreciate the leadership of you, Chairman Rockefeller, and this committee. And we look forward to continuing to work with Congress, the administration, industry, and other stakeholders, on privacy protection going forward. Thank you.

[The prepared statement of Mr. Leibowitz follows:]

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

Introduction

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, I am Jon Leibowitz, Chairman of the Federal Trade Commission ("FTC" or "Commission").[1]

We are pleased to be testifying today alongside General Counsel Cameron Kerry of the Department of Commerce and the newest member of the FTC, Commissioner Maureen Ohlhausen. The Commission supports the privacy efforts and approach de-

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

veloped by the Department of Commerce, and we look forward to working with the Department of Commerce, the Administration, and Congress as they move forward in their efforts in this arena. Members of this Committee in particular have demonstrated that they understand how important it is that consumers'—and especially children and teens'—personal data be treated with care and respect.

This is a critical juncture for consumer privacy, as the marketplace continues to rapidly evolve and new approaches to privacy protection are emerging in the United States and around the world. After careful consideration, the Commission recently released the final privacy report ("Final Report"). The Final Report sets forth best practices for businesses to guide current efforts to protect consumer privacy while ensuring that companies can continue to innovate. The Commission urges industry to use this guidance to improve privacy practices and accelerate the pace of self-regulation. Importantly, we have seen promising developments by industry toward a Do Not Track mechanism and we ask the Committee to continue to encourage industry to move towards full implementation. The Report also calls on Congress to consider enacting general privacy legislation. We reiterate today our call to Congress to enact legislation requiring companies to implement reasonable security measures and notify consumers in the event of certain security breaches, as well as targeted legislation that would provide consumers with access to information about them held by data brokers.

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

This testimony begins by describing the Commission's Final Report. It then offers an overview of other recent policy efforts in the areas of privacy and data security and concludes by discussing the Commission's recent enforcement and education efforts.

II. Final Privacy Report

The FTC recently released its Final Report, setting forth best practices for companies that collect and use consumer data.[2] These best practices can assist companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. To the extent these best practices exceed existing legal requirements, they are not intended to serve as a template for law enforcement or regulations under laws currently enforced by the FTC.[3]

The Final Report supports the three key principles laid out in the preliminary staff report.[4] 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

---

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

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

[4] The Commission received over 450 public comments from various stakeholders in response to the preliminary report, which were highly informative to the Commission as it refined the final framework.

purpose, safely disposing of data no longer in use, and implementing reasonable procedures to promote data accuracy.

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

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

In addition, the Final Report makes general and specific legislative recommendations. The Report supports the development of general privacy legislation to ensure basic privacy protections across all industry sectors, and can inform Congress, should it consider such privacy legislation.[5] The Commission recommends that any such legislation be technologically neutral and sufficiently flexible to allow companies to continue to innovate. In addition, the Commission believes that any legislation should allow the Commission to seek civil penalties to deter statutory violations. Such legislation would provide businesses with the certainty they need to understand their obligations as well as the incentive to meet those obligations, while also assuring consumers that companies will respect their privacy. We believe this approach would foster an environment that allows businesses to innovate and consumers to embrace those innovations without risking their privacy. The Final Report also calls on Congress to enact legislation requiring companies to implement reasonable security measures and notify consumers in the event of certain security breaches,[6] as well as targeted legislation for data brokers, discussed below. We look forward to working with Congress and other stakeholders to craft this legislation.

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

A. Do Not Track

The Final Report advocates the continued implementation of a universal, one-stop mechanism to enable consumers to control the tracking of their online activities across websites, often referred to as "Do Not Track," which the Commission first called for in December 2010 and Chairman Rockefeller has sought through his legislative proposal.[7] We recognize the benefits to such online data collection, including more relevant advertising and free online content that consumers have come to expect and enjoy. However, we have concerns that too many consumers either do not

---

[5] Earlier this year, the Administration released its final "White Paper" on consumer privacy, recommending that Congress enact legislation to implement a Consumer Privacy Bill of Rights. *See Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), available at *http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.*

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

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

understand they are trading their privacy for free online content or have not made an informed choice to do so.

The Commission commends industry efforts to improve consumer control over behavioral tracking in response to our calls. As industry explores technical options and implements self-regulatory programs, and as Congress examines Do Not Track, the Commission continues to believe that an effective Do Not Track system should include five key principles. *First,* a Do Not Track system should be implemented universally to cover all parties that would track consumers. *Second,* the choice mechanism should be easy to find, easy to understand, and easy to use. *Third,* any choices offered should be persistent and should not be overridden if, for example, consumers clear their cookies or update their browsers. *Fourth,* a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes.[8] *Fifth,* an effective Do Not Track system should go beyond simply opting consumers out of receiving targeted advertisements; it should opt them out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction (*e.g.,* preventing click-fraud or frequency capping for ads). 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. And unlike the Do Not Call Registry, a Do Not Track mechanism should be implemented by the private sector.

Early on, the companies that develop web browsers stepped up to the challenge to give consumers choices about how they are tracked online, sometimes known as the "browser header" approach. When consumers enable Do Not Track, the browser transmits the header to all types of entities, including advertisers, analytics companies, and researchers, that track consumers online. Just after the FTC's call for Do Not Track, Microsoft developed a system to let users of Internet Explorer prevent tracking by different companies and sites.[9] Mozilla introduced a Do Not Track privacy control for its Firefox browser that an impressive number of consumers have adopted.[10] Apple subsequently included a similar Do Not Track control in Safari.[11]

The online advertising industry, led by the Digital Advertising Alliance ("DAA"), has also led efforts by implementing a behavioral advertising opt-out program. The DAA's accomplishments are notable: it has developed a notice and choice mechanism through a standard icon in ads and on publisher sites; deployed the icon broadly, with reportedly over 900 billion impressions served each month; obtained commitments to follow the self-regulatory principles from advertisers, ad networks, and publishers that represent close to 90 percent of the online behavioral advertising market; and established an enforcement mechanism designed to ensure compliance with the principles.[12] The DAA is also working to address one of the long-standing criticisms of its approach—how to limit secondary use of collected data so that the consumer opt-out extends beyond simply blocking targeted ads and to the collection of information for other purposes. The DAA has released principles that include limitations on the collection of tracking data and prohibitions on the use or transfer

---

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

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

[10] The Mozilla Blog, *Mozilla Firefox 4 Beta, Now Including "Do Not Track" Capabilities* (Feb. 8, 2011), *blog.mozilla.com/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/;*

Alex Fowler, *Do Not Track Adoption in Firefox Mobile is 3x Higher than Desktop,* MOZILLA PRIVACY BLOG (Nov. 2, 2011), *http://blog.mozilla.com/privacy/2011/11/02/do-not-track-adoption-in-firefox-mobile-is-3x-higher-than-desktop/.*

[11] Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser,* WALL ST. J., Apr. 13, 2011, available at *http://online.wsj.com/article/SB10001424052748703551304576261272308358858.html.* Google has taken a slightly different approach—providing consumers with a browser extension that opts them out of most behavioral advertising on a persistent basis. Sean Harvey & Rajas Moonka, *Keep Your Opt Outs,* GOOGLE PUBLIC POLICY BLOG (Jan. 24, 2011), *http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html.*

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

of the data for employment, credit, insurance, or health care eligibility purposes.[13] The DAA is now working to fully implement these principles. Just as important, the DAA recently moved to address some persistence and usability criticisms of its icon-based opt out by committing to honor the tracking choices consumers make through their browser settings.[14]

At the same time, the World Wide Web Consortium ("W3C"), an Internet standards-setting body, has convened a broad range of stakeholders to create an international, industry-wide standard for Do Not Track, including DAA member companies; other U.S. and international companies; industry groups; and public interest organizations. The W3C group has done admirable work to flesh out how to make a Do Not Track system practical in both desktop and mobile settings as reflected in two public working drafts of its standards.[15] Some important issues remain, and the Commission encourages all of the stakeholders to work within the W3C group to resolve these issues.

While work remains to be done on Do Not Track, the Commission believes that the developments to date, coupled with legislative proposals, provide the impetus towards an effective implementation of Do Not Track. The advertising industry, through the DAA, has committed to deploy browser-based technologies for consumer control over online tracking, alongside its ubiquitous icon program. The W3C process, thanks in part to the ongoing participation of DAA member companies, has made substantial progress toward specifying a consensus consumer choice system for tracking that is practical and technically feasible.[16] The Commission anticipates continued progress in this area as the DAA members and other key stakeholders continue discussions within the W3C process to work to reach consensus on a Do Not Track system in the coming months.

B. Data Brokers

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

The Final Report addresses the particular importance of consumers' ability to access information that data brokers have about them. Data brokers are companies that collect information, including personal information about consumers, from a wide variety of sources in order to resell such information for a variety of purposes, including verifying an individual's identity, differentiating one consumer's records from another's, marketing products, and preventing financial fraud. Such entities often have a wealth of information about consumers without interacting directly with them. Data brokers can compile data that can be used to benefit consumers, such as to help authenticate consumers in order to prevent identity theft or provide them with relevant offers and deals for products and services. However, consumers are often unaware of the existence of these entities, as well as the purposes for which they collect and use data.[17]

The Commission has monitored data brokers since the 1990s, hosting workshops, drafting reports, and testifying before Congress about the privacy implications of data brokers' practices.[18] Following a Commission workshop, data brokers created

---

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

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

[15] *See* Press Release, W3C, *Two Drafts Published by the Tracking Protection Working Group* (Mar. 13, 2012), available at *http://www.w3.org/News/2012#entry-9389;* Press Release, W3C, *W3C Announces First Draft of Standard for Online Privacy* (Nov. 14, 2011), available at *http://www.w3.org/2011/11/dnt-pr.html.en.*

[16] A system practical for both businesses and consumers would include, for users who choose to enable Do Not Track, significant controls on the collection and use of tracking data by third parties, with limited exceptions for functions such as security de-identified data, and frequency capping. As noted above, a website's sharing of behavioral information with third parties is not consistent with the context of the consumer's interaction with the website and would be subject to choice. Do Not Track is one way for users to express this choice.

[17] As noted above, in connection with online tracking, it is generally inconsistent with the context of the interaction for a consumer-facing entity to share the consumer's data with a third party. Accordingly, such transfers of personal information would be subject to choice.

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

the Individual References Services Group (IRSG), a self-regulatory organization for certain data brokers that set forth principles to restrict availability to certain non-public information.[19] The industry ultimately terminated this organization. Although a series of public breaches—including one involving ChoicePoint—led to renewed scrutiny of the practices of data brokers,[20] there have been no meaningful broad-based efforts to implement self-regulation in this area in recent years.

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

The Commission has long supported legislation that would give access rights to consumers for information held by data brokers.[21] For example, Senator Pryor and Chairman Rockefeller's S.1207 includes provisions to establish a procedure for consumers to access information held by data brokers.[22] The Commission continues to support legislation in this area to improve transparency of the industry's practices.[23]

The Commission also recommends that the data broker industry explore the possibility of creating a centralized website where data brokers could identify themselves to consumers, describe how they collect consumer data, and disclose the types of companies to which they sell the information.[24] The Commission staff intends to discuss with relevant companies how this website could be developed and implemented voluntarily, to increase the transparency and provide consumers with tools to opt out.[25]

III. Other Policy Initiatives

In addition, the Commission holds public workshops and issues reports to examine the implications of new technologies and business practices on consumer privacy. We outline four notable examples below.

First, in February 2012, the Commission released a staff report on mobile applications ("apps") for children.[26] The report found that in virtually all cases, neither app stores nor app developers provide disclosures that tell parents what data apps collect from children, how apps share it, and with whom. The report recommends that all members of the children's app ecosystem—the stores, developers and third parties providing services—should play an active role in providing key information to

---

nesses of the Collection and Use of Consumer Information (June 18, 2003), available at *http://www.ftc.gov/bcp/workshops/infoflows/030618agenda.shtm.*

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

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

[21] *See, e.g.,* Prepared Statement of the FTC, *Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer Protection,* 111th Cong. (May 5, 2009), available at *http://www.ftc.gov/os/2009/05/P064504peertopeertestimony.pdf.*

[22] Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011); *see also* Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011).

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

[24] *See, e.g.,* Tanzina Vega & Edward Wyatt, *U.S. Agency Seeks Tougher Consumer Privacy Rules,* N.Y. TIMES, Mar. 26, 2012, available at *http://www.nytimes.com/2012/03/27/business/ftc-seeks-privacy-legislation.html?pagewanted=all* ("'It's not an unreasonable request to have more transparency among data brokers.'") (quoting Jennifer Barrett Glasgow, Chief Privacy Officer for Acxiom).

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

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

parents.[27] The report also encourages app developers to provide information about data practices simply and succinctly. The Commission has already reached out to work with industry to provide parents with the information they need, and some industry participants have taken positive steps to improve disclosures going forward.

To discuss how members of the mobile and online ecosystems can best disclose their data practices to consumers, the Commission will host a public workshop later this month.[28] The workshop will address the technological advancements and marketing developments since the FTC first issued its online advertising disclosure guidelines known as "Dot Com Disclosures,"[29] including the advent of smartphones and tablets. The workshop will examine whether and how to revise the Dot Com Disclosures in the current online and mobile advertising environment and will include a specific panel on mobile privacy disclosures.[30]

Second, the FTC hosted a workshop in December 2011 that explored facial recognition technology and the privacy and security implications raised by its increasing use.[31] Facial detection and recognition technology has been adopted in a variety of new contexts, ranging from online social networks to digital signs and mobile apps. Commission staff sought comments on the privacy and security issues raised at the workshop, which it will address in a report in the coming months.

Third, as discussed in the Final Report, the FTC intends to examine the practices of large platforms such as Internet browsers, mobile operating system providers, Internet Service Providers, and large social media platforms that can collect data from numerous sources to build extensive profiles about consumers. Commission staff will host a workshop in the second half of 2012 to examine questions about the scope of such data collection practices, the potential uses of the collected data, and related issues.

Finally, the Commission is undertaking a comprehensive review of the COPPA Rule in light of rapidly evolving technology and changes in the way children use and access the Internet.[32] In September 2011, the Commission proposed modifications to the Rule intended to update the Rule to meet changes in technology, assist operators in their compliance obligations, strengthen protections over children's data, and provide greater oversight of COPPA safe harbor programs.[33] For example, the Commission proposed adding geolocation information and cookies used for behavioral advertising to the definition of "personal information," which would have the effect of requiring parental consent for collection of this information. In addition, the Commission proposed adding a new provision addressing data retention and deletion. The Commission received over 350 comments on its proposed amendments to the COPPA Rule, which are being reviewed by FTC staff.

IV. Enforcement

In addition to its engagement on the policy front, enforcement remains a top priority for the agency. To date, the Commission has brought 36 data security cases; almost 80 cases against companies for improperly calling consumers on the Do Not Call registry;[34] 86 cases against companies for violating the Fair Credit Reporting Act ("FCRA");[35] more than 100 spam and spyware cases; 18 COPPA cases;[36] 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.

---

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

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

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

[30] In addition to examining mobile disclosures, the Commission continues to examine other privacy and security issues associated with the mobile ecosystem. *See, e.g.,* FTC Workshop, *Paper, Plastic . . . or Mobile?: An FTC Workshop on Mobile Payments* (Apr. 26, 2012), available at *http://www.ftc.gov/bcp/workshops/mobilepayments/*.

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

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

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

[34] 16 C.F.R. Part 310.

[35] 15 U.S.C. §§ 1681e–i.

[36] 15 U.S.C. §§ 6501–6508.

Where the FTC has authority to seek civil penalties, it has aggressively done so. It has obtained $60 million in civil penalties in Do Not Call cases; $21 million in civil penalties under the FCRA; $5.7 million under the CAN–SPAM Act;[37] and $6.6 million under COPPA. Where the Commission does not have authority to seek civil penalties, as in the data security and spyware areas, it has sought such authority from Congress.

Two highly publicized privacy cases—against Google and Facebook—will benefit more than one billion consumers worldwide. The Commission charged Google with deceiving consumers by taking previously private information—the frequent contacts of Gmail users—and making it public in order to generate and populate a new social network, Google Buzz.[38] This, the Commission alleged, was done without the users' consent and in contravention of Google's privacy promises. As part of the Commission's decision and consent order, Google must protect the privacy of consumers who use Gmail as well as Google's many other products and services. Under the order, if Google changes a product or service in a way that makes any data collected from or about consumers more widely available to third parties, it must seek affirmative express consent to such a change. In addition, the order requires Google to implement a comprehensive privacy program and obtain independent privacy audits every other year for the next 20 years.

The FTC's case against Facebook alleged numerous deceptive and unfair practices.[39] These include the 2009 changes made by Facebook so that information users had designated private—such as their "Friends List" or pages that they had "liked"—became public. The complaint also charged that Facebook made inaccurate and misleading disclosures relating to how much information about users' apps operating on the site could access. For example, Facebook told users that the apps on its site would only have access to the information those apps "needed to operate." The complaint alleges that in fact, the apps could view nearly all of the users' information, regardless of whether that information was "needed" for the apps' functionality. The Commission further alleged that Facebook made promises that it failed to keep: It told users it would not share information with advertisers, and then it did; and it agreed to make inaccessible the photos and videos of users who had deleted their accounts, and then it did not. Similar to the Google order, the Commission's consent order against Facebook prohibits the company from deceiving consumers with regard to privacy; requires it to obtain users' affirmative express consent before sharing their information in a way that exceeds their privacy settings; and requires it to implement a comprehensive privacy program and obtain outside audits. In addition, Facebook must ensure that it will stop providing access to a user's information after she deletes that information.

Most recently, the Commission announced a settlement with the social network Myspace. The FTC complaint alleged that, despite promising its users that it would not share consumers' personal information with advertisers, Myspace provided advertisers with the "Friend ID" of users who were viewing particular pages on the site. With the Friend ID, the advertiser could locate the user's Myspace personal profile to obtain his or her real name and other personal information. The advertiser could also combine the user's real name and other personal information with additional information to link broader web-browsing activity to a specific named individual. The proposed order prohibits Myspace from misrepresenting the privacy and confidentiality afforded to users' information, and requires Myspace to create a comprehensive privacy program and undergo third-party audits every other year for the next 20 years.

Finally, the Commission continues to make children's privacy a priority, as demonstrated by a recent a settlement with RockYou, the popular social media gaming company.[40] Despite its claims to have reasonable security, RockYou allegedly failed to use reasonable and appropriate security measures to protect consumers' private data, resulting in hackers gaining access to 32 million e-mail addresses and RockYou passwords. In addition, the Commission charged that RockYou collected personal information from approximately 179,000 children it knew to be under 13 without providing notice or obtaining parental consent, as required by COPPA and despite claims to the contrary. Under the Commission's settlement, RockYou must

---

[37] 15 U.S.C. §§ 7701–7713.

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

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

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

implement a data security program and undergo audits every other year for the next 20 years and pay a $250,000 civil penalty.

V. Education

The FTC conducts outreach to businesses and consumers in the area of consumer privacy. The Commission's well-known OnGuard Online website educates consumers about many online threats to consumer privacy and security, including spam, spyware, phishing, peer-to-peer ("P2P") file sharing, and social networking.[41] Furthermore, the FTC provides consumer education to help consumers better understand the privacy and security implications of new technologies. For example, last year the Commission issued a guide that provides consumers with information about mobile apps, including what apps are, the types of data they can collect and share, and why some apps collect geolocation information.[42]

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.[43] In addition, the FTC has developed education resources specifically for children, parents, and teachers to help children stay safe online. 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.[44] In less than one year, the Commission distributed more than 7 million copies of *Net Cetera* to schools and communities nationwide.

Business education is also an important priority for the FTC. The Commission seeks to educate businesses by developing and distributing free guidance. For example, the Commission developed a widely-distributed guide to help small and medium-sized businesses implement appropriate data security for the personal information they collect and maintain.[45] The Commission also creates business educational materials on specific topics—such as the privacy and security risks associated with peer-to-peer file-sharing programs and companies' obligations to protect consumer and employee information from these risks[46] and how to properly secure and dispose of information on digital copiers.[47] These publications, as well as other business education materials, are available through the FTC's Business Center website, which averages one million unique visitors each month.[48] The Commission also hosts a Business Center blog,[49] which frequently features consumer privacy and data security topics; presently, approximately 3,500 attorneys and business executives subscribe to these e-mail blog updates.

Another way the Commission seeks to educate businesses by publicizing its complaints and orders and issuing public closing and warning letters. For example, the Commission recently sent warning letters to the marketers of six mobile apps that provide background screening services.[50] The letters state that some of the apps included criminal record histories, which bear on an individual's character and general reputation and are precisely the type of information that is typically used in employment and tenant screening. The FTC warned the apps marketers that, if they have reason to believe the background reports they provide are being used for employment screening, housing, credit, or other similar purposes, they must comply with the FCRA. The Commission made no determination as to whether the companies are violating the FCRA, but encouraged them to review their apps and their policies and procedures to ensure they comply with the Act.

---

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

[42] *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.*

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

[44] *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.*

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

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

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

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

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

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

VI. Conclusion

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

The CHAIRMAN. Thank you, sir.

The Honorable Cameron F. Kerry, General Counsel, U.S. Department of Commerce.

STATEMENT OF HON. CAMERON F. KERRY, GENERAL COUNSEL, U.S. DEPARTMENT OF COMMERCE

Mr. KERRY. Thank you, Chairman Rockefeller, Ranking Member Toomey, distinguished members of the Committee. I'm grateful for the opportunity to testify today about the administration's Blueprint for data privacy.

This Blueprint is a framework to enhance consumer privacy while fostering economic growth, job creation, and exports for American businesses.

The Federal Trade Commission has been a global leader in this area as well as a partner to the Department of Commerce and a valued adviser to the National Science and Technology Council in developing the Privacy Blueprint. So I welcome being able to join Chairman Leibowitz and Commissioner Ohlhausen at the witness table today.

The explosion in the collection and storage and analysis of data and digital information offers new frontiers of knowledge and innovation and growth. But Senator Toomey asked the question, what is the market failure here? We are now at a tipping point that presents a dual market failure.

First, while many companies earned trust as responsible stewards of consumers' personal information, it exceeds the ability of even the most sophisticated consumers to understand and control what information is collected about them. And second, this asymmetry allows outliers and outlaws that are not good stewards of information to take advantage of consumers' trust and lack of information.

That is why a great many companies, consumer groups, the FTC, and the administration support baseline consumer privacy legislation. When it comes to sustaining trust in the digital economy, business and consumer and government interests converge.

The administration's Privacy Blueprint articulates a Consumer Privacy Bill of Rights: individual control, transparency, respect for context, access and accuracy, security, and focused collection and accountability. And it calls for Congress to give these broad principles the force of law.

We recommend two mechanisms to apply these principles. The first is giving the FTC the direct authority to enforce the individual provisions of the Bill of Rights as enacted, rather than relying entirely on its Section 5 authority, as currently framed.

The second is authorizing the FTC to grant safe harbors from enforcement for codes of conduct that address how best to follow the Privacy Bill of Rights in specific contexts.

The National Telecommunications and Information Administration of the Department of Commerce is carrying out the administration's Blueprint by initiating stakeholder-driven processes to develop codes of conduct. NTIA is reviewing recommendations on the first topic and on the process, including your comments, Chairman Rockefeller, thank you.

NTIA should be selecting a topic and convening the first meetings very soon.

In addition, I have asked a working group to put the administration's Privacy Blueprint into legislative language we are drafting. And we stand ready to work with this Committee and with other Members of Congress to put baseline privacy legislation into law.

What we do here in America is paramount to U.S. consumers and companies, but we cannot ignore the global reach of the Internet. Europe is in the process of honing its approach to data privacy. Other countries around the world understand the need for rules of the road and are looking for models.

We have the clear opportunity, as President Obama said in his preface to the Privacy Blueprint, to offer the world a dynamic model of how to provide strong privacy protection and enable ongoing innovation in new information technologies.

Baseline privacy legislation will ground our system firmly, so America can be an example for the world and pave the way for privacy standards that are interoperable around the globe. Leading by example will encourage other countries to build multi-stakeholder processes, flexibility, and accountability into their commercial data privacy networks. This model will promote the free flow of information across national borders, which helps U.S. companies and U.S. consumers alike.

Mr. Chairman, when I speak to international audiences, I point to the deeply held privacy values of Americans that are embedded in our Constitution and in privacy laws that couple statutory protection in areas like health records with strong enforcement by the FTC and by state attorneys general. And I get a lot of thank yous from companies for defending our system.

But they want and they need more. They want the U.S. Congress to send a clear message to the world that the United States cares about privacy and will protect the privacy of consumers in all sectors.

Mr. Chairman, I thank you again for the opportunity to be here today, to provide our views. And I welcome the Committee's questions.

[The prepared statement of Mr. Kerry follows:]

PREPARED STATEMENT OF HON. CAMERON F. KERRY, GENERAL COUNSEL, U.S. DEPARTMENT OF COMMERCE

Summary

Commercial privacy protections have not kept pace with the explosive growth of the Internet. Consumers are deeply concerned about their privacy, but are unable to determine which companies respect their privacy and how their personal data are being collected, stored, and used. Similarly, American businesses need to determine and meet the privacy expectations of their customers in order to maintain their customers' trust, but still wish to innovate within these bounds. Consumers and American businesses share a strong interest in defining and protecting privacy interests to protect consumers, provide a level playing field for businesses, and build an environment of trust that benefits innovation and the digital economy.

To this end, the Administration's Privacy Blueprint articulates a Consumer Privacy Bill of Rights—and calls on Congress to give this baseline privacy protection the force of law. The seven basic principles of the Privacy Blueprint (based on globally recognized Fair Information Practices) are: (1) individual control, (2) transparency, (3) respect for context, (4) security, (5) access and accuracy, (6) focused collection, and (7) accountability. The Administration supports giving the Federal Trade Commission (FTC) the authority to enforce the principles of the Privacy Bill of Rights, as codified. The FTC also should have the authority to provide safe harbors for companies that adopt context-specific codes of conduct that set forth how they will follow the Privacy Bill of Rights. Such codes of conduct should be developed through multistakeholder processes that include broad participation from all interested parties, including consumer groups and businesses.

The Administration supports legislation that provides strong baseline privacy protections in a manner that promotes growth and innovation in the digital economy. Such legislation would allow businesses to implement privacy protections in ways that are specific and appropriate for their industries. It would avoid being too prescriptive or tailored to specific technologies, potentially stifling innovation and inhibiting the development of new products or services, or being so inflexible that it fails to cover the next generation of changes. Nor should legislation impose unnecessary burdens on our businesses. These considerations will help the United States strengthen consumer privacy protections while promoting continued innovation.

I. Introduction

Chairman Rockefeller, Ranking Member Hutchison, and distinguished Committee Members, thank you for the opportunity to testify on behalf of the Department of Commerce about the Administration's recently-released policy blueprint, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (the Privacy Blueprint, attached). I welcome this opportunity to discuss ways to enhance consumer privacy that will foster economic growth, job creation, and exports for American businesses.

As President Obama said in the Privacy Blueprint "[n]ever has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones." The need for privacy protections has grown in proportion to the expansion of the Internet itself. Every day, an increasing share of our commercial transactions, our social interactions, and our participation in public discussion depends on the Internet as a medium. The way we create and share our communications increasingly relies on new technologies that are networked—and increasingly raises new questions about how data associated with these communications are collected, stored, and used. Ultimately, sustaining the social and economic benefits of networked technologies depends on consumer trust. People must have confidence that companies will handle information about them fairly and responsibly.

Privacy protections have not kept up with this explosion of Internet use and new technology. Due to inadequate protection of data, millions of Americans have their personal information exposed in data breaches every year. These breaches lead to concrete harm for consumers: for 12 consecutive years, identity theft has topped consumer complaints received by the FTC, accounting for 15 percent of all complaints.[1]

Consumers also lack transparency into how companies collect and use data. Not only is it a cliché to say nobody reads privacy policies, but studies have indicated that the effort would be hopeless, because an average user would have to devote 250 hours a year just to read the labyrinthine privacy policies of the websites they visit in a year.[2] Even if those policies all provided a clear roadmap to companies' use of data, that is too much to ask; it is as much as 45 minutes of dense textual reading for each and every site visited in a day, a full one-eighth of a working year, *every year,* just to *read* the privacy policies. All the promise of the Internet, and the benefits and efficiencies it can provide, would be dragged down by the anchor of privacy policies if we had to slog through all that, much less negotiate details of sub-optimal privacy policies or find alternative providers for services with unacceptable ones.[3]

Instead, consumers are subject to terms and conditions they have not read or they decide not to use services that may be beneficial and innovative. Neither is a good result. In the first instance, consumers may give up information and rights without understanding the risks sufficiently. In the second instance, commerce and the

---

[1] FTC Releases Top Complaint Categories for 2011: Identity Theft Once Again Tops the List, Feb. 28, 2012, available at *http://ftc.gov/opa/2012/02/2011complaints.shtm*.

[2] Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies,* I/S: A Journal of Law and Policy for the Information Society, 2008 Privacy Year in Review Issue, available at *http://www.is-journal.org/*.

[3] *See http://mashable.com/2011/01/27/the-real-reason-no-one-reads-privacy-policies-infographic/*.

adoption of useful technology are slowed. For example, recent articles about new cloud storage services have recounted how privacy concerns are affecting consumer adoption.[4] In the end, some consumers may use cloud services without reading the privacy policies while others may shy away from such services completely.

At the same time, businesses recognize the need and benefit of baseline privacy legislation. Such legislation would provide rules of the road that would facilitate the flow of information and trade globally while protecting consumers.[5] As one commenter stated: "consumers want it, we believe companies need it, and the economy will be better for it."[6]

The Privacy Blueprint seeks to help consumers navigate the patchwork of privacy expectations that currently exists as they traverse the Internet and to give businesses clearer rules of the road. The goal is both to protect consumers and to ensure that the Internet remains a platform of commerce and growth, and an economic driver for our country. This position may become jeopardized if privacy concerns are not addressed, as consumers across all age ranges report avoiding companies that do not sufficiently protect their privacy.[7] And these concerns are spreading to quickly developing areas of technology, such as mobile computing.[8]

Consumers and American businesses share a strong interest in sustaining the trust that is essential to supporting innovation, keeping the Internet growing, and maintaining the growth of the digital economy. Consumers need ways to get a better understanding about what information is collected about them and how it may be used, as well as safeguards that ensure the information is adequately protected. Businesses need clearer benchmarks for good practices, and companies that handle personal data responsibly should be able to stand out from companies that behave carelessly.

To this end, the Obama Administration has articulated the Consumer Privacy Bill of Rights and called on Congress to adopt this Bill of Rights in privacy legislation that will establish a minimum set of privacy protections for data collected about individual consumers. Such legislation would provide clear protections to consumers, a level playing field for businesses, and foster an environment of trust that will benefit both.

The Administration is not alone in calling for a new law. A broad array of private sector stakeholders has expressed support for baseline consumer privacy legislation. Consumer advocacy groups and civil liberties organizations, for example, have called for baseline consumer privacy legislation. In addition, many businesses also have supported baseline privacy legislation because they see significant value in obtaining clear privacy guidelines that enable them to earn consumers' trust, and which may also enable them to comply with international expectations. These businesses include large technology leaders that handle significant amounts of personal information and have used personal data to provide innovative new products and services.

My testimony today will cover the recommendations of the Administration's Privacy Blueprint. Looking ahead, it will focus on how legislation can implement the Privacy Bill of Rights, how Department of Commerce multistakeholder processes to develop codes of conduct in specific sectors will move forward, and what the Administration is doing to ensure that our privacy framework promotes growth and trade internationally for American companies.

II. The Consumer Privacy Bill of Rights

In 2009, the Department of Commerce assembled an Internet Policy Task Force. This task force spent two years developing a blueprint for protecting consumer's privacy with extensive consultation of stakeholders including consumer advocacy

---

[4] *See e.g.,* PCWorld, *Google Drive Privacy Policies Slammed,* April 28, 2012, available at *http://www.pcworld.com/article/254600/google_drive_privacy_policies_slammed.html*.

[5] *See,* Department of Commerce Internet Policy Task Force's report, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,* at 34, Dec. 2010, available at *http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf*.

[6] *See id,* (quoting Hewlett-Packard Comment at 2).

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

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

groups, businesses, academics, and other government agencies. The task force began by using the information learned from consulting stakeholders to craft a Privacy and Innovation Notice of Inquiry (NOI).[9] The NOI requested public comment on ways of improving privacy protections while still protecting technological innovations. The task force also organized a Privacy and Innovation Symposium on May 7, 2010.

The initial conclusions obtained from stakeholder discussions, the comments received in response to the NOI, and discussions from the symposium led to the publication in December 2010 of *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,* often referred to as the Commerce Green Paper.[10] This Green Paper proposed a privacy framework and invited further comments on the proposed approach. The framework was refined as a result of further comments and meetings with hundreds of stakeholders representing the full spectrum of privacy interests to come up with a final strategy. This was an effort that engaged agencies across the Executive Branch through the National Science & Technology Council Subcommittee on Commercial Privacy that I co-chaired, and benefited from the valuable partnership and advice of the Federal Trade Commission.

Based on our study, in February the White House released its Privacy Blueprint.[11] This Privacy Blueprint calls for the passage of a Consumer Privacy Bill of Rights; for enforceable codes of conduct to implement that Bill of Rights developed by a spectrum of stakeholders from consumer groups, businesses, and others; and for active engagement with international partners to develop privacy protections that enable trustworthy transfer of data across national borders.

Apart from enforcement of consumer protection laws by the Federal Trade Commission and state attorneys general when privacy practices are unfair and deceptive, Federal privacy protections in the United States are based on a sectoral approach that provides privacy protections tailored to specific industries such as finance, health care, and education. Industries that are not subject to such specific privacy laws, however, account for large shares of daily Internet usage; these include search engines, social networking sites, behavioral advertisers, and location-based services. For industries that are not covered by more specific laws, the Privacy Blueprint calls for baseline privacy protections in the form of a Consumer Privacy Bill of Rights.

The Consumer Privacy Bill of Rights articulates a set of principles that clarify to businesses and consumers alike what expectations the consumer should have from their Internet experience. The seven basic principles are:

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

---

[9] Department of Commerce, Notice of Inquiry on Information Privacy and Innovation in the Internet Economy, 75 Fed. Reg. 21226, Apr. 23, 2010, available at *http://www.ntia.doc.gov/files/ntia/publications/fr__privacynoi__04232010.pdf*.

[10] The Privacy Blueprint builds on the Department of Commerce Internet Policy Task Force's report, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,* Dec. 2010, available at *http://www.ntia.doc.gov/files/ntia/publications/iptf__privacy__greenpaper__12162010.pdf*.

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

These principles are based on globally recognized Fair Information Practice Principles (FIPPs), which originated in the Department of Health, Education and Welfare's 1973 report, *Records, Computers, and the Rights of Citizens.* Congress incorporated these principles into the Privacy Act of 1974. Since then, a consistent set of FIPPs has become the foundation for global privacy policy through, for example, the Organization for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("OECD Privacy Guidelines") and the Asia-Pacific Economic Cooperation's Privacy Framework. The Administration sought to remain consistent with these existing globally-recognized FIPPs as it developed the Consumer Privacy Bill of Rights.

Many individuals and organizations that commented on the Commerce Department's Privacy and Innovation Green Paper noted that changes in the ways information is generated, collected, stored, and used called for some adaptation of existing statements of the FIPPs. The digital economy of the 21st Century, driven by distribution of devices and connectivity and vast increases in computing speed, storage capacity, and applications, is data-intensive, dynamic, and increasingly driven by consumers' active participation. We therefore updated the traditional FIPPs to suit the challenges posed by the digital economy. The most significant changes are found in the principles of Individual Control, Respect for Context, Focused Collection, and Accountability.

1. Individual Control

The principle of Individual Control addresses two salient aspects of the networked world. First, networked technologies offer consumers an increasing number of ways to assert control over what personal data is collected. Companies should take advantage of these technologies by offering consumers, at the time of collection, usable tools and clear explanations of their choices about data sharing, collection, use, and disclosure.

Second, the Individual Control principle calls on consumers to use these tools to take responsibility for controlling personal data collection, especially in situations where consumers actively share data about themselves, such as online social networks. In these cases, control over the initial act of sharing is critical. Consumers can take significant steps to reduce harms associated with the misuse of their data by using improved tools available to gain a better understanding of what personal data they are disclosing and to control their data.

2. Respect for Context

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

The Respect for Context principle embodies the flexibility that is at the core of the Consumer Privacy Bill of Rights: it calls for strong protection when the context indicates—when sensitive personal information is at stake, for example—but personal data can flow relatively freely to support purposes that consumers reasonably anticipate in a given context.

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

Similarly, explicit consent may not be required for the use of a consumer's address for the delivery of a product ordered online, but if that company sells the information to a third party such consent may be necessary. Requiring explicit consent in every case inures consumers to accepting all terms and conditions presented to them while limiting such consent to unexpected uses of consumer data empowers consumers.

The sophistication of a company's customers is an important element of context. In particular, the unique characteristics of children and teenagers may warrant different privacy protections than are suitable for adults. Children are particularly susceptible to privacy harms.[12] The Administration looks forward to exploring with stakeholders whether more stringent applications of the Consumer Privacy Bill of Rights—such as an agreement not to create individual profiles about children, even if online services obtain the necessary consent from the child to collect personal data—are appropriate to protect children's privacy.

3. Focused Collection

The Focused Collection principle adapts the "data minimization" and "collection limitation" principles found in traditional FIPPs. Some existing versions of these principles provide a strict standard that makes personal data collection permissible only when it is kept to the minimum necessary to achieve specific, identified purposes. Such a one-size-fits-all standard is unworkable for the networked technologies and new data uses that enable the digital age.

Familiar and increasingly essential Internet services, such as search engines, collect a wide range of data and use it in a wide variety of ways that cannot be predicted when the data is collected. Stores of information like these have the potential to provide new frontiers of human knowledge in addition to new pathways for intrusion on privacy. Such services may be consistent with the Focused Collection principle, provided they reflect considered decisions about what kinds of personal data are necessary to provide the services, how long the data needs to be retained, and what measures may be available to make retained data less likely to be associated with specific consumers. Focused collection will help protect consumers from harm associated with misuse of data that never needed to be collected or retained to begin with. The Focused Collection principle, however, does not relieve companies of any independent legal obligations, including law enforcement orders, that require them to retain personal data.

4. Accountability

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

III. Legislation

A. Codify Baseline Privacy Protection Principles

The Privacy Bill of Rights establishes a set of expectations that consumers can use to understand what they should expect from businesses they deal with, and businesses can use to guide their privacy policies and practices. It establishes a benchmark that consumer and privacy groups, journalists, and policymakers can use to gauge privacy practices. Businesses that incorporate the Bill of Rights into their practices will help differentiate themselves as trustworthy stewards of personal information, enhancing competition based on privacy protection.

These changes can begin without legislation, but the Administration urges Congress to strengthen baseline privacy protections for consumers and to support continued consumer trust in the digital economy by codifying the Consumer Privacy Bill of Rights as part of baseline commercial privacy legislation. The Consumer Privacy Bill of Rights sets forth fundamental protections that have been well received

---

[12] *See* Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,* at 63, March 2012 ("when health or children's information is involved, for example, the likelihood that data misuse could lead to embarrassment, discrimination, or other harms is increased.").

by both consumers and businesses, and legislation is supported by businesses as well as civil society.

The Commerce Committee has a long history of avoiding technical mandates in legislation, which the Administration applauds. The principles in the Privacy Bill of Rights are intentionally broad to avoid technical mandates or excessively prescriptive requirements. The digital economy is constantly changing as are the risks and solutions to consumer privacy concerns. Legislation that is too prescriptive or that allows government to dictate specific technologies may stifle innovation and inhibit the development of new products or services. Similarly, legislation should not impose unnecessary burdens on all businesses to address a privacy concern that is relevant only to a subset of companies. Privacy legislation should be broad and flexible enough to cover existing services as well as future products and services that raise unforeseen concerns. Enactment of the Privacy Bill of Rights as a set of legally enforceable rights would provide strong baseline privacy protections and permit flexibility both in enforcement and in industry compliance.

The Administration Privacy Blueprint recommends two mechanisms to apply the broad principles of the Privacy Bill of Rights to specific circumstances or practices. The first is enforcement of the Bill of Rights by the FTC and state attorneys general. The second is the development of legally enforceable codes of conduct through a voluntary multistakeholder process convened by the National Telecommunications & Information Administration (NTIA) of the Department of Commerce.

B. Grant Direct Enforcement Authority to the FTC

The Administration supports giving the FTC the direct authority to enforce the individual provisions of the Consumer Privacy Bill of Rights as enacted in law rather than relying only on its authority under Section 5 of the FTC Act to address unfair and deceptive practices or acts. Under Chairman Leibowitz as well as under Republican-appointed chairs in the preceding decade, the FTC has developed a body of law as well as expertise in privacy using its Section 5 authority. Giving the FTC direct authority to enforce the Bill of Rights would give future direction to this body of law, strengthen protection of consumers, and permit the FTC to address emerging privacy issues through specific enforcement actions governed by applicable procedural safeguards.

Baseline privacy protections enforced by the FTC would provide a level playing field for companies. Currently, a number of companies offer consumers strong privacy protections. Bad actors, however, are abusing the trust of consumers and using their information in ways not reasonably expected by their customers. Such actions undermine consumer trust in the digital economy to the detriment of businesses and consumers alike. Granting direct enforcement authority to the FTC would enable the Commission to take action against outliers and bad actors even if their actions do not violate a published privacy policy so as to constitute a deceptive practice or act.

C. Safe Harbor for FTC Approved Codes of Conduct Developed Through Multistakeholder Processes

The Administration also supports the use of multistakeholder processes to address consumer privacy issues that arise and change as quickly as networked technologies and the products and services that depend on them. These processes should be open to a broad range of participants, including companies, privacy advocates, academics, and civil and criminal law enforcement representatives, and facilitate their full participation to find creative solutions through consensus building. Specifically, the Privacy Blueprint directs the Department of Commerce, through the NTIA, to convene interested stakeholders to address consumer privacy issues in transparent, consensus-based processes that are open to all interested stakeholders.

The Administration supports codifying this role for NTIA in baseline privacy legislation because legislation would reinforce NTIA's mission and its ability to convene stakeholders. Under the Administration's recommended framework, companies would face a choice: follow the general principles of the statutory Consumer Privacy Bill of Rights, or commit to following a code of conduct that spells out how those rights apply to their businesses. If the FTC determines that this code of conduct adequately implements the Consumer Privacy Bill of Rights, the FTC would forbear from enforcing the provisions of the Consumer Privacy Bill of Rights implemented in the code of conduct against companies that subscribe to it, so long as they live up to their commitment. This approach would provide greater certainty for companies and stronger incentives for all stakeholders to work toward consensus on codes of conduct, but it requires authority from Congress to work most effectively.

There is a model for this safe harbor approach in the context of privacy in the Children's Online Privacy Protection Act of 1998 (COPPA). The FTC has years of

experience in implementing COPPA and the statute has been praised for providing parents with the tools they need to protect the privacy of children under 13.

The expected outputs of these multistakeholder processes are context-specific codes of conduct that companies may choose to adopt as public commitments setting forth how they will follow the Privacy Bill of Rights. Once a company publicly commits to follow a code of conduct, the Administration expects that this commitment will be enforceable by the FTC and state attorneys general, just as companies' privacy policies and other promises are enforceable today.

The multistakeholder approach to privacy will strike a balance between certainty for companies, strong protections for consumers, and the flexibility necessary to promote continued innovation. Implementing the general principles in the Consumer Privacy Bill of Rights, as enacted in legislation, across the wide range of innovative uses of personal data should allow for a flexible, fast-paced process to determine how to define concrete practices that embody the broader principles in a specific setting. This process must be capable of addressing consumer privacy issues that arise and change quickly in the networked world. In addition, it should focus on specific business settings to help stakeholders address concrete privacy issues and business requirements, leading to practices that protect privacy without discouraging innovation. The process must also allow a broad range of stakeholders, including consumer groups and privacy scholars to participate meaningfully so they can ensure the codes of conduct carry out the principles of the Privacy Bill of Rights. For consumer and privacy advocates, the privacy multistakeholder process provides an opportunity to influence these practices through direct engagement with companies.

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

Thoughtful and balanced baseline commercial privacy legislation is good for consumers and industry. As the digital economy opens the world to commerce and social interactions, the United States should provide the leadership necessary to promote consumer privacy and trust in a manner that promotes innovation and competition. We should not cede this role to other countries that may impose unnecessarily restrictive burdens on U.S. industry with little or no consumer benefit.

The Administration is developing specific statutory suggestions to implement the Consumer Privacy Bill of Rights and welcome the opportunity to work with this Committee to enact baseline privacy legislation.

IV. Developing Enforceable Codes of Conduct through Multistakeholder Processes

The Administration has begun to take action to implement the Consumer Privacy Bill of Rights before baseline legislation is enacted. NTIA has begun to move ahead with stakeholder-driven processes to develop codes of conduct based on the Bill of Rights.

Immediately after the Privacy Blueprint was issued, NTIA sought comment from stakeholders on two sets of questions: which substantive issue is suitable for an initial effort to develop an enforceable code of conduct, and what procedures should the process to address this issue follow. NTIA suggested a number of substantive issues that are relatively discrete and manageable with the potential to deliver significant benefits to consumers through a code of conduct. The request asked stakeholders to comment on the pros and cons of taking up these issues and to offer other issues that meet the criteria of definability and potential consumer benefit. NTIA also asked for input on procedures that will make the process manageable yet open to all interested stakeholders' participation, transparent, and consensus-based.

The comment period closed on Monday, April 2, and the Commerce Department is in the process of reviewing the submissions. NTIA received comments from consumer groups, businesses, academics, and Members of Congress, including the Chairman of this Committee.

I anticipate that NTIA will soon select an initial topic and convene an initial public meeting to begin developing a code of conduct. Part of the business of this initial meeting will be for stakeholders to reach agreement on the procedures they will use to work together. While NTIA likely will provide some guidance and perspective, based on its participation in other multistakeholder processes as well as its review of comments on this process, NTIA will avoid imposing its judgment on the group.

In other words, NTIA's role will be to convene stakeholders and facilitate discussions that ensure all voices are heard, but it will not be the decision-maker on the substantive elements of privacy codes of conduct. The government's role will be as a convener and a facilitator to forge consensus.

V. International Interoperability

What we do here in America is of paramount importance to U.S. consumers and companies, but we cannot ignore the global dimensions of the Internet. The dynamism of the digital economy is linked directly to flows of data across borders. This is why an essential element of the Administration's Blueprint for consumer privacy is international engagement.

Americans expect to follow blog posts and tweets from around the world. We expect our e-mail to pop-up nearly instantaneously without thinking about whether it crossed national borders to get there. We demand information, goods, and services 24 hours a day, 7 days a week, regardless of whether they are provided from across town or across the globe.

In today's digital economy it is vital to maintain cross-border data flows to keep U.S. businesses tapped into the markets of the world and drive the continued growth of this sector. Over $8 trillion were exchanged over the Internet last year, and this amount is growing.[13] The digital economy accounted for 15 percent of U.S. GDP growth over the five-year period from 2004 to 2009.[14] Total retail e-commerce sales for 2011 reached an estimated $194.3 billion, 16.1 percent more than in 2010, and accounting for 4.6 percent of total retail sales versus 4.3 percent in 2010.[15] We must ensure that American companies that are leaders in Internet technology, cloud computing, and e-commerce, as well as innovative startups, have continued access to markets unimpeded by regulations that erect barriers to information flow at national borders and Balkanize the Internet. To do this, the United States must remain on the cutting edge of the digital economy in terms of both technology and policy-making as it relates to the Internet.

The Privacy Blueprint recognizes that international interoperability should start with mutual recognition of commercial data privacy frameworks. The Department of Commerce has been at the forefront of commercial privacy interoperability efforts, beginning with our negotiation of the U.S.-EU Safe Harbor Framework in 2000 and most recently with our leadership in the development of a system of Cross Border Privacy Rules in the Asia Pacific Economic Cooperation. Recently, Secretary Bryson and European Commission Vice President Reding reaffirmed their commitment to the U.S.-EU Safe Harbor Framework in a joint statement stating, "[t]his Framework, which has been in place since 2000, is a useful starting point for further interoperability. Since its inception, over 3,000 companies have self-certified to the Framework to demonstrate their commitment to privacy protection and to facilitate transatlantic trade. The European Commission and the Department of Commerce look forward to continued close U.S.-EU collaboration to ensure the continued operation and progressive updates to this Framework."

We look forward to exploring additional interoperability mechanisms with our European partners in particular, because they are in the midst of reviewing their privacy framework. Our European partners have taken note of our multistakeholder approach. Although domestically focused, the codes of conduct developed through the multistakeholder process could have global relevance, because consumers around the world are faced with similar privacy challenges.

Alongside these international initiatives, privacy legislation will firmly ground our consumer data privacy system here so that we can set the best example for the world and set the stage for necessary mutual recognition by other countries. Leading by example will encourage other countries to build multistakeholder processes, transparency, and flexibility into their commercial data privacy frameworks. This

---

[13] Bipartisan Policy Center, *FCC Chairman Julius Genachowski: Prepared Remarks on Cybersecurity;* Feb. 22, 2012, *http://transition.fcc.gov/Daily__Releases/Daily__Business/2012/db0222/DOC–312602A1.pdf,* at 1.

[14] McKinsey Global Institute, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity,* May 2011, *http://www.mckinsey.com/Insights/MGI/Research/Technology__and__Innovation/Internet__matters* at 15–16.

[15] U.S. Census Bureau, *Quarterly Retail E-Commerce Sales: Fourth Quarter 2011,* Feb. 16, 2012, *http://www.census.gov/retail/mrts/www/data/pdf/ec__current.pdf,* at 1.

will help foster the free flow of information, which will benefit U.S. companies and consumers alike. We should anchor our own consumer data privacy system in law to guarantee the international interoperability our companies and our citizens need.

This is a critical time in the world of consumer data privacy. Europe is in the process of honing its approach to data privacy, and other countries around the world are starting to understand the need for rules of the road for the increasingly data-driven digital economy. We have a clear opportunity, as President Obama said to "offer to the world a dynamic model of how to offer strong privacy protection and enable ongoing innovation in new information technologies." It is incumbent upon us to take the reins of the digital economy and ensure its forward momentum.

VI. Conclusion

We ask Congress to give the Consumer Privacy Bill of Rights the force of law. These rights will provide protection for consumers and define comprehensible rules of the road for the rapidly growing marketplace for personal data. As envisioned in the Administration's Privacy Blueprint, the Consumer Privacy Bill of Rights would provide a set of standards that many responsible companies are already meeting, and legislation would serve to put these companies on a level playing field with those who are less careful with personal data.

Mr. Chairman, thank you again for the opportunity to provide our views on legislation to protect consumer privacy and promote innovation in the 21st Century. We look forward to working with you and other stakeholders toward enactment of these consumer data privacy protections. I welcome any questions.

The CHAIRMAN. Thank you very much, sir.

Commissioner Ohlhausen, welcome.

STATEMENT OF HON. MAUREEN K. OHLHAUSEN, COMMISSIONER, FEDERAL TRADE COMMISSION

Ms. OHLHAUSEN. Thank you. Chairman Rockefeller, Ranking Member Toomey, and members of the Committee, I'm pleased to join Chairman Leibowitz, who is presenting FTC's testimony, and Cameron Kerry, General Counsel of the Department of Commerce.

Privacy is an important topic for American consumers, and I commend you for holding this hearing. But let me say at the outset that my comments and the views expressed in this statement are my own and do not necessarily represent the views of the Commission or any other commissioner.

As you know, my tenure as an FTC commissioner began on April 4, so while privacy is an issue in which I have tremendous interest and commitment, my views on privacy from the perspective of a commissioner are just over a month old.

While I have read the March 2012 privacy report and formed some initial thoughts, I was not at the Commission during its development and release. I'm just now in the process of fully educating myself on the specifics of the report and thinking through the implications of its recommendations. So I'm not yet ready to commit myself to specific positions on all aspects of the privacy issues raised in the report.

I am, however, happy to share some of my preliminary views on the best ways to safeguard consumer privacy, as well as my thoughts about where the Commission should deploy its resources.

To start, I firmly believe that consumers should have the tools to protect their personal information through transparency and choice. As I said during my confirmation hearing, I support the FTC's strong record of enforcement in the area of privacy. The Commission's written testimony highlights many of our enforcement efforts relating to privacy and data security.

The FTC has brought more than 100 spam and spyware cases, and more than 30 data security cases, including cases against ChoicePoint, CVS, and Twitter. We have also charged companies with failing to live up to their privacy promises, as in the highly publicized privacy cases against companies such as Google and Facebook, which together will protect the privacy of more than 1 billion users worldwide.

As a commissioner, I will urge continuation of this strong enforcement record.

As I also said in my confirmation hearing, I support enactment of data security legislation. The legislation should empower the FTC to promulgate regulations for the protection of personal data from unauthorized access, as do the current bills by Chairman Rockefeller and Chairman Pryor.

As a parent, I am especially concerned about protecting our children's privacy in the face of rapid technological advances. I support the commission's multipronged approach in this area: enforcement, regulation, policy, research, and education.

Since the enactment on the Children's Online Privacy Protection Act of 1998 (COPPA), the Commission has brought 18 COPPA enforcement actions. In the ongoing proceeding to amend the rule, I will carefully consider the record as I formulate my views.

Turning to the Commission's privacy report, I would like to commend some important aspects of it. It calls for a policy of privacy by design, by which companies build privacy protections into their everyday business practices. This helps minimize the risk of privacy breaches and concerns from the outset and should be considered a best practice by companies as they develop new products and services.

Appropriate use of the notice and choice concept is also core to a sound privacy policy. And I support the report's recognition that there is no single best way to offer notice and choice in all circumstances. I also agree with the concept of reducing burdens on consumers and businesses by identifying circumstances for which choice is not necessary because the collection and use of consumer data is consistent with the context of the transaction or with the relationship with the consumer.

As I have already noted, Congress has given the commission enforcement and policy tools to provide a strong framework with which we can protect American consumers. Some of my colleagues, however, have supported additional privacy legislation that would go beyond Section 5. The exact contours of such legislation are not yet defined, but my colleagues gave general guidance in the privacy report.

The privacy report was clear, however, that the recommended legislation would reach practices that would not be challenged under the current interpretation of Section 5, however.

I believe this gives me the opportunity to develop my own opinion on what else, in addition to Section 5, may be beneficial to consumers, such as whether additional general privacy legislation is needed. I will consult with FTC staff, my fellow commissioners, as well as many other stakeholders, to gather their views on what problems and possible solutions they see in the area of consumer privacy.

Some of the issues I will examine are what harms are occurring now that Section 5 cannot reach, and how should harm be measured? As my colleague, Commissioner Rosch, noted in his dissent to the privacy report, the Commission has, in the past, specifically advised Congress that, absent deception, it will not enforce Section 5 against alleged intangible harm.

And the FTC's own unfairness statement suggests that the focus should be on monetary, as well as health and safety harms, rather than on more subjective types of harm.

Although the Commission's privacy report did not reject the fundamental insight of the harm-based approach, it appears to embrace an expansion of the definition of harm to include reputational harm or the fear of being monitored or other intangible privacy interests. As an initial matter, I have reservations about such an expansion.

Even absent deception, financial and medical information is protected under current law, which likely reflects most consumers' expectations. In other areas, however, consumers appear to have diverse views about sharing information. Thus, it is important to proceed carefully to avoid impinging on many consumers' preferences.

If a consumer is provided with clear notice prior to the collection of information, there is likely no basis for concluding that a consumer cannot make an informed choice.

I would also like to find out more about the progress of the self-regulatory and technology-based efforts underway to provide consumers greater transparency in choice about the collection and use of their data.

Finally, new restrictions may also have an effect on competition by favoring entrenched entities that already have consumer information over new entrants who need to obtain such information, or encouraging industry consolidation for purposes of sharing data. As a competition agency, the FTC should be sensitive to these concerns as well.

Clearly, the technology sector is developing at lightning speed, and we now face issues unheard of even a few years ago. I wish to proceed cautiously in exploring the need for any additional general privacy legislation, however.

I have concerns about the ability of legislative or regulatory efforts to keep up with the innovations and advances of the Internet without also imposing unintended, chilling effects on many of the enormous benefits consumers have gained from these advances, or without unduly curtailing the development in success of the Internet economy.

Thank you for allowing me to participate in today's hearing. This committee has shown strong leadership in the area of consumer privacy, and I look forward to working with you to ensure that American consumers' privacy is protected. Thank you.

[The prepared statement of Ms. Ohlhausen follows:]

PREPARED STATEMENT OF MAUREEN K. OHLHAUSEN, COMMISSIONER, FEDERAL TRADE COMMISSION

Chairman Rockefeller and members of the Committee. I am pleased to join Chairman Leibowitz, who is presenting the FTC's testimony and Cameron Kerry, General Counsel at the Department of Commerce. This is an important topic for American consumers and I commend you for holding this hearing. Let me say at the onset

of my comments that the views expressed in this statement are my own and do not necessarily represent the views of the Commission or any other Commissioner.

As you know, my tenure as an FTC Commissioner began on April 4. So while privacy is an issue in which I have tremendous interest and commitment, my views on privacy from the perspective of a Commissioner are just over a month old. While I have read the March 2012 Privacy Report and formed some initial thoughts, I was not at the Commission during its development and release. I am just now in the process of fully educating myself on the specifics of the report and thinking through the implications of its recommendations. So, I am not yet ready to commit myself to specific positions on all aspects of the privacy issues raised in the Report.

I am, however, happy to share some of my preliminary views on the best ways to safeguard consumer privacy as well as my thoughts about where the Commission should deploy its resources. To start, I firmly believe that consumers should have the tools to protect their personal information through transparency and choices. As I said during my confirmation hearing, I support the FTC's strong record of enforcement in the area of privacy. The Commission's written testimony highlights many of our enforcement efforts relating to privacy and data security. The FTC has brought more than a hundred (100) spam and spyware cases and more than thirty (30) data security cases, including cases against ChoicePoint, CVS, and Twitter. We have also charged companies with failing to live up to their privacy promises, as in the highly publicized privacy cases against companies such as Google and Facebook, which together will protect the privacy of more than one billion users worldwide. As a Commissioner, I will urge continuation of this strong enforcement record.

As I also said in my confirmation hearing, I support enactment of data security legislation. The legislation should empower the FTC to promulgate regulations for the protection of personal data from unauthorized access, as do the current bills by Chairman Rockefeller and Chairman Pryor.

As a parent, I am especially concerned about protecting our children's privacy in face of rapid technological advances. I support the Commission's multi-prong approach in this area: enforcement, regulation, policy research, and education. Since the enactment of the Children's Online Privacy Protection Act of 1998, the Commission has brought eighteen (18) COPPA enforcement actions. In the ongoing proceeding to amend the rule, I will carefully consider the record as I formulate my views.

Turning to the Commission's Privacy Report, I would like to commend some important aspects of it. It calls for a policy of "privacy by design" by which companies build privacy protections into their everyday business practices. This helps minimize the risk of privacy breaches and concerns from the outset and should be considered a best practice by companies as they develop new products and services.

Appropriate use of the "notice and choice" concept is also core to a sound privacy policy, and I support the Privacy Report's recognition that there is no single best way to offer notice and choice in all circumstances. I also agree with the concept of reducing burdens on consumers and businesses by identifying circumstances for which choice is not necessary because the collection and use of consumer data is consistent with the context of the transaction or with the relationship with the consumer.

As I have noted, Congress has given the Commission the enforcement and policy tools to provide a strong framework with which we can protect American consumers. Some of my colleagues, however, have supported additional privacy legislation that would go beyond Section 5. The exact contours of such legislation are not yet defined, but my colleagues gave general guidance in the privacy report. The privacy report was clear that the recommended legislation would reach practices that would not be challenged under current Section 5, however.

This gives me the opportunity to develop my own opinion on what else in addition to Section 5 may be beneficial to consumers, such as whether additional general privacy legislation is needed. I will consult with FTC staff, my fellow Commissioners, as well as many other stakeholders to gather their views on what problems and possible solutions they see in the area of consumer privacy.

Some of the issues I will examine are:

> What harms are occurring now that Section 5 cannot reach and how should harm be measured? As my colleague Commissioner Rosch noted in his dissent to the Privacy Report, the Commission has specifically advised Congress that absent deception, it will not enforce Section 5 against alleged intangible harm, (FTC letter to Ford and Danforth, 1984), and the FTC's own unfairness statement suggests that the focus should be on monetary as well as health and safety harms, rather than on more subjective types of harm. Although the Commis-

sion's Privacy Report did not reject the fundamental insights of the harm-based approach, it appears to embrace an expansion of the definition of harm to include "reputational harm," or "the fear of being monitored," or "other intangible privacy interests" (*see* Report at iii, 20, 31), and, as an initial matter, I have reservations about such an expansion.

Thus, even absent deception, financial and medical information is protected under current law, which likely reflects most consumers' expectations. In other areas, however, consumers appear to have diverse views about sharing information. Thus, it is important to proceed carefully to avoid impinging on many consumers' preferences. If a consumer is provided with clear notice prior to the collection of information, there is likely no basis for concluding that a consumer cannot make an informed choice.

I would also like to find out more about the progress of the self-regulatory and technology based efforts underway to provide consumers greater transparency and choice about the collection and use of their data.

Finally, new restrictions may also have an effect on competition by favoring entrenched entities that already have consumer information over new entrants who need to obtain such information, or encouraging industry consolidation for purposes of sharing data. As a competition agency, the FTC should be sensitive to these concerns as well.

Clearly, the technology sector is developing at lightning speed and we now face issues unheard of even a few years ago. I wish to proceed cautiously in exploring the need for any additional general privacy legislation, however. I have concerns about the ability of legislative or regulatory efforts to keep up with the innovations and advances of the Internet without also imposing unintended chilling effects on many of the enormous benefits consumers have gained from these advances or without unduly curtailing the development and success of the Internet economy.

Thank you for allowing me to participate in today's hearing. This Committee has shown strong leadership in the area of consumer privacy, and I look forward to working with you to ensure that American consumers' privacy is protected. I am happy to answer any questions.

The CHAIRMAN. Thank you very much, Commissioner.

I'll start with the questioning. I'll make this one to Chairman Leibowitz.

The Digital Advertising Alliance has spent a lot of time developing its own consumer guidelines, and they have pledged to follow these guidelines and honor their customers' privacy concerns. And that's a good thing.

But we all know, at least I know, that in spite of their good intentions, and you just see this so many times, whether it's a coal mine, whether it's natural gas, whether it's a telephone company, whatever, whatever, whatever, repeats and repeats, sometimes industries' self-regulatory efforts do not end up protecting consumers.

In my experience, corporations are unlikely to regulate themselves out of profits. Let me give you an example.

Back in the 1990s, consumers were getting bogus charges crammed, which you referred to, on their telephone bills. And one, I suppose, could say that consumers should understand everything on their telephone bills, and once they've read it in writing, if they can see the writing, they're so informed, and, therefore, their responsibilities have been replete.

The big telephone carriers came to Congress at that time, back in the 1990s, and they told us that they would take care of this problem. They told us Congress didn't have to pass a law, and that they would eliminate cramming on its own.

As you well know, Chairman Leibowitz, the telephone industries' efforts to stop cramming were a huge failure. But my question to

you is why might the DAA's self-regulatory effort have a better chance of succeeding?

Mr. LEIBOWITZ. Well, let me just start by saying, as you know, we brought a major cramming case today. It was a contempt action against a company that we believe had violated an order.

And when I heard Senator Toomey say "a 20-year order," when I first got to the Commission, I wondered why do we have 20-year orders? We have 20-year orders because this contempt action came 13 years after we put this company under order. We think it was more than $50 million in injury to consumers with bogus charges placed on their bills.

So we want to work with you and this committee, in a bipartisan way, to stop cramming.

With respect to the Digital Advertising Alliance, I think they have made meaningful progress, and I do think that Do Not Track will be available for consumers, I'm optimistic, by the end of the year, one way or another, with your support and with your efforts.

I would say this, though. We have to make sure that Do Not Track, with a few enumerated exceptions for anti-fraud efforts, is about "do not collect." It can't be, "I can collect consumers' information but then I just won't target them with advertisements, but I will monetize it, I will sell it."

The CHAIRMAN. You cut it off at the starting point. You cut it off at the starting point.

Mr. LEIBOWITZ. I cut it off at the starting point?

The CHAIRMAN. Yes.

Mr. LEIBOWITZ. Did you want me to——

The CHAIRMAN. No, no forget it.

Mr. LEIBOWITZ. Right, sorry.

Anyway, so I think we have to work on it.

I will say this, going back to points that several of you have made, I was on a West Coast trip to the Bay Area, meeting with a bunch of technology companies, and they were wonderful. We talked about privacy. We talked about competition issues. This was just a few weeks ago. And all of them want to be helpful on privacy. A lot of them wanted to be helpful on Do Not Track.

And indeed, we're not debating anymore about whether there will be a Do Not Track initiative. The industry alliance has said they will support a form of Do Not Track. The only question is precisely what will be in it and when it will be effectuated.

But one of the things I heard is that companies are sometimes concerned that they want to do the right thing, but they don't want to be at a competitive disadvantage. And that's why I think your efforts are very, very helpful here.

The CHAIRMAN. My time is not up.

So you go back to the DAA, and they say they're going to do this on their own. But my understanding is that the DAA effort leaves some rather large loopholes, as you've observed at least to this point, and I'd like to know about that.

Mr. LEIBOWITZ. Well, I think it depends on what the exceptions might be to allowing consumers to opt out from third party tracking. So if it's just for anti-fraud purposes and perhaps for what's known as frequency capping, so people don't get the same ad sent to them over and over and over, that might be legitimate.

If it applies to things like marketing research, it depends on how it's defined, because you certainly don't want a loophole that swallows up the commitment. That's why I think your hearing next week will be very important.

The CHAIRMAN. Yes, we're going to have that hearing.

Mr. LEIBOWITZ. I know.

The CHAIRMAN. Thank you.

Senator Toomey?

Senator TOOMEY. Thanks very much, Mr. Chairman.

Just to be very clear, I think I know how you'll answer this, but Section 5 of the FTC Act does authorize and empower the Commission to make enforcement actions against a company that violates its own stated privacy policy.

Do any of you believe that you lack sufficient enforcement authority in that regard and need any kind of legislative change, in that respect?

Mr. LEIBOWITZ. So I would say it's a terrific tool for us, but it doesn't do everything.

We have brought a number of cases, as Commissioner Ohlhausen mentioned, about companies that have violated their privacy commitments to consumers, probably more than 40, including ones against Facebook and Google.

Having said that, there are a lot of gaps in the law. So for example, we did a report on kids' privacy applications, "apps," that go to kids through either the Android Google system or through the Apple store.

So these apps are great for kids, but only about a quarter of them had privacy policies. We can't mandate a privacy policy, but I think everyone understands that privacy policies would be a useful thing to have.

Now, we've gone back, and we've talked to Apple and Google. And they want to work with us to ensure that there are privacy policies, so parents know what they're giving to their children when they're putting kids' apps on their iPhones or their smartphones.

But part of the reason I think that the majority of the Commission is supportive of general privacy legislation, and you have to get it right of course, is because it would fill in gaps. Part of it is because I think a lot of businesses want more certainty that you can get when you're not taking a case-by-case approach, which is what we have to do now.

We do case-by-case, and we do policy. We don't really do regulations, except where it comes to kids' privacy, and that's because Congress gave us specific authority to.

Ms. OHLHAUSEN. So that is one of the things that I want to examine, as I get more settled in as commissioner, is if there are things that the FTC's current authority can't reach.

But initially, I would say if there's a deceptive statement in a privacy policy, that is a very straightforward case for the FTC, and it's successfully brought very many of them.

Senator TOOMEY. And that was my question.

Ms. OHLHAUSEN. OK.

Mr. LEIBOWITZ. Yes.

Senator TOOMEY. So with respect to a violation of a stated policy, nobody feels as though there is any ambiguity or insufficient authority?

Ms. OHLHAUSEN. Correct.

Mr. LEIBOWITZ. None.

Senator TOOMEY. OK.

I think everybody here acknowledges, but just to be clear, do you all agree that there are many companies operating on the Internet that actively compete on the basis of the privacy policies that they offer, that that is one of the features that they bring attention to?

Mr. LEIBOWITZ. I think that's a good point. And I think we have started to see that. And of course, you know, one side of our agency is consumer protection and the other side is competition, and so we like to see that.

I believe when Google changed its privacy policy, effective, I think, at the beginning of March, Microsoft had full-page ads in the *New York Times* saying, you know, "If you want more privacy protection, use Bing."

So, yes, we're starting to see that.

Ms. OHLHAUSEN. I believe that companies are starting to compete on those issues. But of course, that has to be based on consumer interest. That's an attribute that consumers care about. So it's a little circular.

Senator TOOMEY. Well, that's the nature of the beast. If there's a feature that is important to consumers, business, pursuing their own self-interest, will, in fact, try to attract consumers by providing that feature, and they will compete on that basis.

I find your discussion about Do Not Track very interesting. As I understand it, this is an industry effort. This is not mandated by legislation.

Mr. LEIBOWITZ. Correct.

Senator TOOMEY. It's not mandated by regulation. It's a voluntary approach, which you're commending and which the industry apparently sees as in its own interest to pursue.

So what do you think of this dynamic, whereby an industry, presumably with input from consumers, discovers a process that works for both?

Mr. LEIBOWITZ. Well, on Do Not Track, I think the majority of the commission is very supportive of this process. They are making meaningful progress.

Now I think part of that is because companies want to do the right thing. Part of it may be that the Chairman's legislation is out there, and I think it probably has a fair amount of support.

But we see progress, and we're hopeful that, one way or another, we get to the finish line by the end of the year.

Again, some of it depends on precisely what's in the Do Not Track effort, but we do commend their progress.

Mr. KERRY. Senator Toomey, there is competition on privacy offerings. We would like to see more competition. Part of the reason to introduce a set of privacy principles, including transparency and control, is to create more of an active conversation between businesses and consumers, so consumers can make choices, understand the benefits.

The problem with existing law today, the reason that we believe that additional FTC authority is required, is that too much hangs on privacy policies. And there's research out there that indicates that you have to spend 250 hours a year to read every single privacy policy for the average consumer. That's just not something that people are able to do.

So people don't really have a choice about the contents of what's in a private policy. And as Chairman Leibowitz mentioned, there are companies out there that don't have privacy policies, and the existing authority doesn't reach those.

So what the FTC found about mobile apps is consistent with a broader survey of the top 50 applications found. Only a third of them had privacy policies.

So how do you deal with people that don't have privacy policies? There are no promises that you can hold them to under Section 5.

Senator TOOMEY. I want to point out, if I could, in closing, the premise here is, of course, that consumers want these privacy features that you're advocating are not available. And so the premise is there's this huge untapped potential in the marketplace that nobody has been smart enough to figure out.

Because if all of that is true, of course, there's a huge incentive for a company to simply offer those policies, advertise extensively, and then take all kinds of market share away from the not-so-clever competitors who haven't figured out that that's important to consumers.

So I think that we ought to proceed very cautiously when that's an underlying assumption.

The CHAIRMAN. I'll call on Senator Kerry, but I have to point out, Senator Toomey, that's an outstanding assertion, outstanding degree of faith in the knowledge and time of the people.

Senator Kerry?

Senator KERRY. Thank you, Mr. Chairman.

Commissioner Ohlhausen, eBay, Hewlett Packard, Microsoft, Intel, Verizon, other industry leaders, support the legislation that Senator McCain and I have introduced. Obviously, these are all capable companies and important to consumers, et cetera.

You said there might be an unintended chilling effect. They don't see an unintended chilling effect. They've signed up. They think this is important.

Do you not have faith in the American consumer, if they're given choices, that they can make those choices? And what's the unintended chilling effect to the American consumer?

Ms. OHLHAUSEN. Thank you, Senator Kerry. You raise a very important issue. And that's one of the things that I want to explore.

As I said, I'm one month into my tenure, and this is one of the things I want to find out more about.

But I do think that there is the possibility that companies that are already entrenched and have the data that they need to create their products may not have the same concerns as a new company that may have a new product that we haven't even thought of yet that may use consumer data in a different way.

Senator KERRY. But they're all going to be held to the same standard. The issue here is the individual American consumers' privacy. I mean, they're all going to be held to the same standard.

I mean you've set forth the idea that, conceivably, I think you have an economic or physical harm standard that you are applying. But the problem is, what happens if there is, you know, if no risk of economic or physical harm can be proven, but something very personal to people is exposed, a health issue, that they might have cancer? What if their sexuality is exposed? What if they might be having an affair or something, and that's exposed?

That's damage. It's a violation of their privacy.

How do you wind up with this sort of notion that it's only a physical or economic harm?

Ms. OHLHAUSEN. Senator, what I was addressing was how the FTC has already said it would apply its unfairness authority, and what it has told Congress in the past what the limits were of that.

For the FTC to recommend new legislation that would take into account additional harms is something that I think needs careful consideration.

Senator KERRY. Well, that's what we're trying to give it. That's exactly what we're doing. We've been giving this careful consideration for 2 years now. It seems to me, we need to kind of break through here a little bit.

Let me try to get further in that, because some of the argument from Senator Toomey and others is sort of this notion that somehow this is going to interfere with the freedom to create new apps and so on and so forth. I just don't see that.

Consumers choosing how their information is going to be managed is not going to affect what people are going to offer. They're going to offer it with protections, I would assume.

But let me ask specifically the other two witnesses, what other privacy principles, other than just this idea of transparency and choice? There are other privacy principles at stake here, like data retention limits, for instance, or purpose specification, et cetera.

Can you talk about, either of you, sort of what the breadth of interests are here that go beyond just the transparency choice?

Mr. KERRY. Thank you, Senator Kerry.

As I said in my remarks to Senator Toomey, we can't depend just on notice and choice. You know, that is part of the problem with the existing system.

The principles that we've outlined—transparency, respect for context, security—incorporate, I think, some of the additional principles that you have talked about.

We articulated the principle of focused collection, which incorporates both use limitations and data minimization.

Senator KERRY. Can you sort of break it down in a practical way of how that would affect somebody?

Mr. KERRY. Well, the principle recognizes, and the reason we've articulated it a little bit differently than simply data minimization, is that, in the age of big data, there's a great deal of data collection that has public benefits, benefits to public health, to research, and often in unforeseen connections in data.

So we don't want to discourage that, but what we do want to discourage, I think consistent with the principle of privacy by design, as the FTC has articulated it, is that people make conscious, considered decisions about what data they need to collect and what data they need to retain.

Mr. LEIBOWITZ. Yes, and if I could just followup, I think embedded in your approach are several important principles, one of them Mr. Kerry mentioned, which is privacy by design. Another one is more transparency, because that could be one of the benefits of having stakeholders involved in developing codes of conduct.

We have found, and we discussed this in a previous hearing, we have found privacy policies in the mobile space that are 102 clicks. Nobody reads that except our staff, who we asked to read it.

And then the other thing, and this is part of the reason why I think businesses are so supportive of things like Do Not Track and of general privacy legislation is it creates a virtuous cycle. If consumers have more control, they generally feel like they have more trust in the Internet, and they engage in more commerce.

And so I think part of the reason why companies support general privacy legislation is because it's the right thing to do. I think part of it is because it becomes a virtuous cycle.

Now as my colleague Commissioner Ohlhausen has mentioned, you do have to watch out for barriers to entry, because on our competition side, you sometimes see the big guys doing things to make it tougher for new innovators. But we have not seen that problem on privacy issues thus far.

The only other point I just wanted to mention is that we try not to take speculative harm into account when we bring cases. We do take reputational harm into account from time to time, and these are bipartisan, unanimous cases.

So for example, in the Google Buzz order that we have, Google tried to jumpstart its first social network, Google Buzz, by taking confidential Gmail information, which they had said would remain private, and making it public.

And by doing that, certain information, like the fact that someone might be seeing a psychiatrist and be communicating on Gmail with that psychiatrist, became known to other users.

And so that kind of harm, where it's not speculative, I think is one that we do take into account under our statute.

Senator KERRY. Well, I appreciate it.

Thank you, Mr. Chairman. Let me just say, I think it's important—I mean, look, if you have that choice and transparency, you'd be better than you are today, there's no question about that. But you'd still have a problem, because people could still take your information, use it anyway they wish, store it indefinitely. And you wouldn't have any control over a third-party purchase or a third sale or, you know, what's the standard by which that information is going to be kept? What happens to it after it has been there for a long period of time?

There are a lot of things there where there's an expectation, I think, that has to be protected here, or people have to have a greater knowledge about, than just the choice of what they may do.

The CHAIRMAN. Thanks, Senator Kerry.

Senator Klobuchar?

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. Thanks for holding this hearing. Thanks to our witnesses.

I wanted to first thank you, Chairman Leibowitz, for the work on cramming that I know you're doing. It has been something that I've been focused on for a while, along with our attorney general in Minnesota. And we've made some strides with some of the major telephone companies, as you know, agreeing for landlines to police this in a better way. And I saw yesterday you announced you're seeking a civil contempt ruling against the third-party billing company.

So I want to thank you for that, even though it's exactly not on topic, it is kind of, but then move on to some other things.

Today, I introduced, along with Senator Blumenthal and a few other Senators, and we have companion House legislation, a bill on password privacy, and it's called the Password Protection Act.

And this of course came out of a number of us had gotten contacted by people who had been asked for passwords, and there's been some reports on it. And we worked, actually, with Facebook and Google and Twitter and a lot of the groups. And there seems to be some widespread support for putting some kind of a rule in place to make clear that at least the data that people intend to have be private is private, what I think former Justice Brandeis used to call the right to be left alone.

With the new technology, it's very difficult for the laws to keep up. And I was just wondering what the FTC, and you, Mr. Kerry, what the Department of Commerce, is doing with regard to these issues and if you have things come up with password issues and the like?

If you want to start?

Mr. LEIBOWITZ. Well, we have some concern, and we've expressed some concern, about the practice of employers asking for Facebook passwords. And we have communicated that to Facebook.

It sounds like Facebook is working with you. They've also noted that this may not be consistent with their terms of service.

And so it is something we are concerned about. It may be something, by the way, that isn't within our unfair deceptive acts or practices authority. It's an interesting question we were discussing today before I came up here.

But we want to work with you going forward on your legislation.

Senator KLOBUCHAR. Very good.

Mr. Kerry?

Mr. KERRY. Thanks, Senator Klobuchar.

Our proposals, frankly, focus on the relationship between consumers and the companies that they deal with, not with their employers.

But I would say is that the use of that information by employers is reflective of one of the critical realities of where we are in the world of information today, that there is so much information out there about people. And the ability to collect and to aggregate that information has gotten so extensive that it is possible to learn things about people that constitute sensitive information, even though that sensitive information hasn't been put out there, you know, by itself.

To take Chairman Leibowitz's example of somebody doing a search on health information, now, we protect health information under HIPAA. Health care providers have to protect that. But you

could find, you know, by aggregating information, you can find out health information but not be subject to those protections.

So the ability to aggregate information creates new risks of harm that haven't existed.

Senator KLOBUCHAR. Right. And it's the same with the information that might be under password, things about people's religious status, things you would not ask about in an interview that would be behind a password.

So, you know, we're hoping, working with the business community, there will be some support here, too, as well as what the rules of the game are for them. And so we have been working on that.

My last question is just about industry self-regulation. I think it is important to recognize the proactive steps industry has undertaken to set up and follow best practices, self-regulatory agreements. Now we just need to get the word out, and make sure they are easy for consumers to use, if they want to.

How are your agencies working with industry to help get the word out about consumers' right to privacy and how they can make privacy decisions that are right for them? Basically, how do you educate the public about the tools that are out there now, and in addition to what we may be working on, but what's out there now? And how are you working with self-regulation entities to make sure that these policies are consumer-friendly?

Mr. LEIBOWITZ. Our report, "Protecting Consumer Privacy in an Era of Rapid Change"—I think most of the members of this community are familiar with it—was drafted after working with stakeholders. We held numerous workshops. We put out a draft report, which companies generally liked. We also got more than 460 comments from industry representatives, consumer groups, and various other people who had something to say. And some of those comments are very detailed and very, very helpful.

I would say that the pace of self-regulation has been fairly uneven. And I think that even if you ask the best companies, companies with the best privacy practices, about that, they would say that's part of the reason why they are interested in things like Do Not Track standards and privacy legislation, is so that we will be migrating towards a more even playing field, and also one where consumers have more trust in the Internet, which, again, contributes to a virtuous cycle of more trust and more commerce online.

Senator KLOBUCHAR. OK, very good. I think I'm out of time. And I will get any other answers in writing from all of you, and also put in a question on cloud computing, something I'd like to ask you all about, so thank you very much.

The CHAIRMAN. Thank you, Senator.

Senator Pryor?

STATEMENT OF HON. MARK PRYOR,
U.S. SENATOR FROM ARKANSAS

Senator PRYOR. Thank you, Mr. Chairman.

Let me start with you, if I may, Ms. Ohlhausen. I'm curious about your impression of the average Internet users' understanding and realization of the extent that his or her information is being collected, and then how it's being used, and how it might affect their lives.

I'm just curious about your sense of how the average Internet user, how much he gets of all this.

Ms. OHLHAUSEN. Well, thank you, Senator Pryor.

That is one of the issues I'd like to find out more about as I talk to FTC staff and stakeholders. I do believe that there are consumer expectations that financial information will be secured, that medical information will be secured.

But as you get away from some of those areas, I do think, for example, in first-party marketing issues, the FTC, in its online behavioral advertising and also in this privacy report, has noted that consumers do expect that the website that they are dealing with may be serving them ads, may be using information to market to them subsequently.

As you move away from that paradigm of a one-on-one relationship, I think those are good questions that I would like to explore further.

Senator PRYOR. Mr. Leibowitz, let me ask you a three-part question.

From your standpoint, first, are there adequate tools available? And second, are consumers sufficiently aware of those tools? And then third, are they exercising their choice and their controls?

Mr. LEIBOWITZ. That's a great series of questions.

I would say for some things, adequate tools are available. So for example, if you want to go online, Mozilla, I believe Google, and possibly even Microsoft, offer browsers where you can go incognito. So that's an interesting way for consumers if they want to, and if they are aware, to use a tool that empowers them.

I think the best companies generally are better about empowering consumers and giving them more tools and more information.

But in some instances, consumers just aren't aware and this goes back to Senator Toomey's point. You know, we all would like to see more competition for privacy, but when you have privacy policies that are on the mobile space, that are dozens of clicks to read through, it's just hard to have competition without transparency and understanding what your tools might be and what your options are.

And I'd also say this, some companies give better protections in the teen space, which I know some of you are concerned about. Others don't. And so we have encouraged companies—again, this is not a regulation, we don't regulate in that space—to give more opt-in approaches to teens, because as we all know, kids are sometimes tech savvy but judgment poor.

Senator PRYOR. Right.

Yes, I actually was going to ask about teens next, Mr. Leibowitz, if we could go to that.

And that is, I know that we don't require privacy policies right now. But should we require privacy policies when it comes to kids and teens?

Mr. LEIBOWITZ. I think that's something we would like to work with you on, because I think if you can encourage or require companies, again, because under the Children's Online Privacy Protection Act there are some specific obligations. As this committee knows, we're in the process of updating the COPPA obligations.

I think that's a really good thing to have, so that teens understand some of the consequences. All too often, it's after they recognize the importance of privacy, which most consumers do recognize, if you look at any polling data, but all too often, teens recognize the importance of privacy only after they've sent or posted something or read something that caused some harm.

So I want to work with you on that issue going forward.

Senator PRYOR. That would be great. And as we work on that, I'd love to get your thoughts on if, and if so, how, operators are misusing teens' personal information. I know you probably have some data, but a lot of anecdotal evidence on that.

But let me get to Mr. Kerry, if I can, because I'm almost out of time here.

And, Mr. Kerry, I know a few moments ago, when Senator Klobuchar was wrapping up, it looked like you had an answer for her and you had a document in your hand, you were maybe going to answer, so I'll give you a chance to do that.

But first, let me ask about state attorneys general. Is it the administration's or the Department of Commerce's view that State AGs and the FTC should have the authority to seek civil penalties for violation of voluntary privacy commitments or codes of conduct?

Mr. KERRY. Senator, we believe that state attorneys general along with the FTC should be the prime enforcement vehicle. It's important that that enforcement have some weight. We would certainly be glad, as we move forward, to work on legislative language, to work with you to look at how best to do that.

Senator PRYOR. And did you want to——

Mr. KERRY. Sure, Senator Klobuchar had asked, I think, the question about building consumer awareness. The document I was getting out, Chairman Leibowitz held up his agency's report. The appendix in the White House Blueprint sets out the Consumer Privacy Bill of Rights. And in doing that, we tried to put it in plain and simple language, and put it into a stand-alone document that is something that consumers can use to understand what to expect from businesses as a tool to build consumer awareness.

And that's something we will work to implement through the multistakeholder processes that we've now embarked on. I think it's important to say that those processes are not just self-regulation. We want to involve all stakeholders, to involve consumer groups, so that the codes of conduct look out for the interests of everybody and not just the affected business community.

The CHAIRMAN. It was interesting to me that in some of the comments that were made, people talked about breaking the Internet, as if this onslaught—and it was also interesting to me that some didn't talk at all about consumers. They talked about the rights of an Internet to be able to develop in any way, shape, or form that would be, and didn't get around to talking about the effects on consumers.

So I want to get at this, Mr. Kerry, with you, and also with all three of you, actually.

This breaking the Internet policy, that if we were to pass some legislation—I mean we've been working actually, Senator Kerry said, too, that's specific. We have been working on this for about

10 years on the Commerce Committee, without the vigor that we have been recently, but this is an ongoing process.

So privacy laws already protect people's phone conversations. They protect people's television habits. Privacy laws protect people's medical records, their financial data. And clearly, our privacy is protected in other technologies where there is sensitive information.

Now how does this—which is called protecting the American people in ways in which they have every right to expect to be protected and expect very thoroughly to be projected—do we get into breaking the Internet?

It's unclear to me that in any way, by any of these types of things, do we attack the rights and privacy of the Internet in their own business.

Mr. KERRY. Well, I'm pleased to answer that question, Mr. Chairman, because preserving the dynamism, the innovation, the economic growth that the Internet has been such a powerful instrument of has been absolutely a guiding premise of the work that we've done.

And that's why the model that we've adopted doesn't follow a traditional rulemaking model. That simply doesn't work in the Internet environment. It doesn't operate at Internet speed.

That's why we've incorporated in a multistakeholder model, building on top of a baseline, a floor of rights that consumers can expect that would apply across the board, regardless of the business, regardless of the sector, to develop a set of codes of conduct using the same structures of multistakeholder policy development standards, consensus, that have been so successful in the Internet space.

The World Wide Web Consortium, the IEEE, these are the governing bodies of the Internet that have operated not as the product of any one government, but as a public-private partnership involving business, involving civil society.

It's worked tremendously and successfully. It could work successfully in this space.

Mr. LEIBOWITZ. Yes, and if I could just follow up, Mr. Chairman?

I think the General Counsel is exactly right. Privacy and innovation generally go hand in hand, and you can protect consumers and promote innovation.

And with respect to Do Not Track, the proof of that is that the business community supports it and is supportive of moving forward with a Do Not Track option for consumers.

The CHAIRMAN. But was it not—and I need to call on you, Commissioner.

Ms. OHLHAUSEN. OK.

The CHAIRMAN. But was it also not true that a number of companies got very enthusiastic about doing Do Not Track on their own right after your report came out?

Mr. LEIBOWITZ. I would say there was, among the browser companies like Microsoft and Mozilla and Apple, a lot of support for it. There continues to be. Again, there are a few, you know——

The CHAIRMAN. I'm asking about the timing question. Am I wrong on that?

Mr. LEIBOWITZ. Yes, they were very supportive early on, and we think they have made progress since.

The CHAIRMAN. No, that's not the question I asked.

They came out in support right after your two reports came out.

Mr. LEIBOWITZ. Yes, yes. More of them also came out after the report; that is correct.

The CHAIRMAN. Yes.

Mr. LEIBOWITZ. Yes, sir.

The CHAIRMAN. Commissioner?

The CHAIRMAN. We're still on breaking the Internet.

Ms. OHLHAUSEN. Yes, I figured we were.

So I think that's a very important issue and one that some commenters have raised concerns about.

And in the debate, you get a wide array of views. People express great concerns about that, and other people have great concerns about consumer privacy.

And I think the FTC generally has tried to strike the balance of meeting consumer expectations. So if consumers have protections and expect protections about their financial information and their medical information, I think the FTC has done a good job in bringing cases that advance those expectations for consumers. They are deception-based cases often, but occasionally there are fairness-based cases.

So I think, for me, that's one of the most important things that I need to look at it is, is this going to meet consumer expectations, and is this going to meet consumer preferences, because consumers do also enjoy using a lot of the new benefits, new services, that the Internet offers.

So if we have a solution that consumers ultimately end up unhappy with, because they've lost some of these services, these conveniences that the Internet has provided them, I'm not sure we're striking things in the right balance.

But I think the important thing is to strike the right balance for the benefit of consumers.

The CHAIRMAN. Thank you.

Senator Udall?

STATEMENT OF HON. TOM UDALL,
U.S. SENATOR FROM NEW MEXICO

Senator UDALL. Thank you, Mr. Chairman. And sorry I wasn't here earlier. As you know, we have so many things going on.

The CHAIRMAN. We were all talking about it.

[Laughter.]

Senator UDALL. Yes. I understand.

And I hope you all forgive me, but an incredibly important subject. The Chairman always focuses, I think, on what the American people are concerned about.

And I just hear a lot of discussion in New Mexico about this whole privacy issue. And I apologize if I'm going over any ground that you've already hit here.

But I just had a couple of questions.

Chairman Leibowitz, the FTC has recently settled privacy cases with well-known online companies used by millions of Americans. Could you explain how these settlements will benefit consumer on-

line privacy and how have these settlements encouraged other companies to change or improve their privacy policies?

Mr. LEIBOWITZ. Well, if you are talking about our settlements with, say, Google, for Google Buzz, and Facebook, we found what we believed to be violations of the law. Essentially, those companies made commitments about keeping information private that we believe they did not keep, or they didn't honor their commitments. And so we brought cases against them and had settlements.

In the settlements, they're required to be monitored. They have to engage in privacy by design. And most importantly, if you combine the Facebook and the Google matters, they protect more than a billion consumers worldwide. And if those companies want to change their privacy settings, they have to give consumers an opt-in going forward to do that.

And then of course, when you are under order, we, unlike most attorneys general, and you've missed this discussion, but I know you were—who have fining authority, we do not have fining authority. But if you are under order, we can then fine you for second violation. We hope, of course, we don't see second violations here.

Senator UDALL. Yes.

And, Mr. Kerry, you note in your testimony that the European Union is moving forward with data privacy regulations. Is there concern if Europe moves forward with privacy rules while the U.S. does nothing, that European regulations will essentially become the global norm that U.S. companies follow?

Mr. KERRY. Senator, thank you, yes, that is a concern. It's a concern that we've heard from many companies.

I said in my oral remarks that I defend the American system of privacy and the commitment that we have in our laws. But we do not want to let other countries set a default standard.

There are certainly points in common between what we are proposing and what the European Commission has proposed. But there are also concerns that there are ways that that gets into prescribing technology and other kinds of prescriptions that could operate as barriers to entry, that could inhibit the free flow of information across international borders.

So it is important to move forward here. I think we are here because our mission, as this committee knows well, is to promote the domestic and international commerce of the United States. We would not be promoting privacy legislation if it did not promote the foreign and domestic commerce of the United States.

I think the fact that we are sitting here alongside Chairman Leibowitz, who has also proposed advocating for legislation, reflects the convergence of economic and business and consumer interests in this area.

It's important to consumers. It's important to business. It's important to global commerce.

Senator UDALL. Thank you.

Commissioner, do you have any thoughts on those two?

Ms. OHLHAUSEN. Well, I do believe the international element of privacy regulation is very important. But I have to admit, it's something I need to educate myself on a little further before I could offer anything very useful at this point.

Senator UDALL. Thank you.

Thank you, Chairman Rockefeller. I really appreciate it.

The CHAIRMAN. Thank you, the Right Hon. Tom Udall of the State of New Mexico.

I'd just like to close with a couple.

We talk about the Digital Advertising Alliance is making it very clear they want to cooperate, and they appear to be doing so. But there are two areas where they still can collect information under their own definition. And I think one of those is market research, and the other is product development.

Now, that doesn't take me to a series of blisses or sins, but I get very nervous when I read that about those two little snippets being able to swallow up the rule.

What is it that allows them to get? And after your question, can you talk about what you are doing to make sure that they don't get that, if you can?

Mr. LEIBOWITZ. Well, I think from the perspective of the majority of the Commission, we entirely agree with you. Do Not Track has to mean "do not collect" if it's going to mean anything. There might be a few narrow, enumerated exceptions, for example, for anti-fraud purposes.

But we are working with the Digital Advertising Alliance at this point. We think by the end of the year, I believe that one way or another, whether it's legislative or whether it's by virtue of resolving some of these matters—and of course, there's another forum, the World Wide Web Consortium, where a lot of the companies are working with technologists and consumer groups to come up with a standard and what it would entail.

But one way or another, we believe that—I believe that—by the end of the year, there is going to be meaningful Do Not Track for American consumers, so they can opt out of third-party advertisements, and that's critically important for consumers, if you want to have more trust, as the General Counsel said, in Internet commerce.

The CHAIRMAN. I'd agree with that, and I guess I'll just close with this, that the statement was made here that it's in the nature of the Internet industry, the Web industry, whatever, to compete for the trust of consumers, and that in so doing, they will get the trust of consumers. And therefore, there's no need to even consider regulation.

That does sort of go against my general theory of corporate America. I mean, in other words, if you talk about competition, that is some of the most, you know, cutthroat competition that exists going on in precisely that world at this time. People merging and swallowing and doing all kinds of things.

It doesn't make sense to me that people would compete for something which is not in their economic interest, except as they are required to do so by a higher power, which understands that protection is not just what is already on the books, but protection is a part of the rule of law, so to speak, in America.

Mr. LEIBOWITZ. Well, if I can just respond to that. Imagine Commissioner Ohlhausen and I are competitors. And she wants to do the right thing, and I want to collect as much information as I possibly can and monetize it in every way I can. Well, she's at a com-

petitive disadvantage, because I'm making more money while she is trying to protect consumers. And so that's——

The CHAIRMAN. She's being virtuous.

Mr. LEIBOWITZ. She is being virtuous, and she is virtuous.

[Laughter.]

Mr. LEIBOWITZ. And she's a wonderful member of the Commission already.

[Laughter.]

Ms. OHLHAUSEN. And if I'm a corporation, I would probably try to advertise the fact that I am virtuous and get consumers to come to my company rather than——

Mr. LEIBOWITZ. But of course, if the Leibowitz Corporation isn't playing along, and we're making more money, you know, it's not necessarily fair to the Ohlhausen Corporation.

So, you know, you understand this. And that's why things like voluntary stakeholder-driven codes of conduct can be very, very useful. It's why, at the end of the day, we're hoping that—the Digital Advertising Alliance and the companies behind it represent, I think, 90 percent of all advertising on the Internet. When you get to 90 percent, if they're all making commitments not to collect—and again, a lot of those companies I believe, having talked to them individually, would be very comfortable with limitations on collection, the kind you and I envision. I think that would be very, very meaningful for consumers.

Mr. KERRY. And if I could add that the trust that the Ohlhausen brand would build up would permit another company, we won't call it the Kerry Company, to operate under the radar, without respecting the same standards. That's why we need a baseline.

The CHAIRMAN. Exactly.

I thank all three of you very, very much. This is a new beginning in this whole area.

And the floor is not an easy place, and the Senate is not an easy place to get legislation passed, as you may have noticed. But that doesn't stop us. We've got to do our work.

And it's incredibly important work, particularly in this particular new age, controlling of the new age, set of business that we are dealing with.

So I thank you and the hearing is adjourned.

[Whereupon, at 4:05 p.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO HON. JON D. LEIBOWITZ

Principles that Require Protection

Question 1. According to a survey from *Consumer Reports,* 71 percent of respondents from a recent survey said that they had concerns about companies distributing their information without permission, while 56 percent said they had similar concerns about companies that hold onto data "even when the companies don't need it anymore." Cases brought to date on privacy rely on the FTC's ability to protect people from deception. That is, a company cannot do something with your information that they told you they would not do. That is insufficient in the minds of many Americans as reflected in this poll since fighting deception is not a requirement for consent for collection or distribution and it does not place any limits on data retention. Deception is also silent on the other fair information practice principles including the right to access. Can you talk about why the other privacy principles like data retention limits and purpose specification are necessary and not simply a regime of notice and choice?

Answer. Our report notes that "privacy by design" should 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. By implementing these principles, companies can shift the burden away from consumers who would otherwise have to seek out privacy protective practices and technologies. For example, in a pure "notice and choice" regime, consumers would have to sift through privacy policies to determine which companies maintain reasonable data security, and exercise choice by only doing business with those companies. Consumers should not bear this burden; instead, companies should make reasonable security the default.

Tracking and Your Property

Question 2. For a company to track an individual's behavior and activities on the Internet, it has to put a tracking technology on a person's computer or smartphone. Do you believe it is the right of the collectors of information to place such tracking devices on a person's property and collect information without that person's knowledge or participation or collect information that has nothing to do with the service being provided and if not, what in the law stops that from happening today?

Answer. Online tracking is a ubiquitous practice that is largely invisible to consumers, and numerous surveys show some level of consumer discomfort with online tracking. A person's computer or smartphone is his property, and consumers need to have the ability to learn what information is being collected and how it is used and shared—especially with respect to invisible data collection.

A majority of the Commission continues to call for the implementation of a Do Not Track mechanism that would give consumers a choice about whether to be tracked. Although we have asked Congress to consider enacting general privacy legislation to set baseline standards, we have not called for Do Not Track legislation specifically, in part because industry has responded to our call and is making progress. I am optimistic that, by the end of the year, industry will have developed a Do Not Track mechanism that meets five criteria: it should be implemented universally; it should be easy to use; any choices offered should be persistent and should not be deleted if, for example, consumers clear their cookies or update their browsers; an effective Do Not Track system would opt them out of collection of tracking data, with some narrow exceptions like fraud detection; and a Do Not Track system should be effective and enforceable.

Who is Authorized to Share Your Data?

Question 3. A Wall Street Journal examination of 100 of the most popular Facebook apps found that some seek the e-mail addresses, current location and sex-

ual preference, among other details, not only of app users but also of their Facebook friends. Should consumers expect that things they share with a group of friends they choose on social networking sites in turn makes those friends authorized distributors of access to them and their information? Does that raise any concerns for you?

Answer. We share your concern about the privacy of information collected through applications, particularly personal data such as photos and videos, address books, and location information. Many consumers are not aware of the extent of data being collected through apps and how that data is being used. In our case against Facebook, for example, we challenged the company's failure to disclose that a user's privacy settings did not prevent apps used by their friends from accessing personal information. Recent reports also highlight apps access and sharing practices—for example, a recent FTC staff report about children's mobile applications revealed that consumers are provided with very little information about applications' data collection and sharing practices. As a result, consumers are increasingly uneasy about the privacy of such information.

The lack of transparency and choice in the app marketplace is an example of why the FTC believes that Congress should consider baseline privacy legislation that includes increased transparency, simpler choice, and privacy by design. In the meantime, we will continue to encourage everyone—stores, developers, and third parties—to step up their privacy efforts and provide meaningful privacy protections for consumers.

At the same time, if consumers choose to share their information with hundreds of friends, they should be aware that those friends could actively further share their information, through oral conversations, e-mails, tweets, and the like. We have tried to educate consumers on safe social networking, and have developed materials for consumers, parents, teens, kids, and educators. Among other things, we tell consumers to be careful what they post online, because they may not be able to take it back.

Communication over Open WiFi

Question 4. The FTC, the FCC, and the Department of Commerce concluded that Google violated no laws when it collected private communications transmitted over unencrypted WiFi connections. Should collectors respect fair information practice principles if that information is transmitted over a WiFi network or is that not necessary in this context?

Answer. As a general matter, our privacy report recommends that companies implement privacy by design as part of best practices—which includes reasonable limits on data collection as well as implementing data security for the information that is collected.

Section 5 of the FTC Act is a broad statute that allows us to accomplish a great deal, but we can only use it to challenge practices that are deceptive or unfair. We cannot use it for everything—for instance, in most circumstances we cannot mandate privacy policies under Section 5. This is why we believe Congress should enact data security legislation and consider implementing general privacy legislation to give baseline protections for all consumers.

Inconsistencies in Law

Question 5. Today, we have laws governing privacy when a bank is collecting your information or when a doctor or hospital is collecting your information. We also have laws governing telephone companies tapping your communications or cable companies tracking your watching habits. Isn't similar or identical information collected and use without a governing framework on the Internet every day and what makes that disparity in law rational?

Answer. Presently, there is some existing sector-specific legislation that already imposes privacy protections and security requirements through legal obligations. However, these laws do not necessarily apply to all business or all personal information, and as a result consumers may be vulnerable both online and offline. Because of these legislative gaps, our privacy report calls for Congress to consider general privacy legislation and sets forth a framework to encourage best practices by providing an important baseline for entities not subject to sector-specific laws. We believe that by implementing privacy by design, increased transparency, and better control, companies can promote consumer privacy and build trust in the marketplace.

The European Privacy Standard

Question 6. What is your understanding of where the European privacy protection legal framework update stands and how does it compare to what your agencies have proposed?

Answer. The European Commission proposed its revised privacy framework on January 25 of this year. The EU Parliament and the EU member states are currently reviewing that proposal. Part of the proposal is for a regulation to cover commercial and civil regulatory activities. The FTC has followed that part of the proposal very closely. FTC staff has shared views with European Commission counterparts, both before the proposed regulation's release in January and since, and our most senior officials have maintained an open dialogue with the various European stakeholders on a variety of privacy issues.

As to how the European Commission proposal compares to the frameworks proposed by the Administration and the FTC, we are largely pursuing the same ultimate goals on both sides of the Atlantic. In fact, the frameworks show many similarities. These include promoting privacy-by-design, improving transparency, providing rights to access and rectify information, promoting the development of industry codes of conduct, strengthening data security, protecting children's privacy, and exploring the idea of giving consumers the ability to erase certain personal information that they have previously put on the Internet.

Another point of comparison is the issue of comprehensive privacy legislation, which the Europeans have and which has been proposed for the United States commercial sector. We view such legislation as important for privacy protection in the U.S. that, in addition to protecting U.S. consumers, also helps to build an internationally interoperable framework for data transfers that both protect people and also encourage the free flow of information. The goal is not complete harmonization with the EU, but rather interoperability between different systems based on larger shared values and based on practical solutions to bridge differences in our respective regimes.

Of course, we think there is also room for improvement in the proposed EU regulation. For example, we have discussed with our European colleagues the available mechanisms for commercial cross-border data transfers between the EU and the U.S. We are also discussing the issue of cooperation between regulatory authorities, especially on enforcement matters. Our concern is to ensure that transfer restrictions on data in the proposed regulation do not unduly interfere with legitimate information exchanges and cooperation between regulatory authorities like the FTC and its counterparts.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO HON. MAUREEN K. OHLHAUSEN

Principles that Require Protection

Question 1. According to a survey from *Consumer Reports,* 71 percent of respondents from a recent survey said that they had concerns about companies distributing their information without permission, while 56 percent said they had similar concerns about companies that hold onto data "even when the companies don't need it anymore." Cases brought to date on privacy rely on the FTC's ability to protect people from deception. That is, a company cannot do something with your information that they told you they would not do. That is insufficient in the minds of many Americans as reflected in this poll since fighting deception is not a requirement for consent for collection or distribution and it does not place any limits on data retention. Deception is also silent on the other fair information practice principles including the right to access.

In your testimony, you state, "I firmly believe that consumers should have the tools to protect their personal information through transparency and choices."

In light of the clear evidence that there are numerous collectors of information that provide the people on whom they are collecting information with neither transparency nor clear choices, would you support a law requiring the tools you believe consumers should have?

Answer. Although a substantial portion of the FTC's privacy enforcement has been based on deception as your question indicates, there are other legal avenues available to the FTC in this area. Thus, if there is consumer harm occurring from sharing data with third parties, I would first consider whether we should make fuller use of existing FTC statutory authority. For instance, the Commission has routinely used its unfairness authority to reach conduct that did not involve a deceptive statement but caused substantial harm that is not outweighed by any countervailing benefits to consumers or competition, and that consumers themselves could not have avoided reasonably. A number of these cases involve the sharing of consumer information with third parties in a way that risked substantial consumer harm. For example, in 2004 the FTC used its unfairness authority to obtain a settlement from Gateway Learning Corporation for renting personal information provided

by consumers on the Gateway Learning Website without seeking or receiving the consumers' consent.[1] The FTC has also used its unfairness authority on multiple occasions to target companies that failed to use reasonable security measures to protect sensitive consumer data.[2] the FTC also has actively enforced other statutes that prohibit sharing sensitive consumer data with third parties under certain circumstances, such as the Children's Online Privacy Protection Act (COPPA), the Fair Credit Reporting Act (FCRA), and the Gramm-Leach-Bliley Act (GLB).

I am aware of concerns about data brokers that monetize and sell consumer data to other companies in ways that may be invisible to consumers. The FTC's recent Privacy Report, which issued before I arrived at the Commission, described three types of data brokers: (1) those whose products and services are used for eligibility decisions, such as credit, employment or insurance and whose practices are already covered by the FCRA; (2) data brokers who collect and sell consumer data for marketing purposes; and (3) data brokers whose products are used for purposes other than marketing and FCRA-regulated eligibility purposes. Some of these uses include fraud prevention or risk management to verify the identity of consumers.

When developing an appropriate approach to the regulation of third party data collection, it is important to protect consumers from harmful practices while still permitting beneficial uses, such as fraud prevention and, in many cases, marketing. Several data security bills have included provisions that seek to provide consumers transparency and choice about information practices, and I will evaluate these proposals carefully.

Question 2. How would you apply your commitment to transparency and choices in the case of companies that do not collect information directly from the consumer but buy it from other collectors or harvest it from publicly available information?

Answer. As stated above, if there is consumer harm occurring from sharing data with third parties, I would explore whether we should undertake enforcement using existing FTC deception and unfairness authority, as well as other statutes such as COPPA, the FCRA, HIPAA, and Gramm-Leach-Bliley. I would also evaluate current industry practices of third party data collectors, including any self-regulatory programs. Finally, I will consider whether there is consumer harm occurring that cannot be reached by current enforcement and self-regulatory programs to determine if additional protections are necessary.

Tracking and Your Property

Question 3. For a company to track an individual's behavior and activities on the Internet, it has to put a tracking technology on a person's computer or smartphone. Do you believe it is the right of the collectors of information to place such tracking devices on a person's property and collect information without that person's knowledge or participation or collect information that has nothing to do with the service being provided and if not, what in the law stops that from happening today?

Answer. It is my understanding that tracking for online behavioral advertising is typically done through the placement of a cookie on a device (such as a computer, tablet, or smartphone) to collect information about sites visited by a user. I believe that sites and services that place such cookies should provide consumers clear notice of this practice. Consumers should have the right to decline to accept such cookies for marketing purposes. I also understand that many sites and browsers provide consumers with a variety of tools that allow them to express their preferences regarding tracking mechanisms. The FTC has brought enforcement actions against entities that have failed to honor such consumer choices. For instance, in 2011 the

---

[1] Decision and Order, In re Gateway Learning Corp., 138 F.T.C. 443 (Sept. 10, 2004). In this case, the FTC claimed that the material revisions Gateway made to its privacy policy, and the retroactive application of those revisions to information it had previously collected from consumers constituted an unfair act or practice because the conduct caused substantial injury to consumers that was not outweighed by countervailing benefits to consumers of competition. The Complaint also alleged that the revisions were false and misleading.

[2] *See* Complaint, In re BJ's Wholesale Club, Inc., FTC File No. 0423160 (Sept. 20, 2005) (The FTC alleged that BJ's Wholesale's failure to take appropriate security measures to protect its consumers' sensitive information constituted an unfair practice. The Complaint argued that BJ's security failures allowed unauthorized persons to access sensitive consumer information, and use that information to make fraudulent purchases.); Complaint, In re DSW, Inc., FTC File No. 0523096 (Dec. 1, 2005) (The FTC alleged that DSW's failure to take reasonable security measures to protect sensitive consumer data was an unfair practice. According to the Complaint, DSW's data-security failures allowed hackers access to consumer's credit card, debit card, and checking account information.); Complaint, In re CardSystems Solutions Inc., FTC File No. 0523148 (Feb. 23, 2006) (The FTC alleged that CardSystem's failure to take appropriate security measures to protect sensitive information of its consumers constituted an unfair practice. The Complaint claimed that due to the security failures, a hacker was able to gain access to sensitive consumer information that enabled him to counterfeit cards to make fraudulent purchases.)

FTC obtained settlements from two online behavioral advertising networks, challenging the companies' privacy policies that allegedly deceptively tracked online activities, even after consumers opted out of such tracking.[3] It is my further understanding that several self-regulatory organizations offer consumers a blanket opt-out from receiving targeted ads for marketing purposes.

Data Security vs. Data Privacy

Question 4. Commissioner Ohlhausen, in your testimony, you support enactment of data security legislation, stating "the legislation should empower the FTC to promulgate regulations for the protection of personal data from unauthorized access." If that is appropriate, and I agree that it is, why shouldn't the FTC have authority to promulgate regulations to protect personal data from unauthorized acquisition from the individual in question in the first place, an authority it does not have today and one you state it should only have after a risk to harm is exposed?

Answer. I believe that it is necessary to strike the right balance in regulating the collection and use of consumer information by legitimate actors, and focusing on consumer harm is an important part of this balance. There is an important distinction between a data breach and the collection and use of consumer information by a first party, as the FTC's Self-Regulatory Principles for Online Behavioral Advertising from 2009 and recent privacy report recognize. In the case of a data breach, there are no benefits to consumers or legitimate businesses or to competition from allowing data to be stolen and possibly used for fraudulent purposes. Requiring reasonable precautions against such breaches will enhance consumer welfare. By contrast, as the FTC has recognized in the guidance it has issued, consumers generally expect that first parties will collect and use their data. They also understand that they may receive benefits from the sharing of their data, such as free content or personalized services. Although there may be inappropriate sharing of information with third parties in some circumstances, there are also beneficial uses such as fraud prevention, risk management to verify the identity of consumers, and marketing. Because prohibiting these beneficial uses may reduce consumer welfare and harm competition, we should evaluate whether certain practices are causing consumer harm and whether consumers would be, on balance, better off if these practices were prohibited.

Question 5. Is it your position that the breach of personal data on a company's database should not be illegal if the information does not pose a provable economic harm? For example, should data breach legislation cover the hacking of a database of magazine subscriptions that would expose a person's sexual orientation or religious affiliation, or does that fail to meet the harm prerequisite?

Answer. If an entity that collects consumers' personal information has promised to protect such information and fails to take reasonable precautions resulting in a breach, that failure is actionable under the FTC's current deception authority regardless of resulting economic harm. As for the FTC's unfairness authority, which includes a harm standard, the FTC has long recognized that harm to consumers is not limited solely to economic consequences and may include other factors, such as health and safety risks. It may also include a broader class of sensitive personal information. For instance, in 2007 the district court affirmed the FTC's action against *Accusearch* alleging the unauthorized disclosure of consumers' phone records was likely to cause substantial injury, including unwarranted risk to their health and safety, from stalkers and abusers, and was unfair.[4]

However, not every breach of data can be given the same weight, and the FTC has required companies to take reasonable precautions based on the sensitivity of the data the entity holds. Protecting against all breaches is close to impossible. Thus, in determining what breaches should be a law violation, the breadth of consumer harm must be considered in light of the costs of preventing a breach. I support the goals of data security legislation proposed by members of this Committee.

Who is Authorized to Share Your Data?

Question 6. A *Wall Street Journal* examination of 100 of the most popular Facebook apps found that some seek the e-mail addresses, current location and sex-

---

[3] *See* Complaint, In re Chitika, Inc., FTC File No, 1023087 (March 14, 2011) (alleging that Chitika's opt-out mechanism in its privacy policy, which allowed consumers to "opt-out" of having cookies placed on their browsers and receiving targeted ads but only lasted for 10 days, was deceptive); Complaint, In re ScanScout, Inc., FTC File No. 1023185 (Nov. 8, 2011) (alleging that ScanScout's claim that consumers could opt-out of receiving targeted ads by changing their computer's web browser settings was deceptive because ScanScout used Flash cookies, which could not be blocked by browser settings).

[4] *FTC* v. *Accusearch, Inc.* No. 06–CV–105–D, 2007 U.S. Dist. LEXIS 74905 (D. Wyo. Sept. 28, 2007), aff'd 570 F.3d 1187 (10th Cir. 2009).

ual preference, among other details, not only of app users but also of their Facebook friends. Should consumers expect that things they share with a group of friends they choose on social networking sites in turn makes those friends authorized distributors of access to them and their information? Does that raise any concerns for you?

Answer. Social networking is increasingly popular and it is clear that many consumers feel comfortable freely sharing their personal information and preferences with a large group of friends and acquaintances. As social networking becomes the norm in our society, I think consumers need to be aware that the information they share on these sites can be easily passed on by their friends and acquaintances. Educating consumers so that they are aware of the risks as well as the benefits of sharing information of social networking sites allows consumers to make informed choices that reflect their preferences. The FTC has an active consumer education program and has created and widely disseminated a Net Cetera guide for youth online behavior. Also, as you know, the FTC has brought several enforcement cases (Google, Facebook and Twitter) in the social network arena to ensure that consumer preferences are respected.

Communication over Open WiFi

Question 7. The FTC, the FCC, and the Department of Commerce concluded that Google violated no laws when it collected private communications transmitted over unencrypted WiFi connections. Should collectors respect fair information practice principles if that information is transmitted over a WiFi network or is that not necessary in this context?

Answer. As suggested in the FTC's letter to Google closing the wireless network investigation, a company collecting data in any fashion, including when transmitted through a WiFi network, is in a better position to ensure the privacy and security of that data when it follows best practices, such as collecting only the information necessary to fulfill a business purpose and disposing of the information that is no longer necessary to accomplish that purpose. Additionally, it is advisable that any company collecting data institute adequate internal review processes to identify risks to consumer privacy resulting from the collection and use of information that is personally identifiable or reasonably related to a specific consumer. Because there was no misrepresentation and Google did not use the information it collected and promised to destroy it, it would have been difficult to meet the deception or harm requirements for a violation of the FTC Act.

Inconsistencies in Law

Question 8. Today, we have laws governing privacy when a bank is collecting your information or when a doctor or hospital is collecting your information. We also have laws governing telephone companies tapping your communications or cable companies tracking your watching habits. Isn't similar or identical information collected and used without a governing framework on the Internet every day and what makes that disparity in law rational?

Answer. There are a variety of statutes, such as HIPAA, the FCRA, and Gramm-Leach-Bliley, that govern the collection and use of consumers' financial and medical information in many circumstances, including over the Internet. The FTC has also brought a variety of enforcement actions under its deception and unfairness authority to protect consumers' financial, medical, and other sensitive information from unauthorized release or usage both online and offline. If there is harm occurring from sharing consumers' financial or medical data or the content of their online communications without their knowledge or consent, I would explore whether we should undertake enforcement using existing FTC deception and unfairness authority, as well as other statutes such as COPPA, the FCRA, HIPAA, and Gramm-Leach-Bliley. I would also evaluate the current industry practices of third party data collectors, including any self-regulatory programs. Finally, I will also consider whether there is consumer harm occurring that cannot be reached by current enforcement and self-regulatory programs to determine whether additional protections are necessary.

The European Privacy Standard

Question 9. What is your understanding of where the European privacy protection legal framework update stands and how does it compare to what your agencies have proposed?

Answer. Regarding the question of where the European privacy legal framework update stands, I agree with Chairman Leibowitz's response relating to the status of the EU's privacy update.

With response to the second part of the question, I was not on the Commission during the release of the FTC's Privacy Report and am in the process of educating

myself about the extent of the EU Privacy and Electronic Communications Directive update's interoperability with the U.S. privacy framework.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. AMY KLOBUCHAR TO HON. JON D. LEIBOWITZ AND HON. MAUREEN K. OHLHAUSEN

Question. The United States has been a leader in cloud computing—as the use of "the cloud" continues it is important to work with foreign countries with consumers of cloud computing or house data storage centers. We need to make sure they have strong security standards, enforcement, and consumer protections in place. This international component is mentioned in both reports—what work have you done so far to move forward on this cooperation? And are you working with the Department of State?

Answer. The FTC has promoted strong security standards, enforcement, and consumer protections for cloud computing in several ways. First, the FTC has made substantial efforts to improve enforcement cooperation with its foreign counterparts in the area of consumer protection and privacy generally. The passage of the U.S. SAFE WEB Act in 2006, which strengthened the FTC's ability to share information with and provide investigative assistance to foreign law enforcement authorities, has been a key part of these efforts. The Act is scheduled to sunset in 2013; we have urged Congress to renew the legislation permanently to ensure that we have the tools necessary to cooperate with our foreign partners on such issues of mutual interest. Among those issues are ones involving cloud computing.

Second, we play a leadership role in several international enforcement networks that address issues relevant to cloud computing. One example is the Global Privacy Enforcement Network, which we launched jointly with several foreign counterparts. Our aim is to facilitate more practical cooperation among privacy enforcement authorities on matters, including cloud computing, that cross borders. Agencies from twenty countries now participate.

Third, we have worked to support enforceable codes of conduct to leverage private sector efforts with enforcement to provide strong yet flexible protections for cross-border data transfers. In the Asia-Pacific Economic Cooperation forum (or APEC), for example, the FTC and the Department of Commerce have worked with other economies to develop the APEC Cross-Border Privacy Rules system, which provides baseline privacy protections supported by an enforcement backstop. APEC is also exploring the system's application in the context of cloud computing. In the transatlantic context, the FTC provides the enforcement support for the "Safe Harbor" system enabling data transfers from the European Union to the United States, and has recently brought several cases to vindicate the integrity of this framework.

Fourth, we also work closely with the Department of State and other U.S. agencies in developing strong and sensible international policies in this area. FTC staff participate with State in such fora as the OECD's Working Party on Information Security and Privacy. We have also worked with the Department of State in the U.S.-EU information society dialogue, where several issues related to cloud computing are being addressed. We also have extensive bilateral exchanges with our foreign counterparts, and routinely solicit their input for FTC conferences. One example is the FTC's 2009 conference on securing personal data in the global economy, conducted in conjunction with OECD and APEC, which analyzed data-security issues in a global information environment where data can be stored and accessed from multiple jurisdictions.

We believe that data security, consumer protection and privacy enforcement are critical to the success of any platform, including cloud computing, and we will continue to reach out to our foreign partners to ensure that these issues are properly addressed.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. AMY KLOBUCHAR TO HON. CAMERON F. KERRY

Question. The United States has been a leader in cloud computing—as the use of "the cloud" continues it is important to work with foreign countries with consumers of cloud computing or house data storage centers. We need to make sure they have strong security standards, enforcement, and consumer protections in place. This international component is mentioned in both reports—what work have you done so far to move forward on this cooperation? And are you working with the Department of State?

Answer. Because cloud computing touches on many important economic and policy interests, the United States government's approach is to bring to bear a wide array

of agencies and coordinate their efforts. Issues regarding cloud computing are often raised in meetings of the National Science and Technology Council, particular within the Committee on Technology's Subcommittees on Privacy and Global Internet Governance. The Subcommittee on Privacy, which I co-chair along with Assistant Attorney General Christopher Schroeder of the Department of Justice's Office of Legal Policy, has a working group entirely focused on international engagement. This working group is led by members of the State Department, the International Trade Administration (ITA, a bureau of Commerce), and the National Telecommunications and Information Administration (NTIA, a bureau of Commerce), and has representatives on it from Defense, Homeland Security, Federal Trade Commission, Office of Science and Technology Policy, Office of the Director of National Intelligence, National Security Staff, United States Trade Representative, Treasury, and more than a dozen other agencies.

Commerce works closely with State and other Administration agencies on the international components of cloud computing. State's efforts in this area are spearheaded by Ambassador Philip Verveer, coordinator for International Communications Information Policy. Ambassador William Kennard, Chief of the U.S. Mission to the European Union and former Chairman of the Federal Communications Commission, has also been extremely engaged.

Within Commerce, the National Institute of Standards and Technology (NIST), as part of its Cloud Computing Program, has assumed a technology leadership role in advancing Cloud Computing interoperability, portability and security standards, guidelines, and technology. NIST works in a collaborative model with over 2500 individuals and organizations from academia, industry, standards organizations, United States federal, state and local governments, and the international community to provide a neutral objective basis for understanding and addressing the underlying technical challenges related to the emerging model of cloud computing. In this program, NIST has worked very closely with the Department of State, Department of Homeland Security, and other Commerce bureaus to open a dialogue with the international community, and has been very effective in this role. For example, in NIST's 2012 Cloud Computing Forum & Workshop held in Washington, D.C. on June 5–7, senior government officials from Canada, the People's Republic of China, and Japan presented views on the benefits of cloud computing for public services, along with United States CIO Steve Van Roekel, in a session moderated by Ambassador Verveer. This event was open to the public and had 500 registered attendees. In this same event, NIST hosted a standards panel that included international standards organizations. NIST has contributed to and participates in international standards bodies along with United States industry.

State, Commerce, Justice, and other agencies are also examining cloud computing issues as they arise as topics for discussion in multilateral forums, such as the Organization for Economic Co-operation and Development and Asia-Pacific Economic Cooperation (APEC). Ensuring the free flow of data across borders is an important priority in any new trade agreement, such as the TransPacific Partnership.

State and Commerce are cooperating on cloud discussions with the Government of Japan to discuss ways in which cooperation can improve commerce, healthcare, consumer safety, and disaster preparedness between our nations. Also, Commerce recently held its first meeting with China's Ministry of Commerce on cloud computing in April 2012 in order to learn more about China's plans in this area.

One of the major obstacles we face in cloud computing is a popular misconception around the world that United States laws grant law enforcement more and easier access to personal data stored in the cloud than the laws of peer countries. These unfounded concerns run the risk of hindering the ability of United States companies to compete to provide cloud computing solutions, particularly in Europe.[1] Therefore, an important part of the work of the U.S. government is to educate other governments and citizens about existing privacy protections for personal data in the United States. State, the Justice Department, and Commerce have been engaged in education and outreach efforts in Europe, South America, Asia, and Australia to improve understanding of our privacy protections for data stored in the cloud. Contrary to the mistaken impressions occasionally voiced by foreign governments, the

---

[1] *See, e.g.,* David Rauf, *PATRIOT Act Clouds Picture for Tech,* Politico (Nov. 29 2011) (available at *http://www.politico.com/news/stories/1111/69366.html*); Loek Essers, *European Data Concerns Cloud Outlook for U.S. Vendors: The Dutch Government May Block Bids from U.S. Cloud Vendors,* IDG News Service (Sept. 16 2011) (available at *https://www.networkworld.com/news/2011/091611-european-data-concerns-cloud-outlook-250988.html*); Lothar Determann, *Data Privacy in the Cloud: A Dozen Myths and Facts,* The Computer and Internet Lawyer vol. 28 no. 11 (Nov. 2011) (available at *http://www.bakermckenzie.com/files/Publication/85bf0767-55d0-4679-879d-85987d26b725/Presentation/PublicationAttachment/96b0c239-5feb-46e9–811c-87c66f224629/ar__california__clouddataprivacy__nov11.pdf*).

United States legal framework for protection of civil liberties in the context of legitimate law enforcement access offers a high level of privacy protection. We continue to raise this issue publicly and in bilateral interactions with our allies to be sure that United States cloud computing providers are not unfairly discriminated against in their efforts to offer services around the world.

International discussions about cloud computing and cross border data transfers are too often grounded in myths about the United States legal system that misrepresent our fundamental commitment to privacy and the extensive privacy protections we provide, at the expense of our ability to advocate for international cooperation on creating interoperable standards and protections. While the consumer privacy framework in the United States is strong,[2] Congress can improve existing consumer privacy protections in ways that benefit consumers, foster greater trust in both the Internet and cloud computing, and strengthen our businesses' ability to compete at home and in foreign markets. The baseline privacy protection legislation outlined in the Administration's Privacy Blueprint would help to achieve these goals.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO HON. JON D. LEIBOWITZ

Problems with Empowering State Attorneys General to Enforce Federal Law with Regard to Privacy

Question 1. Mr. Leibowitz, one of the provisions proposed in various pieces of privacy legislation deals with state attorneys general being empowered to enforce Federal law with regard to data security. A likely result if such a provision were to be enacted into law is that state attorneys general would delegate their Federal enforcement power to private contingency fee lawyers. I believe the problem with this approach is that the goals of plaintiffs' lawyers might conflict with a state official's duty to protect the public interest. Plaintiffs' lawyers will be motivated to maximize fees at the expense of the taxpayer. There have also been troubling instances of state attorneys general hiring favored contingency fee lawyers rather than having a transparent and competitive bidding process. Litigation brought by state attorneys general should be motivated by the public good, not by private profit.

Mr. Leibowitz, with respect to proposed data privacy legislation empowering state attorneys general to enforce Federal law, do you believe that the legislation should ensure there is adequate supervision of state attorneys general at the Federal level to assure consistent enforcement of Federal law throughout the United States? Do you believe that state attorneys general empowered to enforce Federal law regarding data security should be restricted from delegating this power to contingency fee lawyers? If not, do you believe that if contingency fees lawyers are employed, the process to hire them should take place in a transparent manner with competitive bidding?

Answer. We support the ability of state attorneys general to enforce any Federal privacy laws, but the Commission has not taken a position on the methods by which the states use their enforcement authority.

The FTC often collaborates with the states in our privacy and data security investigations. For example, in our case against Lifelock the company agreed to pay $11 million to the FTC and $1 million to a group of 35 state attorneys general to settle charges that the company used false claims to promote its identity theft protection services. This joint settlement is just one example of our strong cooperative efforts with the states, and we look forward to working with them on future efforts in the areas of privacy and data security. This sort of collaboration helps ensure that enforcement actions are complementary and consistent. Another means of ensuring consistent enforcement of Federal law is carefully crafting the standards in any legislation to minimize the potential for inconsistent interpretations. We would be happy to work with the Committee on any such proposed legislation.

While I support the ability of state attorneys general to enforce any Federal data security laws, the Commission has not taken a position on the methods by which the states use their enforcement authority.

Definition of Data Broker

Question 2. Mr. Leibowitz, the FTC Privacy Report released a few months ago applauded the Digital Advertising Alliance's self-regulatory privacy program. However,

---

[2] See foreword, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23 2012) (available at *http://www.whitehouse.gov/sites/default/files/privacy-final.pdf*).

the FTC's Privacy Report also calls for legislation to regulate data brokers, but offers no guidance for what constitutes a data broker. As it stands, nearly all of industry engages in business or practices that might constitute data brokerage, and legislation would have a sweeping impact on many, if not all companies.

Mr. Leibowitz, how would you define what a data broker is? I'd like to hear your answer here today, but would also like to have your written answer for the record.

Answer. We would be happy to work with this Committee as it considers legislation concerning data brokers to determine a consensus definition of data brokers. When we developed our privacy report, we considered data brokers to be companies that monetize and sell consumer data to other companies in ways that are often invisible to consumers. Our report described three types of data brokers. First, there are those whose products and services are used for eligibility decisions, such as credit, employment or insurance; these companies' practices are covered by the Fair Credit Reporting Act (FCRA). Second, there are data brokers who collect and sell consumer data for marketing purposes. Finally, there are data brokers whose products are used for purposes other than marketing and FCRA-regulated eligibility purposes. Some of these uses include fraud prevention or risk management to verify the identity of consumers.

Question 2a. Mr. Leibowitz, why do you believe legislation is necessary despite the success of industry's self-regulatory program?

Answer. I believe that industry is making progress on self-regulation in *some* areas. For example, industry has made great strides in implementing a Do Not Track mechanism, but more work remains to be done. But there clearly are other areas that deserve more attention. The data broker industry is an example of an area where self-regulatory efforts have lagged. As our Privacy Report notes, there have been no successful self-regulatory efforts by the data broker industry since the 1990s—despite the highly-publicized ChoicePoint breach and growing public concerns. Given the fact that data brokers are largely invisible to consumers yet can have a dramatic impact on their lives, we have called for targeted legislation to give consumers reasonable access to the data such entities maintain about them, and we are working with data brokers to explore creating a centralized website to increase transparency about their practices and give consumers choices.

The mobile industry is another area where self-regulation is lagging. As detailed in a recent FTC staff report about children's mobile applications ("apps"), consumers are provided with very little information about applications' data collection and sharing practices. Our report found that in virtually all cases, neither app stores nor app developers provide disclosures that tell parents what data apps collect from children, how apps share it, and with whom.

FTC Privacy Report and Cost-Benefit Analysis

Question 3. The section of the FTC Privacy Report discussing the cost-benefit analysis of privacy regulation is disturbingly thin. The report acknowledges that "imposing new privacy protections will not be costless" but makes no attempt to determine what those costs are. Moreover, the proposed benefits to companies are unquantified and anecdotal at best. Businesses are better able to determine and maintain the value of consumer trust in the marketplace than is the FTC. Under the Regulatory Impact Analysis of the Office of Management and Budget, agencies are supposed to consider the qualitative and quantitative costs and benefits of a proposed regulation and any alternatives. That seems particularly important, given that Internet advertising alone directly employs 1.2 million Americans. How do we ensure a comprehensive cost/benefit analysis of privacy regulation or enforcement activity given that the FTC doesn't seem to have done that here?

Answer. As we noted in our report, we agree that it is important to consider costs and benefits associated with our recommendations. However, empirical, quantitative analyses are particularly challenging in this area. The value consumers place on not being tracked as they use the Internet or the costs to them of potential embarrassment or harm arising from unknown or unanticipated uses of information cannot be easily calculated.

It is important to note, however, that the Commission's Final Privacy Report did not and was not intended to set forth a new regulation or serve as a template for law enforcement. Instead, it focused on articulating best practices for companies that collect and use consumer data. The best practice recommendations in the report are designed to be flexible to permit and encourage innovation. Companies can implement the privacy protections recommended in the report in a manner proportional to the nature, sensitivity, and amount of data collected as well as to the size of the business at issue.

In addition, many companies have already implemented many of these practices, and we plan to work with industry to facilitate even broader adoption in the future.

Further, it is noteworthy that a number of leading companies have also asked Congress to consider enacting baseline privacy legislation to provide legal certainty to industry and to build trust with consumers. To the extent that Congress decides to move forward on baseline privacy legislation, the Commission notes that the best practices it recommends in the final report can inform the deliberations.

Risk of Stifling the Internet Economy

Question 4. A report commissioned by Interactive Advertising Bureau recently concluded that the Internet accounted for 15 percent of total U.S. GDP growth. If the Internet were a national economy, by 2016 it would rank as the fifth largest economy in the world. The advertisement supported Internet contributes $300 billion to the U.S. economy and has created about 3 million U.S. jobs. At a time of sustained, grim economic news, the Internet has remained one of the bright spots of the United States economy and that trend is continuing. I'm worried that if we try to rush a quick-fix on the issue of privacy, rather than thoughtfully and carefully dealing with the issue, we'll stifle that important economic advantage we have here in America. How do we make sure that we don't stifle the Internet economy, but still protect consumers? How do you balance these interests?

Answer. Our report articulates best practices for companies that collect and use consumer data. We also recommend—in part in response to calls from leading companies—that Congress consider enacting baseline privacy legislation to provide more legal certainty to industry and to build trust with consumers. All of these recommendations are the result of our extensive work with all stakeholders, and we look forward to working with Congress to make sure that we appropriately balance these interests.

We believe that companies will still be free to innovate—for example, they can find new ways to target ads without tracking or with less tracking, and consumers can continue to receive targeted ads if they so choose. Our recommendations simply seek to give consumers clear, understandable, relevant choices about their information. This conversation will build more confidence in the marketplace and encourage growth.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARCO RUBIO TO HON. JON D. LEIBOWITZ

Question 1. The FTC has endorsed the concept of Do Not Track (DNT), and this feature has been implemented by some browsers and social network services. As you probably are aware, many stakeholders have pointed out that implementing DNT could be difficult and disrupt website operations. My concern is the potential unintended consequences if a DNT mechanism or policy is drafted or implemented poorly, or does not take fully into consideration how the mechanism works. We know that some social networks and service providers utilize tracking functions and collect data to track child predators or prevent underage children from joining a site or service. In these cases, data collection and tracking are being used in an effective way, hence the concern if DNT is implemented poorly or prevents all data collection. Is the FTC taking these concerns into consideration? Is the FTC concerned about unintended harm if a broad DNT policy is implemented poorly?

Answer. The Commission continues to support Do Not Track and believes an effective model with limited exceptions can be implemented successfully. As the Commission developed the Do Not Track recommendation, it was certainly cognizant of unintended consequences and crafted an approach designed to address concerns like those you identify. For example, in the scenario you describe about a social network collecting information about its own users for public safety or criminal purposes, our framework would likely consider this practice to be an acceptable first party practice that is not within the scope of a Do Not Track mechanism. Do Not Track is not intended to prevent or address legitimate data collection and use by first parties with direct relationships with consumers but is designed to address data collection activities by third parties.

With respect to third party tracking, we have stated that any Do Not Track mechanism should be universal, easy, persistent, enforceable, and cover most collection, with some narrow exceptions like fraud detection. Industry has responded to our call for Do Not Track and is making great progress. There are currently broad-based discussions taking place on implementation of Do Not Track to ensure that the implementation is effective and not overbroad. We plan to closely monitor these discussions and are optimistic that an effective Do Not Track mechanism will be in place by the end of the year.

Question 2. As a father of four young children, I am concerned about their safety online, and I want to ensure that children are protected when they use the Internet and new technologies. I understand that the FTC is currently engaged in another review of the Children's Online Privacy Protection Act. Can you update me on the status of that review? At this point, do you believe that Congress needs to update that Act?

Answer. Children's privacy is a top priority for the Commission. We received over 350 comments in response to our proposed changes to the COPPA Rule and are working through them. There are many complicated issues, and we want to be sure we get it right. We hope to have the Rule finalized by the end of the year.

Question 3. In the FTC's Privacy Report there is a section on the articulation of privacy harms. In it, the FTC ultimately concludes that the "range of privacy-related harms is more expansive than economic or physical harms or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data." (p. 8)

Is the FTC implying or concluding that any unanticipated use of data is wrong? Is the FTC implying or advocating for the ability to take enforcement actions against harms that "might arise"? Or is the FTC already doing this? 1Do you think the FTC has blanket authority to regulate all uses of data?

Answer. The Commission's Final Privacy Report did not conclude that any unanticipated use of data was wrong or that the FTC had authority to regulate all uses of data. Rather, the report noted the concern that some unanticipated data uses could cause harm. The report described harms arising from the unexpected and unconsented to revelation of previously-private information, including both sensitive information (*e.g.,* health, financial, children's information, precise geolocation information) and less sensitive information (*e.g.,* purchase history, employment history) to unauthorized third parties. As one example, in the Commission's case (and consent) against Google, the complaint alleged that Google used the information of consumers who signed up for Gmail to populate a new social network, Google Buzz. The creation of that social network in some cases revealed previously private information about Gmail users' most frequent e-mail contacts. Similarly, the Commission's complaint against Facebook (and proposed consent) alleged that Facebook's sharing of users' personal information beyond their privacy settings was harmful.

Another harm the report identified is the erosion of consumer trust in the marketplace. Businesses frequently acknowledge the importance of consumer trust to the growth of digital commerce, and surveys support this view. For example, in the online behavioral advertising area, survey results show that consumers feel better about brands that give them transparency and control over advertisements. Companies offering consumers information about behavioral advertising and the tools to opt out of it have also found increased customer engagement. In its comment to the Commission's Draft Privacy Report, Google noted that visitors to its Ads Preference Manager are far more likely to edit their interest settings and remain opted in rather than to opt out. Similarly, Intuit conducted a study showing that making its customers aware of its privacy and data security principles—including restricting the sharing of customer data, increasing the transparency of data practices, and providing access to the consumer data it maintains—significantly increased customer trust in its company.

Ultimately, the value consumers place on not being tracked online or the costs to them of potential embarrassment or harm arising from unknown or unanticipated uses of information cannot be easily determined. What we do know is that businesses and consumers alike support increased transparency of data collection and sharing practices. Increased transparency will benefit both consumers and industry by increasing consumer confidence in the marketplace.

Finally, nothing in the report changes our existing authority to enforce the FTC Act. We can only bring actions involving unfair or deceptive practices. A practice is deceptive if (1) it is likely to mislead consumers acting reasonably under the circumstances, and (2) it is material, that is, likely to affect consumers' conduct or decisions regarding the product at issue. A practice is unfair if it causes or is likely to cause harm to consumers that: (1) is substantial; (2) is not outweighed by countervailing benefits to consumers or to competition; and (3) is not reasonably avoidable by consumers themselves. In order to prevail in a case under the FTC Act, we must demonstrate to a judge that the case meets these rigorous standards.

Question 4. As you are aware, over the last year, members of the Commerce Committee have asked numerous times about the scope of the FTC's Section 5 authority. With respect to Sec. 5, in follow-up answers you provided to the Committee after your last appearance here you said:

While the vast majority of [the FTC's] antitrust enforcement actions involve conduct that falls within the prohibitions of the Sherman or Clayton Acts, the Commission has a broader mandate, which it discharges by challenging, under Section 5, conduct that is likely to result in harm to consumers or to the competitive process. . . The Commission's recent use of Section 5 demonstrates that the Commission is committed to using that authority in predictable ways that enhance consumer welfare.

You say that you are "committed to using that authority in predictable ways." However, I would note that while the Commission has held workshops on the scope of its Section 5 authority in recent years, it has never issued a formal report or guidelines from those workshops that would give clear direction to the business community about the types of cases that the Commission will pursue outside the traditional Sherman Act constraints.

Question 4a. Do you plan on issuing such formal guidelines? If so, when can we expect to see those guidelines? If not, why?

Answer. I agree that businesses and consumers benefit whenever we are able to improve the clarity and predictability of the laws we enforce, including Section 5. It is worth noting that Congress, in formulating the antitrust laws and Section 5, decided that common law development of competition law was preferable to trying to produce a list of specific violations, recognizing that no such list could be adequate over varying times and circumstances. Congress consciously opted for a measure of flexibility in competition law.

However, sources of guidance do exist. Although the Supreme Court has never squarely articulated the precise boundaries of our Section 5 authority, the case law, complaints, and consent agreements identify the types of conduct to which the FTC has applied its stand-alone Section 5 authority in the past. Recent cases, including *Intel, U-Haul,* and *N-Data,* further illuminate the kinds of conduct the Commission has challenged as unfair methods of competition under Section 5. In addition, a wealth of information is contained in the transcripts and submissions from our October 2008 workshop on the use of Section 5 as a competition statute.

The scope of our Section 5 enforcement authority is inherently broad, in keeping with Congressional intent to create an agency that would couple expansive jurisdiction with more limited remedies, and it is firmly tethered to the protection of competition. The FTC has used its Section 5 authority judiciously in the recent past. We will not hesitate, however, to use Section 5 to combat unfair methods of competition that are within the scope of our jurisdiction.

My fellow Commissioners and I continue to consider the best way to further clarify the bounds of our Section 5 authority, be it a report, guidelines, or some other approach. This will remain a priority during the remainder of my term as Chairman.

Question 5. In your written testimony you state that privacy legislation would provide "businesses with the certainty they need to understand their obligations." Putting the legislation aside, I like that you are advocating for providing certainty for businesses. But in looking at the Privacy Report, I am concerned that the Commission is embracing an expanded definition of harm under Section 5 to include "reputational harm," or "the fear of being monitored," or "other intangible privacy interests." These seem like vague concepts—and I think this expanded harm-based approach would only create more uncertainty. Your testimony and the report appear to be in contrast in this instance. Do you agree? Why or why not?

Answer. We do not believe the harms we identify in the report and describe in the context of our recent enforcement actions are vague or uncertain. The backlash that followed Google's rollout of its Buzz social network and the Facebook changes that were the subject of our consent orders was immediate. Consumers clearly understood the likelihood of harm arising from these changes, and the companies should not have been surprised by the reaction. Thus, we do not believe our continuing use of Section 5 of the FTC Act, even without baseline legislation, will lead to uncertainty or confusion. We are obligated to consider certain specific factors in determining whether a violation of Section 5 exists and will continue to do so in our enforcement actions. Nevertheless, we believe that businesses can benefit from having clear rules of the road for commercial data practices that would provide even more certainty as to their obligations.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO HON. MAUREEN K. OHLHAUSEN

Problems with Empowering State Attorneys General to Enforce Federal Law with Regard to Privacy

Question 1. Ms. Ohlhausen, one of the provisions proposed in various pieces of privacy legislation deals with state attorneys general being empowered to enforce Federal law with regard to data security. A likely result if such a provision were to be enacted into law is that state attorneys general would delegate their Federal enforcement power to private contingency fee lawyers. I believe the problem with this approach is that the goals of plaintiffs' lawyers might conflict with a state official's duty to protect the public interest. Plaintiffs' lawyers will be motivated to maximize fees at the expense of the taxpayer. There have also been troubling instances of state attorneys general hiring favored contingency fee lawyers rather than having a transparent and competitive bidding process. Litigation brought by state attorneys general should be motivated by the public good, not by private profit.

Ms. Ohlhausen, with respect to proposed data privacy legislation empowering state attorneys general to enforce Federal law, do you believe that the legislation should ensure there is adequate supervision of state attorneys general at the Federal level to assure consistent enforcement of Federal law throughout the United States?

Answer. I support data security legislation and believe that state attorneys general should have enforcement authority. However, as you suggest, the legislation must be carefully crafted to ensure that there are clear statutory guidelines by which companies can implement their data security systems and Federal supervision of the efforts of the state AGs. The FTC works frequently and effectively with many state AGs and that model of cooperation to benefit consumers should apply here as well.

Question 2. Do you believe that state attorneys general empowered to enforce Federal law regarding data security should be restricted from delegating this power to contingency fee lawyers? If not, do you believe that if contingency fees lawyers are employed, the process to hire them should take place in a transparent manner with competitive bidding?

Answer. All law enforcement should be motivated by the public good, considering consumer harm, appropriate allocation of scare resources, and litigation costs, and among other factors. Transparency is also an important public goal, as is fostering competition in the procurement of goods and services for government use. Any Federal legislation should encourage transparency and competition at all levels of government but should also avoid being overly prescriptive regarding how states may conduct their legitimate functions.

Definition of Data Broker

Question 3. The FTC Privacy Report released a few months ago applauded the Digital Advertising Alliance's self-regulatory privacy program. However, the FTC's Privacy Report also calls for legislation to regulate data brokers, but offers no guidance for what constitutes a data broker. As it stands, nearly all of industry engages in business or practices that might constitute data brokerage, and legislation would have a sweeping impact on many, if not all companies. How would you define what a data broker is? I'd like to hear your answer here today, but would also like to have your written answer for the record.

Answer. The FTC's recent Privacy Report, which issued before I arrived at the Commission, considered data brokers to be companies that monetize and sell consumer data to other companies in ways that may be invisible to consumers. The Privacy Report described three types of data brokers: (1) those whose products and services are used for eligibility decisions, such as credit, employment or insurance and whose practices are covered by the Fair Credit Reporting Act (FCRA); (2) data brokers who collect and sell consumer data for marketing purposes; and (3) data brokers whose products are used for purposes other than marketing and FCRA-regulated eligibility purposes. Some of these uses include fraud prevention or risk management to verify the identity of consumers. When developing an appropriate definition of a data broker, it is important to protect consumers' personal information from harmful uses while still permitting beneficial uses, such as fraud prevention.

Question 3a. Why do you believe legislation is necessary despite the success of industry's self-regulatory program?

Answer. I believe that data security and breach notification legislation would be appropriate to protect against the unauthorized access of consumer information but I have not endorsed the Privacy Report's call for general privacy legislation.

I think that the best way to safeguard consumer privacy is to give consumers the tools they need to protect their personal information through transparency and choices. The self-regulatory programs appear to have made considerable strides in giving consumers control over who accesses their information and how it is used for marketing purposes. The proposed self-regulation, however, is not aimed at protecting against the unauthorized access of personal data by parties, such as hackers, and thus would not address the types of harms that data security legislation seeks to prevent.

FTC Privacy Report and Cost-Benefit Analysis

Question 4. The section of the FTC Privacy Report discussing the cost-benefit analysis of privacy regulation is disturbingly thin. The report acknowledges that "imposing new privacy protections will not be costless" but makes no attempt to determine what those costs are. Moreover, the proposed benefits to companies are unquantified and anecdotal at best. Businesses are better able to determine and maintain the value of consumer trust in the marketplace than is the FTC. Under the Regulatory Impact Analysis of the Office of Management and Budget, agencies are supposed to consider the qualitative and quantitative costs and benefits of a proposed regulation and any alternatives. That seems particularly important given that Internet advertising alone directly employs 1.2 million Americans. How do we ensure a comprehensive cost/benefit analysis of privacy regulation or enforcement activity given that the FTC doesn't seem to have done that here?

Answer. With privacy, as with all public policy issues within the FTC's jurisdiction, to produce the best result for consumers we should conduct a careful analysis of the likely costs and benefits of any proposed regulation. The Privacy Report, which was issued before I started at the Commission, discusses costs and benefits in general terms but does not contain a cost/benefit analysis. I believe that a review of what consumers and competition are likely to lose and gain from any new regulation would be helpful to ensuring the best outcome for consumers. For example, in the case of advertising, the FTC has consistently recognized the crucial role that truthful non-misleading information contained in advertising plays not just in informing consumers but also in fostering competition between current participants in the market and lowering entry barriers for new competitors. I believe that we should consider factors regarding the possible effects of reducing information available in market for consumers and competitors when analyzing the likely effects of new privacy regulations.

Risk of Stifling the Internet Economy

Question 5. A report commissioned by Interactive Advertising Bureau recently concluded that the Internet accounted for 15 percent of total U.S. GDP growth. If the Internet were a national economy, by 2016 it would rank as the fifth largest economy in the world. The advertisement supported Internet contributes $300 billion to the U.S. economy and has created about 3 million U.S. jobs. At a time of sustained, grim economic news, the Internet has remained one of the bright spots of the United States economy and that trend is continuing. I'm worried that if we try to rush a quick-fix on the issue of privacy, rather than thoughtfully and carefully dealing with the issue, we'll stifle that important economic advantage we have here in America. How do we make sure that we don't stifle the Internet economy, but still protect consumers? How do you balance these interests?

Answer. The best way to ensure a proper balance of the interests in the Internet economy and consumer protection is for the FTC to continue its carefully targeted enforcement against deceptive and unfair acts and practices on the Internet while proceeding cautiously in exploring the need for additional generally privacy legislation and promoting self-regulatory efforts aimed at providing access and choice to consumers. For example, I support a careful analysis of consumer harms that are not currently being addressed by enforcement or self-regulation before recommending any additional privacy legislation.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARCO RUBIO TO HON. MAUREEN K. OHLHAUSEN

Question 1. The Internet has had a transformative impact on society, both in America and around the world. One of the great things about the Internet and something that has contributed to its success is the fact that many of the most popular services and sites that consumers use are free, and they have remained free because of online advertising, including behavior based advertising. More and more in our economy, the ability to tailor services to more efficiently and effectively meet consumers' needs is driven by the collection of data and the delivery of tailored ads.

And these industries create jobs and contribute greatly to our economy. Do you agree that the FTC should balance these considerations when implementing privacy policies? How is the FTC doing this?

Answer. Yes, I agree that the FTC should balance these considerations. Because the FTC's ultimate goal is to optimize consumer welfare, when implementing privacy policies, close attention needs to be paid to potential outcomes and whether agency activity is actually improving consumer welfare. Consumer data can help firms to better understand the needs of their customers and to develop new and innovative products and services. The FTC has also recognized the crucial role that truthful non-misleading advertising plays in fostering competition between current participants in the market and lowering entry barriers for new competitors, resulting in overall benefits for consumers. Therefore, any potential competitive effects resulting from new privacy restrictions, such as a firms' ability to efficiently and effectively meet consumers' needs, should be considered against the benefit that consumers may derive from these policies. It is important to balance the actual privacy-enhancing benefits with the costs of such proposals in order to ensure the best outcome for consumers.

Question 2. As you know, certain telecommunications providers are subject to dual regulation by both the FTC and FCC. And depending on the service and technology, companies may be subject to multiple sections of the Telecommunications Act, or none at all. Do you think this dual regulation leads to confusion or negatively impacts some providers? Do you think that the Congress should look at eliminating dual regulation?

Answer. Generally, confusion can be avoided by making narrowly tailored, well-defined regulations that retain the focus of the agencies' missions. In the instances where dual regulation is contradictory, overly broad, or no longer represents industry conditions, eliminating dual regulation may be beneficial. For example, I support eliminating the FTC's common carrier exemption, which was based on the existence of a pervasively regulated, monopoly telecommunications industry that no longer reflects the state of the industry.

○