S. HRG. 110–791

BROADBAND PROVIDERS AND CONSUMER PRIVACY

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

SEPTEMBER 25, 2008

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

U.S. GOVERNMENT PRINTING OFFICE

48–450 PDF WASHINGTON : 2009

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 TENTH CONGRESS

SECOND SESSION

DANIEL K. INOUYE, Hawaii, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	KAY BAILEY HUTCHISON, Texas, *Ranking*
JOHN F. KERRY, Massachusetts	TED STEVENS, Alaska
BYRON L. DORGAN, North Dakota	JOHN MCCAIN, Arizona
BARBARA BOXER, California	OLYMPIA J. SNOWE, Maine
BILL NELSON, Florida	GORDON H. SMITH, Oregon
MARIA CANTWELL, Washington	JOHN ENSIGN, Nevada
FRANK R. LAUTENBERG, New Jersey	JOHN E. SUNUNU, New Hampshire
MARK PRYOR, Arkansas	JIM DEMINT, South Carolina
THOMAS R. CARPER, Delaware	DAVID VITTER, Louisiana
CLAIRE MCCASKILL, Missouri	JOHN THUNE, South Dakota
AMY KLOBUCHAR, Minnesota	ROGER F. WICKER, Mississippi

MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
LILA HARPER HELMS, *Democratic Deputy Staff Director and Policy Director*
CHRISTINE D. KURTH, *Republican Staff Director and General Counsel*
PAUL NAGLE, *Republican Chief Counsel*

CONTENTS

	Page
Hearing held on September 25, 2008	1
Statement of Senator Dorgan	1
Statement of Senator Hutchison	2
Statement of Senator Klobuchar	26
Statement of Senator Thune	29
Statement of Senator Vitter	3
Statement of Senator Wicker	31

WITNESSES

Attwood, Dorothy, Senior Vice President, Public Policy and Chief Privacy Officer, AT&T Inc.	4
Prepared statement	5
Sohn, Gigi B., President, Public Knowledge	15
Prepared statement	16
Stern, Peter, Executive Vice President, Chief Strategy Officer, Time Warner Cable	8
Prepared statement	10
Tauke, Thomas J., Executive Vice President, Verizon	11
Prepared statement	13

APPENDIX

Inouye, Hon. Daniel K., U.S. Senator from Hawaii, prepared statement	37

BROADBAND PROVIDERS AND CONSUMER PRIVACY

THURSDAY, SEPTEMBER 25, 2008

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

The Committee met, pursuant to notice, at 10:06 a.m., in room SR–253, Russell Senate Office Building, Hon. Byron L. Dorgan, presiding.

OPENING STATEMENT OF HON. BYRON L. DORGAN, U.S. SENATOR FROM NORTH DAKOTA

Senator DORGAN. The hearing will come to order.

This is a hearing of the Senate Commerce Committee. We have a hearing today on broadband providers and consumer privacy, a subject which is interesting and new, relatively new, to this Committee. It is the second of a number of hearings on this subject.

I wish all of you good morning.

I am joined by Senator Hutchison who is the Ranking Member. Senator Inouye is not able to be with us and has asked me to chair the hearing. I chaired the previous hearing on this subject as well at his request, and I am happy to do that.

This hearing is to provide an examination of the privacy rights of Internet users and the practices of broadband providers. The Commerce Committee has had a long interest in the subject of protecting privacy, and now I feel we need to take a closer look at Internet users' privacy as the field of online advertising develops.

I want to make it clear that I understand and I think all of my colleagues in the Congress would understand that there are many benefits to online advertising. It is an architecture that is important to our economy. It allows many of the sites and services that we all know and understand to grow and thrive. So this is not an inquiry about whether advertising is relevant or important. Advertising on the Internet plays an important role in Internet commerce.

While most of the conversation about Internet advertising in the past years has been focused on economic benefits, however, consumers say in surveys that they worry about privacy. Survey results released today from *Consumer Reports* shows that 72 percent of consumers are concerned that their online behavior is being tracked or profiled, and they are concerned about that. The poll found that 93 percent of Americans think Internet companies should always ask permission before using personal information.

I think it is the case that the invisibility of data collection practices and users' ability to control their information is a concern, and I think it is time that the Senate and regulators try to understand and focus on what are the privacy questions and the aspects of the issue of privacy that we should be dealing with.

In July, we held a hearing on privacy to examine concerns about consumers being profiled and being tracked online. There is a lot the Committee has yet to learn about data collection practices. We learned some things at the last hearing. We heard from NebuAd, a company that was working with some Internet service providers to gain access to the content on their networks in order to provide advertisers profiles of broadband providers' customers. NebuAd later halted those plans.

In July, the broadband providers were not able to attend our hearing. For many of them, this was a new area, and today we appreciate the participation of AT&T, Verizon, and Time Warner Cable. It should be noted that these companies had not previously agreed to provide customer data to NebuAd or similar companies.

We also appreciate the participation today of Public Knowledge at this hearing.

We will focus on privacy expectations for customers of Internet service providers. People do expose themselves online by where they go and what they do, and often type in sensitive information, personal information, and financial information. We have very little competition in the broadband market. As a matter of fact, around most of this country, most Americans have one or at the most perhaps two choices for broadband. And as broadband service is so vital to the American people and to our communities, we want to make sure that providers are respecting the privacy protections of consumers and that those protections are in place. Internet service providers have access to all of that customer's information and behavior, and the question is what is being done with it.

Again, let me emphasize that I appreciate the Internet service providers being willing to come to us today and talk about these issues because the issues are not just important to policymakers. These issues I think are important in the long term to Internet service providers as well.

I do think we need to update our privacy laws and we need to ensure we have similar protection across platforms. We need to protect sensitive information, make sure customers know what companies are doing with their information so that customers can make informed choices about their participation, and are given clear information about opt-in or dealing with other regimes that might be established.

This is the second hearing, and I assume that the Commerce Committee will want to hear more as we enter the next session of Congress. Now the Committee is here to listen and to thank the witnesses for testifying.

Let me call on my colleague from Texas, Senator Hutchison.

STATEMENT OF HON. KAY BAILEY HUTCHISON,
U.S. SENATOR FROM TEXAS

Senator HUTCHISON. Well, thank you, Senator Dorgan. I appreciate your calling attention to this issue, and I want to say that it

is an important issue that we look at because we know that there are many advertising opportunities now on the Internet, which is a good thing, as the Senator said. It is good for the economy. It is also good for business to be able to target advertising and be able to have efficient use of the advertising dollars.

I also think it is helpful to consumers to be able to find the products they are looking for, the services that they are looking for in a targeted way, and that provides more free service on the Internet, which is what we all want. So that is the good side of advertising.

On the other side, we surely need to be informed. Consumers need to be informed about what online entities are doing with their personal data information, and of course, since so many, especially in our rural areas, depend on broadband for commerce, as well as health care and education, people are putting more of their personal information online. So I think transparency and disclosure are very important.

I would say I hope we do not charge into legislating in this area before we do fully understand what is possible, what is not possible, what is helpful, and what is not helpful, and what would help the right type of opportunities but not hinder the overall ways that we can have access to advertising. So it is a complicated area and one that we ought to look at, fully understand before we rush into legislation that could curb our economy.

I want to say that I am not going to be able to stay. I have to be on the floor at 10:30, but I appreciate your calling this hearing and I will certainly look at the testimony later.

Senator DORGAN. Senator Hutchison, thank you very much.

I share the view. I do not think that there will be a stirring here to rush toward some sort of legislative approach. I think, first, it is very important that we understand this. There may well need to be legislative solutions at some point in the future, but first, I think it is a complicated area and we need to understand it. I certainly agree with that.

Senator Vitter?

STATEMENT OF HON. DAVID VITTER, U.S. SENATOR FROM LOUISIANA

Senator VITTER. Thank you very much, Mr. Chairman, for calling this hearing as well. We examined this issue earlier this year in a hearing with other online companies. So I am looking forward to the views of these Internet service providers and others on this very important issue.

I agree we need to look at this carefully. We need to attack bad behavior. We need to do it in a way that will not be out of date tomorrow as technology advances, and I think we need to do it in a way that is not technology-specific, picking winners and losers, but sets a broad-based policy in a way that can effectively be implemented.

So I look forward to listening closely to the testimony to figure out how we can best accomplish that. Thank you.

Senator DORGAN. Thank you, Senator Vitter.

We have four witnesses today. We will, by consent, include their entire statements as a part of the permanent record and ask the witnesses to summarize their statements.

First, we will hear from Ms. Dorothy Attwood, who is the Senior Vice President for Public Policy and Chief Privacy Officer for AT&T Services. Ms. Attwood, thank you for being with us. You may proceed.

STATEMENT OF DOROTHY ATTWOOD
SENIOR VICE PRESIDENT, PUBLIC POLICY
AND CHIEF PRIVACY OFFICER, AT&T INC.

Ms. ATTWOOD. Thank you very much. Thank you, Senator Dorgan and other Committee Members, for providing AT&T the opportunity to discuss online behavioral advertising and its important privacy implications.

My name is Dorothy Attwood and I am AT&T's Senior Vice President and Chief Privacy Officer.

Senator Dorgan, AT&T appreciates your leadership on this issue. It has fomented a necessary and productive discussion among all key stakeholders, and it has encouraged our industry to listen closely to our customers and take a careful look at how best to engage in different modes of online advertising. Indeed, you will hear today a remarkable consensus about the overriding importance of a consumer-focused approach to online advertising and the need to ensure that consumers maintain ultimate and effective control over their information.

American consumers benefit immeasurably from our Internet ecosystem, which is rich in innovative services and varied content information and entertainment. Online advertising is a key component of this ecosystem as it fuels investment and enables many free and discounted services and funds today's vast diversity of Internet content.

But online advertising, especially new forms of highly targeted behavioral advertising, also raise important consumer privacy concerns that policymakers and industry must carefully weigh. Setting proper policy in this area is crucial to maximizing the consumer benefit of a healthy Internet marketplace.

Online behavioral advertising is the practice of tracking a consumer's web browsing and search activity across unrelated Websites. Notably, both the tracking and the association of the websites are largely invisible to the end user and the resulting information is used to create a distinct user profile and deliver highly targeted or personalized advertising. It is, indeed, a next generation capability and it can clearly be distinguished from the simple and longstanding practice of tracking a consumer's use of an individual Website or obviously related Websites.

AT&T does not today engage in online behavioral advertising either through the so-called "deep packet" inspection or any other technique. Of course, if done properly, the practice can be valuable to consumers and can measurably improve their online experience. But we believe just as strongly that it is essential to include strong privacy protections in the design of any online behavioral advertising program and that any privacy framework should shed clari-

fying light on what is today something quite invisible to the consumer.

Thus, we will engage in online behavioral advertising only after validating the various technologies and only after establishing clear and consistent methods to ensure the protection of and ultimate consumer control over consumer information. Our deployment of any online behavioral advertising practice will be governed by the imperative of meaningful consent and a consumer-focused privacy framework based on the following principles: transparency, customer control, privacy protection, and customer value.

More specifically, we believe that a forward-looking advertising practice requires a forward-looking customer notice and consent model. For this reason, AT&T will not use consumer information for online behavioral advertising without an affirmative advance action by the customer that is based on a clear explanation of how the consumer's action will affect the use of her information. This means that a consumer's failure to act will not result in any collection and use of that consumer's information for online behavioral advertising purposes by default.

Even though AT&T and most other Internet service providers do not engage in online behavioral advertising, make no mistake, this practice is well underway today. Already ad networks and search engines track and store a vast trove of data about consumers' online activities, and the technologies they use have evolved just beyond tracking consumers' web surfing activity at sites at which they sell advertising. They now also have the ability to observe a user's entire web browsing experience at a granular level. If anything, this largely invisible practice of ad networks and search engines raise at least the same privacy concerns as do other online behavioral techniques that ISPs could employ.

For this reason, we believe that any privacy framework for online behavioral advertising must apply to all entities involved in Internet advertising, including ad networks, search engines, and ISPs. A policy regime that applies only to one set of actors will arbitrarily favor one business model or technology over another, but most importantly represent only a partial and entirely unpredictable solution for consumers.

Thus, we urge all entities that engage in online behavioral advertising, including especially those who already are engaging in the practice, to join AT&T in committing to a policy of advance, affirmative consumer consent.

Again, thank you for the opportunity to speak here today, and I look forward to your questions.

[The prepared statement of Ms. Attwood follows:]

PREPARED STATEMENT OF DOROTHY ATTWOOD, SENIOR VICE PRESIDENT, PUBLIC POLICY AND CHIEF PRIVACY OFFICER, AT&T INC.

Thank you, Chairman Inouye and Ranking Member Hutchison, for providing AT&T Inc. the opportunity to discuss online advertising and, more specifically, the issue that has received a good deal of recent attention, so-called online behavioral advertising. We trust that this hearing will help the discussion evolve past slogans and rhetoric to a more thoughtful examination of the facts and the development of a holistic consumer privacy policy framework that all participants in the online behavioral advertising sphere can and will adopt.

Your interest in these matters surely is warranted. Online advertising fuels investment and innovation across a wide range of Internet activities, and provides the

revenue that enables consumers to enjoy many free and discounted services. Likewise, website publishers make most of their money from advertising, which revenue in turn funds today's vast wealth and diversity of Internet content and information—most of which consumers enjoy, again, for free. On the other hand, online advertising, especially next-generation forms of highly targeted behavioral advertising that involve tracking consumer web browsing and search activities, raise important consumer-privacy concerns that policymakers and industry must carefully weigh. In short, setting proper policy in this area will be crucial to a healthy and growing Internet ecosystem that benefits consumers.

AT&T does not today engage in online behavioral advertising, but we understand the uniquely sensitive nature of this practice. We have listened to our customers and watched the debate unfold, and are responding by advocating for a consumer-focused framework. As described in more detail herein, the pillars of this framework—*transparency, consumer control, privacy protection, and consumer value*—can be the foundation of a consistent regime applicable to all players in the online behavioral advertising sphere—including not just Internet Service Providers ("ISPs"), but also search engines and third party advertising networks—that both ensures that consumers have ultimate control over the use of their personal information and guards against privacy abuses.[1]

In particular, we believe that effective customer control for online behavioral advertising requires meaningful consent and therefore commit that *AT&T will not use consumer information for online behavioral advertising without an affirmative, advance action by the consumer that is based on a clear explanation of how the consumer's action will affect the use of her information.* This concept—often generically referred to as "opt-in"—means that a consumer's failure to act will *not* result in any collection and use by default of that consumer's information for online behavioral advertising purposes. This affirmative consent model differs materially from the default-based privacy policies that advertising networks and search engines—which already are engaged in online behavioral advertising—currently employ. Given the obvious consumer benefits of such a model, we encourage all companies that engage in online behavioral advertising—regardless of the nature of their business models or the technologies they utilize—likewise to adopt this affirmative-advance-consent paradigm.

What is Online Behavioral Advertising?

There is no single, settled definition of online behavioral advertising in statute or case law, but the FTC and others have used the term to refer to it as the tracking of a consumer's web search and web browsing activities—by tracking either the person or a particular Internet access device, be it a computer, data-enabled mobile phone, or some other communications vehicle—to create a distinct profile of the consumer's online behavior. In this sense, it can clearly be distinguished from the simple practice of tracking a consumer's use of an individual website or obviously-related websites (such as those operated under a common trademark, trade name or conspicuously disclosed corporate affiliation), which practice does not necessarily raise the same privacy concerns as online behavioral advertising but which nonetheless can and should expressly be disclosed to Internet users. Privacy concerns about online behavioral advertising are not new—indeed, DoubleClick's (now a Google subsidiary) use of tracking cookies to collect and use information about consumer web browsing activity was the subject of an FTC proceeding in 2000.[2] More recently, the FTC and Congress have appropriately asked questions about the privacy implications of emerging online advertising businesses that involve the tracking of consumer web browsing and search activity. Thus, consistent with the focus of recent public discussion, we consider online behavioral advertising to be: (1) the tracking of user web browsing and search activity across unrelated websites, (2) when the tracking and association of the websites or their components are largely invisible to the user, and (3) the resulting information is used to create a distinct user profile and deliver targeted advertising content.

Online behavioral advertising can take many forms. It can, for instance, involve the use by an ISP of technologies to capture and analyze a user's Internet browsing activities and experience across unrelated websites. These more ISP-specific meth-

---

[1] The policy framework that AT&T proposes here is informed by and should complement the Online Behavioral Advertising Self-Regulatory Principles issued by staff of the Federal Trade Commission in December of last year. Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles, available at *http://www.ftc.gov/05/2007/12/P85900stmt.pdf*.

[2] Letter from Joel Winston, Acting Associate Director, Division of Financial Practices, Bureau of Consumer Protection, Federal Trade Commission, to ChristineVarney, Hogan & Hartson, Re: DoubleClick Inc. (Jan. 22, 2001)(memorializing closure of FTC staff investigation).

odologies are not, however, the only—and certainly are not nearly the most prevalent—forms of online behavioral advertising. Advertising-network technologies have evolved beyond solely tracking consumer web surfing activity at sites on which they sell advertising. They now also have the ability to observe a user's entire web browsing experience at a granular level. Techniques include the ad network "dropping" third-party tracking "cookies" on a consumer's computer to capture consumer visits to any one of thousands of unrelated websites; embedding software on PCs; or automatically downloading applications that—unbeknownst to the consumer—log the consumer's full session of browsing activity.

Ad networks and other non-ISPs employ these capabilities at the individual browser or computer level and they are as effective as any technique that an ISP might employ at creating specific customer profiles and enabling highly targeted advertising. Already ad networks and search engines track and store a vast trove of data about consumers' online activities. Google's practices exemplify the already extensive use of online behavior advertising, particularly by nonISPs. Google logs and stores users' search requests, can track the search activity by IP address and a cookie that identifies the user's unique browser, and can even correlate search activities across multiple sessions, leading to the creation of a distinct and detailed user profile. Through DoubleClick, Google can drop tracking cookies on consumers' computers so that whenever the consumer visits websites that contain a display ad placed by DoubleClick (which can be for virtually any product or service), the consumer's web browsing activity can be tracked across seemingly unrelated sites (*e.g., CNN.com* or *ESPN.com*). Google further has access to enormous amounts of personal information from its registered users, which its privacy policy expressly confirms can be combined with information from other Google services or third parties for the "display of customized content and advertising." And it even scans e-mails from nonGmail subscribers sent to Gmail subscribers for contextual advertising purposes.

Thus, if anything, the largely invisible practices of ad-networks and search engines raise at least the same privacy concerns as do the online behavioral advertising techniques that ISPs could employ, such as deep-packet-inspection, which have application beyond mere targeted advertising, including managing network congestion, detecting viruses and combating child pornography. In short, the privacy and other policy issues surrounding online behavioral advertising are not technology-specific. The relevant touchstones are the manner in which consumer information is tracked and used, and the manner in which consumers are given notice of and are able to consent to or prohibit such practices. Those factors are entirely technology-neutral.

AT&T's Approach to Online Behavioral Advertising

AT&T does not today engage in online behavioral advertising.[3] This is not because AT&T sees no value in this next-generation form of online advertising. Indeed, if done properly, online behavioral advertising could prove quite valuable to consumers and could dramatically improve their online experiences. We do, however, believe it is essential to include strong privacy protections in the design of any online behavioral advertising program, which is why we will initiate such a program only after testing and validating the various technologies and only after establishing clear and consistent methods and procedures to ensure the protection of, and ultimate consumer control over, consumer information. We further intend to work with privacy advocates, consumer privacy coalitions and fellow industry participants in a cooperative, multifaceted effort that we trust can and will lead to a predictable consumer driven framework in this area. In any event, if AT&T deploys these technologies and processes, it will do so the right way.

Against this backdrop, AT&T has already listened closely to its customers and will adopt meaningful and flexible privacy principles that will guide any effort to engage in online behavioral advertising. We summarize this framework as follows:

[3] AT&T does engage in some of the more ordinary and established aspects of online advertising. Like virtually every entity with a retail Internet presence, AT&T tracks usage on its own websites, such as *att.com,* in order to improve the online experience, optimize a particular site's capabilities and ease-of-use, and provide the most useful information to consumers about AT&T's products and services. In addition, like thousands of other businesses that operate websites, AT&T does business with advertising networks and has partnered with providers of online search. For example, on the AT&T broadband Internet access portal, AT&T makes space available for advertising provided by the Yahoo! advertising network, and users of the portal may be shown advertising that is based on their activity across sites signed up to the Yahoo! advertising network. Also by way of example, we have arranged for the Google search box to appear on our *my.att.net* site. In this regard, then, we are no different than any other website publisher.

- *Transparency:* Consumers must have full and complete notice of what information will be collected, how it will be used, and how it will be protected.
- *Consumer Control:* Consumers must have easily understood tools that will allow them to exercise meaningful consent, which should be a sacrosanct precondition to tracking online activities to be used for online behavioral advertising.
- *Privacy protection:* The privacy of consumers/users and their personal information will be vigorously protected, and we will deploy technology to guard against unauthorized access to personally identifiable information.
- *Consumer Value:* The consumer benefits of an online behavioral advertising program include the ability to receive a differentiated, secure Internet experience that provides consumers with customized Internet advertisements that are relevant to their interests. But we think the future is about much more than just customized advertising. Consumers have shown that in a world of almost limitless choices in the content and services available on the Internet, they see great value in being able to customize their unique online experience. That is the ultimate promise of the technological advances that are emerging in the market today.

Call to Action

We believe these principles offer a rational approach to protecting consumer privacy while allowing the market for Internet advertising and its related products and services to grow. But, in order for consumers truly to be in control of their information, all entities involved in Internet advertising, including ad networks, search engines and ISPs, will need to adhere to a consistent set of principles. A policy regime that applies only to one set of actors will arbitrarily favor one business model or technology over another and, more importantly, represent only a partial and entirely unpredictable solution for consumers. After all, consumers do not want information and control with respect to just a subset of potential online advertising or the tracking and targeting that might underlie those ads. Thus, we urge all entities that engage in online behavioral advertising—including especially those who already engage in the practice—to join AT&T in committing to a policy of advance, affirmative consumer consent.

Senator DORGAN. Ms. Attwood, thank you very much for your testimony.

Next, we will hear from Mr. Peter Stern who is the Chief Strategy Officer for Time Warner Cable. Mr. Stern, you may proceed.

STATEMENT OF PETER STERN, EXECUTIVE VICE PRESIDENT, CHIEF STRATEGY OFFICER, TIME WARNER CABLE

Mr. STERN. Good morning, Mr. Chairman, Members of the Committee. My name is Peter Stern. I am Executive Vice President and Chief Strategy Officer at Time Warner Cable.

I am pleased to testify before you today and appreciate this Committee's diligent effort to grapple with the complex and still-evolving Internet advertising marketplace and to assess its impact on consumer privacy.

Presently, Time Warner Cable does not engage in targeted Internet advertising as an ISP or as a Website operator.

If Time Warner Cable decides to engage in such activities, our customers' privacy will be a fundamental consideration. The protection of subscriber privacy is not only important as a matter of public policy. Our ability to succeed depends on winning and retaining the trust of our customers. Accordingly, we support a framework that would provide consumers with the opportunity to affirmatively consent to receive online targeted advertising.

We believe that achieving and sustaining our subscribers' trust requires adhering to a privacy framework that addresses four principles: first, giving customers control; second, providing trans-

parency and disclosure; third, safeguarding personal information; and fourth, providing customers with value.

Let me also add, however, that any such framework can only truly protect the privacy interests of consumers if it is universally adopted by all providers of targeted online advertising. Quite simply, it makes no difference to a consumer whether a targeted online ad is based on data collected by an ISP, an ad network, or an applications provider. A framework that leaves any provider uncovered would leave all users unprotected. In addition, common rules are the only way to ensure all businesses can compete on a level playing field.

Let me elaborate briefly on the four principles I have mentioned.

First, customer control means consumers will be able to exercise affirmative consent before having their online activities collected and used for targeted online advertising. Internet subscribers that decline to consent or fail to act should not have their online activities tracked or used for targeted online advertising. Control also means that the consent mechanism should be easy to use. Customers should be free to change their election at any time, and their election will remain in effect unless they change it.

Second, transparency and disclosure means ensuring that a customer's consent to targeted online advertising is informed. This means giving Internet users clear and timely notice regarding what is collected, how it is used, and what consumers need to do if they do not want to participate. And by this, we do not mean fine print. We mean prominent and plain English.

Third, safeguarding information means preventing unauthorized access to customers' personal information. It also means preventing disclosure or sale of such information to third parties absent consent of the customer.

Last, providing value means offering targeted online advertising in a manner that enhances the Internet experience for consumers. Instead of a barrage of irrelevant ads, consumers can receive ads tailored to reflect their interests. Targeted online advertising can also be used to protect consumers from seeing ads they do not want. Advertising can be a public good when it educates consumers about relevant choices.

Most companies that provide services on the Internet are presently under no obligation to disclose or obtain consent for the collection and use of consumers' online information. While some provide disclosure and give consumers the ability to opt out, this falls short of the principle of consumer control I have articulated.

Therefore, Time Warner Cable believes that the four principles I have outlined should serve as a policy framework that would apply to all companies involved in targeted online advertising. Time Warner Cable stands ready to work with this Committee and other stakeholders to help foster the development and implementation of such a framework.

I thank the Members of this Committee for the opportunity to appear before you today on this important issue, and I would be happy to answer any questions you might have.

[The prepared statement of Mr. Stern follows:]

PREPARED STATEMENT OF PETER STERN, EXECUTIVE VICE PRESIDENT, CHIEF STRATEGY OFFICER, TIME WARNER CABLE

Good morning, Mr. Chairman, Members of the Committee, my name is Peter Stern. I am Executive Vice President and Chief Strategy Officer at Time Warner Cable, where I am responsible for strategy and planning, including for our Road Runner high-speed online service.

I am pleased to testify before you today and appreciate this Committee's diligent effort to grapple with the complex and still-evolving Internet advertising marketplace and to assess its impact on consumer privacy.

Presently, Time Warner Cable does not engage in targeted Internet advertising as an ISP or as a website operator.

Should Time Warner Cable decide to engage in such activities, our customers' privacy will be a fundamental consideration. The protection of subscriber privacy is not only important as a matter of public policy, but it is also central to the success of our business. The bedrock foundation of our business is our relationship with our subscribers. We operate in a highly competitive marketplace, and our ability to succeed depends on winning and retaining the trust of those customers. Accordingly, we support a framework that would provide consumers with the opportunity to affirmatively consent to receive online targeted advertising.

In the context of targeted online advertising, we believe that achieving and sustaining our subscribers' trust requires adherence to a privacy framework that addresses four principles: first, giving customers *control;* second, providing *transparency* and *disclosure;* third, *safeguarding personal information;* and fourth, providing customers with *value*.

Let me also add, however, that we strongly believe that any such framework can only truly protect the privacy interests of consumers if it is universally adopted by all providers of targeted online advertising, including ad networks, application providers and ISPs. Quite simply, it makes no difference to a consumer whether a targeted online ad is based on data collected by an ISP, an ad network or an applications provider. A framework that leaves any provider uncovered would leave all users unprotected. In addition, a common set of rules protecting consumer privacy is the only way to ensure that all businesses that provide online advertising can compete and innovate on a level playing field.

Before I go any further, allow me to clarify our definition of targeted online advertising for the purposes of applying the framework I described. At Time Warner Cable, we define it as displaying different online ads to a consumer based on that consumer's behavior on unrelated websites. So, if ads are delivered to a consumer based on that consumer's particular history of visits to multiple unrelated websites, that's targeted online advertising.

On the other hand, delivering relevant ads to a consumer based on their behavior on an *individual* website (or group of related websites) is *not* targeted online advertising. For example, if you go to Apple's website and search for an iPod, and Apple delivers ads and promotions for iPods while you are still on the Apple website, that's not targeted online advertising. That's being responsive to what you asked for, when and where you wanted it. It becomes targeted online advertising, however, if this information is retained in order to deliver ads for iPods and other portable music players while you are visiting unrelated websites.

Let me elaborate briefly on the four principles I've mentioned.

First, *customer control* means consumers will be able to exercise *affirmative* consent to having their activities collected and used for targeted online advertising. Internet subscribers that decline to consent or fail to act should not have their online activities tracked or used for targeted online advertising. Control also means that the consent mechanisms should be easy to use, to ensure that customers are free to change their election at any time, and that their election will remain in effect unless they change it.

Second, *transparency and disclosure* means ensuring that a customer's consent to targeted online advertising is informed. This means giving Internet users clear and timely notice regarding what type of online usage information is tracked and collected, how that information is used to provide targeted online advertising, and what steps consumers can take should they decline to participate. And by this, we don't mean fine print. We mean prominent and plain English.

Third, *safeguarding personal information* means preventing unauthorized access to customers' personal information. It also should mean preventing disclosure or sale of such information to third parties absent consent of the customer. We also believe that policymakers and the public should continue to discuss whether there are categories of particularly sensitive information, such as personal medical infor-

mation, that should be entirely off limits to targeted online advertising or subject to special controls.

Last, *providing value* means offering targeted online advertising in a manner that enhances the Internet experience for consumers. Time Warner Cable firmly believes that targeted online advertising can benefit consumers. Instead of a barrage of irrelevant ads, subscribers can receive information about services and offerings tailored to reflect their interests. Targeted online advertising can also be used to protect consumers from seeing ads they don't want. Advertising can be a public good, when it educates consumers about relevant choices. Properly implemented, technology can help advertising achieve this potential, possibly even increasing the number of ads consumers want to see.

In addition, targeted online advertising provides important benefits for advertisers and providers of Internet applications and services. Revenues from such advertising can offset the costs of providing services to consumers, and can allow businesses to offer services at discounts or even without direct payment from end users. In this manner, targeted online advertising can deliver value to consumers while helping to preserve and promote access to and enjoyment of the rich diversity of the Internet.

Most companies that provide services on the Internet are presently under no obligation to disclose, or obtain consent for, the collection and use of consumers' online usage information. And in the case of some of the largest ad networks and applications providers, the amount of information such companies possess about consumers dwarfs that obtained by ISPs.

It is certainly true that many providers of targeted online advertising already voluntarily disclose the extent to which they collect and use data about consumers. And some may also provide consumers the ability to "opt out" of participating in such an arrangement. But the extent of such disclosure varies greatly and is often opaque; and the process for opting out can be complicated, and in any case falls short of the principle of consumer control I have articulated.

Therefore, Time Warner Cable believes that the four principles I have outlined—customer control, transparency and disclosure, safeguarding personal information, and providing value—should serve as the cornerstone of a uniform policy framework that would apply to *all* companies involved in targeted online advertising. Time Warner Cable stands ready to work with this Committee and other stakeholders to help foster the development and implementation of such a framework.

I thank the Members of this Committee for the opportunity to appear before you today on this important issue, and I would be happy to answer any questions you might have.

Senator DORGAN. Mr. Stern, thank you very much for being with us.

Next, we will hear from Mr. Tom Tauke, the Executive Vice President of Public Affairs, Policy and Communications at Verizon Communications. Mr. Tauke, you may proceed.

STATEMENT OF THOMAS J. TAUKE, EXECUTIVE VICE PRESIDENT, VERIZON

Mr. TAUKE. Verizon is not engaged in behavioral advertising, but we are very much aware of the concerns that have been expressed by consumers and this Committee about some of the practices that other Internet players are engaged in to send targeted advertising to consumers. Therefore, we have focused attention within Verizon on what policies and practices related to online advertising we should follow to keep faith with our own customers. And we've looked at what practices would work for the entire on-line industry.

Perhaps it would be useful if I just outlined the framework of our thinking.

First, we focused on the consumer and tried to look at the issue from his or her perspective. It seemed clear to us that consumers want information so they know what is going on. They want to be in control of their online experience, and they want to be able to

choose whether or not their online usage is tracked and used to send them targeted advertising.

Second, we concluded that any policy governing online advertising should be centered around the notion of meaningful consent by the consumer. We had a lot of discussion about opt in and opt out. We concluded that those terms are not particularly meaningful in the online world. Most consumers, I suspect, are like me. We are trying to do something online. The screen pops up. We hit "OK" or "continue" and move on, not really aware of what we just opted into.

So we focused on the concept of meaningful consent and what that means. Our sense is that meaningful consumer consent in this context requires three elements.

One, transparency. That means conspicuous and clearly explained disclosure to consumers about what types of data are collected for what purposes and how it will be used.

Affirmative choice is the second principle. With knowledge of what they are choosing, consumers would have to affirmatively act, affirmatively agree to permit tracking of their online activity.

And third, consumer control. Consumers should have the ongoing ability to change their choice.

Senator Dorgan, you put this pretty well in a previous hearing on this issue when you talked about a consumer going into the mall. I believe it was your daughter. If you walk into the store and the store keeps track of what you are doing and buying so they can bill you at the end, you know, you probably think that is OK. And if you do not like it, you walk out. But if someone starts following you around the mall tracking your activity from store to store, you would feel pretty uneasy about that, I suspect, unless you had invited them along.

Using that analogy, what we believe is that before anyone follows a consumer around online to target them for advertising, that the consumer must know what is going on, must make an affirmative choice to permit that activity, and should be able to turn around at any time and say, I do not want you following me around anymore.

We have been talking to other companies engaged in online services, and we believe that there is a lot of support, as evidenced here today, for the recommendations we are making in the testimony I submitted to the Committee. Really, everyone should embrace policies that put the consumer in control of the online experience, and from consumers' perspective, it really does not matter who is doing the behavioral advertising, whether it is companies providing their browser or their search engine, their access, or any other online service. All online players should protect the privacy of online users.

The advertising industry, importantly, also appears to be interested in establishing a set of consistent best practices. That industry has a pretty good record of self-policing, with the Federal Trade Commission helping ensure that the advertising industry's best practices are enforced to protect consumers.

With that model in mind, we are reaching out to the online industry to see if we can develop a set of best practices for online advertising that will protect consumers. And we will work with this

Committee and other interested organizations to figure out how we can make sure the consumers feel secure and in charge when they are online, that the rapidly advancing communications and information processing technology is used to enhance consumers' online experience, not spoil it, and that the Internet continues to open new worlds of opportunities for each of us.

Thank you very much.

[The prepared statement of Mr. Tauke follows:]

PREPARED STATEMENT OF THOMAS J. TAUKE, EXECUTIVE VICE PRESIDENT, VERIZON

Chairman Inouye, Ranking Member Hutchison and Members of the Committee: thank you for the opportunity to discuss the important concerns and perspectives surrounding consumer privacy in the area of online advertising.

Today, more than 60 million American homes are connected to the Internet via broadband, and the wide range of content, services, and applications online—most offered for free—draws more people online every day.

While Verizon does not rely on online advertising as a significant source of revenue, we recognize that it has been a key business model that has helped make the Internet a growth engine for the U.S. economy.

Yet, using consumers' web-surfing data to foster targeted online advertising raises complex and important issues surrounding online privacy. Consumers and policymakers want to understand what personal information is being collected and used for advertising purposes. They want to know what privacy and consumer protections are in place, and what choices are available to participate—or not—in behavioral advertising models.

In a rapidly changing and innovative environment like the Internet, maintaining consumer trust is essential. It is critical that consumers understand what forms of targeted online advertising their service providers and favorite websites employ. If certain practices cause consumers to believe that their privacy will not be protected, or their preferences won't be respected, they will be less likely to trust their online services, and the tremendous power of the Internet to benefit consumers will be diminished. So, maintaining consumer trust in the online experience is critical to the future success of the Internet.

With that in mind, let me begin by describing the online advertising techniques Verizon uses today over its wireline networks.

Verizon's online advertising involves the practices commonly accepted throughout the Internet, such as the use of cookies or ad delivery servers to provide advertising that is limited to users of Verizon's own services or websites. We also provide ad-supported search results to help consumers find the websites they are looking for when they mistype an address. These practices, which are neither new nor unique, improve consumers' interaction with our websites and services, and increase the relevance of the advertising displayed to our customers or to visitors of our sites.

One technology that has received attention of late is "packet inspection." To be clear, Verizon has not used—and does not use—packet inspection technology to target advertising to customers, and we have not deployed the technology in our wireline network for such purposes.

Packet inspection can be a helpful engineering tool to manage network traffic and enable online services and applications consumers may wish to use. The perceived problem with "packet inspection" is not the technology. Many useful technologies can be used for nefarious purposes. The problem arises if packet inspection is used to inappropriately track customers' online activity without their knowledge and consent and invade their personal privacy.

In fact, any technology that is used to track and collect consumer online behavior for the purposes of targeted advertising—regardless of which company is doing the collecting—should only be used with the customer's knowledge and consent in accordance with the law, a company's specific privacy policies, and the privacy principles outlined below.

Protecting our customers' privacy has long been, and will continue to be, a priority at Verizon. We are committed to maintaining strong and meaningful privacy protections for consumers in this era of rapidly changing technological advances. We are strong proponents of transparency and believe that consumers are entitled to know what kinds of information we collect and use, and should have ready access to effective tools that allow them to control the use of that information.

At Verizon we have worked to craft—and communicate to our customers—responsible policies aimed at protecting online privacy.

We can commit—and believe that all companies should commit—to a set of best practices in the area of online behavioral advertising. The principles and best practices should apply to all online companies regardless of their technology or the platform used. The principles underlying the consumer protection practices we support are these:

First, meaningful consent.

Verizon believes that before a company captures certain Internet-usage data for targeted or customized advertising purposes, it should obtain meaningful, affirmative consent from consumers. Meaningful consent requires: (1) transparency, (2) affirmative choice, and (3) consumer control.

Transparency involves conspicuous, clearly explained disclosure to consumers as to what types of data are collected and for what purpose that data is being used, how that data is retained and for how long, and who is permitted access to the data.

Consumers would then be able to use these clear explanations to make an *affirmative choice* that their information can be collected and used for online behavioral advertising. Importantly, a consumer's failure to consent should mean that there is no collection and use of that consumer's information for online behaviorally targeted advertising based on tracking of the consumer's Internet usage.

Finally, *consumer control* means that consumers have an ongoing opportunity to make a different choice about behavioral advertising. In other words, should consumers at some later time choose not to participate in the behavioral advertising, there are equally clear and easy-to-use instructions to make that change. That preference should remain in effect unless and until the consumer changes it.

Second, security practices.

Any company engaged in tracking and collecting consumer online behavioral information must have appropriate access, security, and technological controls to guard against unauthorized access to any personal information.

Third, safeguards for sensitive information.

Special attention must be given to the protection of information of a sensitive nature (*e.g.,* accessing medical websites). This information should not be collected and used for online behavioral advertising unless specific, affirmative consent, and customer controls are in place to limit such use. Specific policies may be necessary to deal with this type of information.

Consistent with our long-standing policies and practices, Verizon also believes that the content of communications, such as e-mail, instant messages, or VoIP calls, should not be used, analyzed, or disclosed for purposes of Internet-based targeted advertising.

Fourth, certification.

It is critical that all participants in online advertising—ad networks, publishers, search engines, Internet service providers, browser developers and other application providers—commit to these common sense principles and best practices through a broad-based, third party coalition. To achieve this, we plan to work with stakeholders in the Internet and advertising arenas, including other companies, industry groups and policy organizations.

The focus of this coalition and the principles should be the protection of consumers, not the technology or applications that happen to enable the data collection. Widespread and uniform adoption of principles will greatly enhance the public trust, address expressed privacy concerns regarding web tracking practices, and serve as a foundation for further discussion with policymakers and consumer groups.

We believe that companies engaged in online behavioral advertising should agree to participate in a credible, third-party certification process to demonstrate to consumers that they are doing what they say with regard to the collection and use of information for online behavioral advertising. This process would confirm that companies are complying with and respecting consumers' expressed choices regarding such data collection.

We believe a framework such as this is a rational approach that protects consumer privacy, while allowing the market for Internet advertising and its related products and services to grow.

Should a company fail to comply with these principles, we believe the Federal Trade Commission has authority over abuses in the privacy area and can take appropriate measures against companies that intentionally violate applicable consumer protection laws.

We hope to use the next few months to work with all players in the Internet space to create and agree to live by industry best practices for online advertising.

Thank you.

Senator DORGAN. Mr. Tauke, thank you very much for your testimony.

Finally, we will hear from Ms. Gigi Sohn, the President and Co-Founder of Public Knowledge. Ms. Sohn, you may proceed.

STATEMENT OF GIGI B. SOHN, PRESIDENT, PUBLIC KNOWLEDGE

Ms. SOHN. Senator Dorgan, Members of the Committee, thanks for giving me the opportunity today to testify on behalf of Internet users.

I would like to focus my comments on the growing use of technologies known as deep packet inspection, or DPI.

The use of DPI technology has serious implications for the privacy rights of Americans. Public Knowledge, in partnership with Free Press, has been analyzing these technologies and their impact on both privacy and an open Internet. Our organizations published a white paper entitled *NebuAd and Partner ISPs: Wiretapping, Forgery, and Browser Hijacking,* which examined the technical and policy aspects of DPI. I applaud the Committee for its scrutiny of the use of these technologies.

Simply put, DPI is the Internet equivalent of the Postal Service reading your mail. While a postal worker might read your mail for any number of reasons, the fact remains that your letter is being read by the very person whose job it is to deliver it.

When you use the Internet for web browsing, e-mail, or any other purpose, the data you send and receive is broken up into small chunks called packets. These packets are wrapped in envelopes which, much like paper envelopes, contain addresses for both the sender and the receiver, though they contain little information about what is inside.

Until recently, when you handed that envelope to your ISP, the ISP simply read the address, figured out where to send the envelope, and handed it off to the proper mail carrier.

Now we understand that some ISPs are opening these envelopes, reading their contents, and keeping varying amounts of information about the communications inside for their own purposes. In many cases, ISPs are actually passing copies of the envelopes on to third parties who, in turn, read and make use of that information. For the most part, customers are not aware that their ISPs are engaging in this behavior. The end result is much like if the Postal Service were to open your letter, photocopy it, hand that copy to a third party, and then reseal the letter so that you would never know it had been opened in the first place.

So far, we have seen ISPs like Comcast use DPI as a means to identify and block certain types of Internet traffic, in violation of the FCC's Internet policy statement. We have also seen advertising companies like NebuAd use DPI to collect browsing histories, online habits, and other potentially personal information about users in order to display advertisements targeted to a specific user's interests.

The very nature of DPI raises grave privacy concerns.

As a result, when evaluating an implementation of DPI, there are three basic questions that must be answered in order to assess both the impact on the user's privacy and the acceptability of the

use of the technology in question. First, what purpose is the collected data being used for? Second, how is the data collected and utilized? Third, how is affirmative informed consent obtained?

Given the power of DPI and the scope of its possible uses, it is critical that we establish industry guidelines and legal protections for users. And while the use of personal data by web service providers is not the focus of today's hearing, such uses raise separate, yet important privacy questions.

Thus, any solution should strive to be comprehensive in scope and ensure that the basic principles of privacy protection are applied across the entire Internet ecosystem. These protections must ensure, first, that the purpose of the use of consumer data is one that is consistent with users' privacy expectations; second, that the amount and type of data collected is narrowly tailored to the proposed use and that the data is not kept or disseminated to third parties past what is necessary; and third, that customers have access to and actually receive adequate information about the proposed use and have affirmatively and actively consented to any practices that might violate their privacy expectations.

To achieve these goals, Congress should pass legislation that encapsulates these requirements and makes clear that the FCC has the power to enforce them.

Even though the Communications Act aims to provide comprehensive privacy protection for users of all communications technologies, gaps in the law have allowed the privacy of some Internet users to fall through the cracks. The time has now come to address these inequalities and guarantee the right to privacy for all Internet users.

In closing, I want to make one extra comment about the legislation. I want to commend the ISPs to my right for adopting the principles they have announced today, transparency, control, privacy protection, consumer value. But the problem is that the ISPs that are not here are the ones that use NebuAd and the ones that told Representative Markey and Representative Barton that they thought that they were acting within the law. And that is why I believe you need comprehensive legislation to ensure that all ISPs and not just the good guys are protecting users' privacies.

Public Knowledge is eager to work with the Committee to craft privacy legislation that will protect all Internet users.

I look forward to your questions.

[The prepared statement of Ms. Sohn follows:]

PREPARED STATEMENT OF GIGI B. SOHN, PRESIDENT, PUBLIC KNOWLEDGE

Chairman Inouye, Ranking Member Hutchison and Members of the Committee, thank you for giving me the opportunity to testify about broadband providers and consumer privacy. I'd like to focus today on the growing use of the collection of technologies known as "Deep Packet Inspection," or DPI, which has immense implications for the privacy rights of the American public. Over the past several months, Public Knowledge, in partnership with Free Press, has been analyzing these technologies and their impact on privacy and an open Internet. In June, our organizations published a white paper entitled *NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking,* which examined the technical and policy aspects of

DPI. I applaud the Committee for its continued scrutiny of the use of these technologies.[1]

I. Introduction

Today's hearing on consumer privacy comes in the wake of two high-profile online consumer privacy violations, both of which involved the use of Deep Packet Inspection (DPI) technology on an Internet Service Provider's (ISP) network.

The first instance came to light in October 2007, when an Associated Press report revealed that Comcast was interfering with its customers' BitTorrent traffic.[2] The report confirmed earlier tests conducted by independent network researcher Robb Topolski, who found that Comcast was analyzing its users' web traffic in order to determine the types of applications and protocols being used. The company then used a technique called "packet spoofing" to delay, degrade and in some cases, block traffic that was identified as being used for BitTorrent, a popular peer-to-peer file sharing protocol. Public Knowledge and Free Press filed a formal complaint with the FCC in November 2007, calling for the Commission to open a formal investigation into the ISP's practices.[3]

In January 2008, the FCC announced that it had opened a formal investigation into Comcast's blocking of BitTorrent traffic. This investigation concluded in August 2008 with the FCC upholding the Public Knowledge and Free Press complaint and reprimanding Comcast for its degradation of its users' traffic. In its ruling against Comcast,[4] the FCC ordered the company to stop blocking BitTorrent traffic and to develop a new set of network management practices that did not violate the FCC's Broadband Policy Statement.[5] In its letter of response to the FCC, Comcast confirmed that it had used DPI equipment from the Sandvine Corporation in order to identify and block BitTorrent traffic.[6]

The second instance surfaced in May 2008, when it was revealed that various regional ISPs had contracted with Knobbed, a company that provided highly targeted behavioral advertising solutions using DPI equipment. In test deployments of this technology, all of the traffic traveling over an ISP's network was routed through a DPI appliance which collected data on specific users, including websites visited, terms searched for and services and applications used. This data was then sent to Knobbed, which in turn, used the data to create detailed user profiles. These profiles were used to display highly targeted advertisements, which were dynamically displayed to the user as he or she surfed the Web.

In May 2008, Representatives Edward Markey (Chairman, Subcommittee on Telecommunications and the Internet) and Joe Barton (Ranking Member, Senate Committee on Energy and Commerce) sent a letter to Knobbed,[7] asking the company to put its pilot tests on hold, pending an investigation into the company's practices. A coalition of 15 consumer advocacy and privacy groups publicly voiced their support for this letter and urged the Congressmen to continue their investigation of Knobbed and other behavioral advertising companies.[8] In June 2008, Public Knowledge and Free Press released a technical analysis of Knobbed's behavioral advertising system, authored by networking researcher Robb Topolski.[9] The report revealed that Knobbed and its partner ISPs repeatedly violated the privacy of users, with little or no notification that DPI equipment was being used. Following the re-

---

[1] I would like to thank Public Knowledge's Equal Justice Works Fellow Jef Pearlman, Policy Analyst Mehan Jayasuriya, and Law Clerk Michael Weinberg for assisting me with this testimony.

[2] *See* Associated Press article, " Comcast blocks some Internet traffic", (October 19, 2007), available at *http://www.msnbc.msn.com/id/21376597*.

[3] *See* Free Press and Public Knowledge, *Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer to Peer Applications,* (November 1, 2007), available at *http://www.publicknowledge.org/pdf/fp__pk__comcast__complaint.pdf* [hereinafter Comcast Complaint].

[4] *See* Federal Communications Commission, *Memorandum Opinion and Order* (August 1, 2008), available at *http://hraunfoss.fcc.gov/edocs__public/attachmatch/FCC–08–183A1.pdf*.

[5] *See* FCC, *Policy Statement,* (August 5, 2005), available at *http://www.publicknowledge.org/pdf/FCC–05–151A1.pdf*.

[6] *See* Comcast Corporation, *Attachment A: Comcast Corporation Description of Current Network Management Practices,* (September 19, 2008), available at *http://downloads.comcast.net/docs/Attachment__A__Current__Practices.pdf*.

[7] Representative Edward J. Markey and Representative Joe Barton, Letter to Neil Smit, President and CEO, Charter Communications (May 16, 2008), available at *http://markey.house.gov/docs/telecomm/letter__charter__comm__privacy.pdf*.

[8] Center for Democracy and Technology *et al., Letter to Representatives Markey and Barton* (June 6, 2008), available at *http://www.cdt.org/privacy/20080606markeybarton.pdf*.

[9] *See* Public Knowledge and Free Press, Knobbed and Partner ISPs: Wiretapping, Forgery and Browser Hijacking (June 18, 2008) available at *http://www.publicknowledge.org/pdf/nebuad-report–20080618.pdf*.

lease of the report, the House Committee on Energy and Commerce convened a hearing on the topic of DPI, wherein Knobbed CEO Bob Dykes was asked to testify.

On August 1, 2008, the House Committee on Energy and Commerce followed up with a letter to 33 ISPs and software companies asking for details regarding how they were using DPI and whether and how they were disclosing those uses to their customers.[10] As a result of the Congressional scrutiny, all of Knobbed's ISP partners, including WOW! (Wide Open West), CenturyTel, Charter, Bresnan and Embarq, have decided to put a hold on their test deployments with Knobbed. In September 2008, Bob Dykes announced that he was leaving Knobbed and following his departure, the company announced that it was abandoning its behavioral advertising initiatives, in favor or more traditional advertising technologies.

II. Deep Packet Inspection

To put it simply, Deep Packet Inspection is the Internet equivalent of the postal service reading your mail. They might be reading your mail for any number of reasons, but the fact remains that your mail is being read by the people whose job it is to deliver it.

When you use the Internet for web browsing, e-mail or any other purpose, the data you send and receive is broken up into small chunks called "packets." These packets are wrapped in envelopes, which, much like paper envelopes, contain addresses for both the sender and the receiver—though they contain little information about what's inside. Until recently, when you handed that envelope to your ISP, the ISP simply read the address, figured out where to send the envelope in order to get it to its destination, and handed it off to the proper mail carrier.

Now, we understand that more and more ISPs are opening these envelopes, reading their contents, and keeping or using varying amounts of information about the communications inside for their own purposes. In some cases, ISPs are actually passing copies of the envelopes on to third parties who do the actual reading and use. In others, ISPs are using the contents to change the normal ways that the Internet works. And for the most part, customers are not aware that their ISPs are engaging in this behavior—much like if the postal service were to open your letter, photocopy it, hand that copy to a third party and then re-seal the letter, so that you would never know it had even been opened in the first place.

III. The Privacy Implications of DPI

It should be clear that the very nature of DPI technology raises grave privacy concerns. An ISP, by necessity, sees every piece of data a user sends or receives on the Internet. In the past, ISPs had little incentive to look at this information and the related privacy concerns provided a strong deterrent against doing so. However, now that technology is widely available to make use of and monetize this information, companies are exploring the limits of what they can do permissibly.

When evaluating an implementation of DPI technology, there are three basic questions that must be answered in order to assess both the impact on a user's privacy and acceptability of use of the technology in question:

1. *Purpose:* What purpose is the collected data being used for?
2. *Collection:* How is the data collected and utilized?
3. *Consent:* How was affirmative informed consent obtained?

An understanding of these questions can inform legislators and policymakers in the formation of policies, which will adequately protect users of Internet connections and services. The uses for DPI are myriad, and most raise serious privacy concerns, but each use should be measured individually against a comprehensive privacy policy.

It is also important to note that there are two parties to any Internet communication. In almost all cases, the party on the other end of a user's line will have no meaningful ability at all to know what kind of monitoring is being employed by that user's ISP or what is being done with the collected data, and will have no opportunity at all to give or to deny consent. For example, if I send you an e-mail and my ISP is using DPI to read the contents of my e-mails, your privacy has just been violated without your knowledge or consent. Any comprehensive privacy policy that addresses technologies like DPI must take into account not only the privacy rights

---

[10] See John D. Dingell (Chairman, Senate Committee on Energy and Commerce), Joe Barton (Ranking Member, Senate Committee on Energy and Commerce), Edward J. Markey (Chairman, Subcommittee on Telecommunications and the Internet), Cliff Stearns (Ranking Member, Subcommittee on Telecommunications and the Internet), *Letter to ISPs* (Aug. 1, 2008), available at *http://markey.house.gov/docs/telecomm/letter__dpi__33__companies.pdf.*

of an ISP's customers, but also those of anyone who communicates with these customers.

A. Purpose

Given DPI's potential to be used as an intrusive tool, we must first ask why the user's traffic is being collected or analyzed at all. Is the use of DPI integral to the functioning of the network or is the technology simply being used to provide the ISP with an additional revenue stream? Does the technology in question primarily benefit the ISP's bottom line, or does it give direct benefits to the customer's use of the Internet? Is it used to protect users or the integrity of the network, or simply to offer new or improved additional services?

Not all uses of DPI are inherently problematic. The first widespread uses of DPI were for security purposes: to stop malicious programs like viruses and worms from passing from one infected computer to another over the Internet. However, as seen in the recent complaint and decision against Comcast at the Federal Communications Commission (FCC), DPI can also be used to engage in impermissible, discriminatory network management practices. Taken to an extreme, we can even imagine a future where DPI is used to record and disseminate every single move a user makes on the Internet—from web browsing, e-mail and instant messaging to VoIP phone calls and video chats—to the ISP's own business advantage.

Understanding the purpose of DPI use is the first step to understanding whether that use will violate a user's expectations of privacy.

B. Collection

After we understand the purpose of a particular use of DPI, we can analyze how the data is collected and used toward that purpose. Is the user's data being collected by the ISP for its own use, or is it being passed to a third party with no connection to the user? Is all of the user's data collected, or a smaller subset of the data? Is the amount collected narrowly tailored to achieve the stated purpose, or broader than necessary, or is the amount of data actually used smaller than that collected?

It is important to note here that we should evaluate both the amount of data which reaches the party using it, and the amount of that data which is used. This is because additional data that is sent to a third party provides more opportunity for abuse of user privacy—even if that third party later chose to discard some of the more personal information. For instance, even though companies like Knobbed may choose to ignore the personal medical records or e-mails of its partner's customers, they were provided the data to do exactly that. This problem is compounded by the fact that an ISP or partner must engage in DPI to even discover what type of data is being transmitted, thereby possibly violating the user's privacy before any decision is made regarding what is to be done with the data.

It is also necessary to identify the ways in which the collected data might be tied to the user's actual identity. Is the data obtained using DPI explicitly tied to data obtained through other means—for example, the ISP's billing information, demographic information, or personal information stored on a third-party website? Can the collected data be later aggregated with this type of information? Will the data itself contain personally identifying information (PII), such as names, addresses, and credit card information submitted to websites? These questions are important because if the data in question contains PII or if it is later connected with other user data, the privacy implications are multiplied.

Implicit in the data collection question are also questions about data storage. Is the collected data kept by the party using it? If so, for how long? Is it kept in its original, complete form, or in some type of summary? Is any PII kept with the stored data?

Understanding what and how data is collected and how well that comports with the stated purpose of the collection is necessary to evaluating whether the collection will violate users' privacy expectations.

C. Consent

No inspection of a user's data will be acceptable without that user's affirmative, informed consent or law enforcement obligations. To ensure this is obtained, we must evaluate both how users are notified of the ways in which their ISP and its partners intend to use DPI, and the method by which those users affirmatively consent (or decline to consent) to those uses. To do this, we must ensure that before a user's data is inspected, the user actually receives complete, useful information, and that the user knowingly and affirmatively assents to the stated uses.

Are the answers to the above questions about purpose and collection accessible for users, and complete in the information they divulge? If any third parties are involved in the monitoring, are their identities provided for the user? Are the answers written so that the average user can make sense of them? Are the policies in ques-

tion detailed in a place and manner that ensures that the user is likely to read them? Is the user actively notified of the presence of and changes to policies and monitoring activities, or are changes made to web pages and written into the Terms of Service—without any notification to the user? Without accurate and easily understandable information that a user is actually aware of, that user cannot make informed choices about how best to manage his or her privacy online.

Finally, what is the process by which users agree (or decline to agree) to the use of these technologies? Are they subject to DPI *before* they receive meaningful notice of its use, or is the user required to take an affirmative action before his or her data is recorded or analyzed? Is the information and the action specific to the monitoring activities, or is it hidden in a larger "Acceptable Use Policy," "End User License Agreement," or other document? Does the user have the meaningful ability to change his or her choice later? Is the user actively offered a periodic chance to withdraw consent, or is he or she only asked once? And is the option not to consent a real one, without crippling or disabling of the user's service as the only alternative?

Without meaningful, informed, affirmative consent on the part of the user, personal data should not be used for any purpose that is not necessary to providing basic Internet service.

IV. ISP Disclosures

In response to Chairman Dingell and Ranking Member Barton's letter, 33 ISPs and software companies described whether and how they were using DPI and whether and how they were disclosing those uses to their customers.[11] These responses are helpful in understanding how, to date, the above three questions have been answered unsatisfactorily.

Carriers that responded to the letter fell into two basic camps. The first group of ISPs did not employ Knobbed's services and did not use any similar DPI equipment. These ISPs generally had not deployed any technologies that could track individual users' browsing habits or correlate advertising information with personal information possessed by the ISP.[12]

The second camp contained those ISPs who performed trials of or deployed third-party DPI-based behavioral advertising systems.[13] Importantly, these ISPs generally did not inspect user data themselves, but passed it off to their partners for analysis. According to these ISPs, they were assured that measures were in place to ensure that those partners did not retain medical information, personal data, e-mails, or other types of especially sensitive data.[14] Also, all of these ISPs stated that they and Knobbed did not tie the tracked Internet data to personal customer data already known to the ISP (billing information, etc.).[15]

However, as a technical matter, the personal data embedded in a user's Internet communications was handed off to the ISP's partners, when the ISP itself is actually responsible for safeguarding its users data. In some cases, the identity of the partner was not divulged to the user. These partners had no direct interactions with the user, meaning that final control of what data was used and how rested not with the user or even the ISP, but with this third party. To return to the postal service analogy, it is as if the ISPs photocopied users' letters and handed these copies to third parties, who agreed to only write down which commercial products were mentioned in the letters, and not anything else that someone might consider sensitive. However, the decision as to what, exactly, should be considered 'sensitive,' is not made by the user but rather, by this third-party company.

Customer notification and consent varied from ISP to ISP, but there were significant trends. ISPs generally posted modified terms of service and often updated the 'Frequently Asked Questions' section on their websites, but usually declined to directly contact users or call attention to the significance of the new service. Knology, for instance, updated their Customer Service Agreement on their website, which is presented to new users, but apparently made no other attempt to draw attention to the change.[16]

The level of detail in the disclosures also fell far short of the minimum that is necessary for customers to make an informed decision. For example, CenturyTel sent an e-mail informing users only that it had "updated its Privacy Policy con-

---

[11] All 33 response letters are available at the House Energy and Commerce Committee's Subcommittee on Telecommunications and the Internet website at *http://energycommerce.house.gov/Press_110/080108.ResponsesDataCollectionLetter.shtml.*

[12] *See, e.g.,* Response Letters of AT&T, Verizon, and Time-Warner.

[13] *See, e.g.,* Response Letters of WOW!, Charter Communications, Knology, and CenturyTel.

[14] *See* Response Letter of Charter Communications 2.

[15] *See* Response Letter of Knology 1.

[16] *See* Response Letter of Knology 2.

cerning Internet Access Services" and provided a web link to the updated policy.[17] The policy in question stated only:

> Online Advertising and Third-party Ad Servers.
> CenturyTel partners with a third party to deliver or facilitate delivery of advertisements to our users while they are surfing the Web. This delivery of advertisements may be facilitated by the serving of ad tags outside the publisher's existing HTML code. *These advertisements will be based on those users' anonymous surfing behavior while they are online.* This anonymous information will not include those users' names, e-mail addresses, telephone number, or any other personally identifiable information. By opting out, you will continue to receive advertisements as normal; except these advertisements will be less relevant and less useful to you. If you would like to opt out, click here or visit *http://www.nebuad.com/privacy/servicesPrivacy.php.*[18]

A later letter sent out by CenturyTel stated the following:

> CenturyTel continually looks for ways to improve your overall online experience. In that regard, we have enhanced our High-Speed Internet service by working with partners to provide targeted, online advertising for your convenience and benefit. Targeted, online advertising minimizes irrelevant or unwanted ads that clutter your web pages. If you do not wish to receive targeted, online advertisements, or if you would simply like more information about CenturyTel's use of online advertising, third-party ad servers and the measures you can take to protect your privacy, please review our Privacy Policy by visiting *http://www.centurytel.com/Pages/PrivacyPolicy/#adv.*[19]

No mention is made at all of providing actual user data (let alone *all* of a user's packets) to third parties. Only a single mention of ads being "based on those users' anonymous surfing behavior" is offered in the first notice, and the second presents the service only as enhanced, "targeted advertising for your convenience and benefit" without mention of the methods involved to deliver said advertisements. It's worth noting that these examples are not unique to CenturyTel or even unusual; rather, they are indicative of the level of detail provided in many ISP notices. Such notices do not make clear to the user what is actually being done with the data they send and receive over the Internet. *None* of the ISPs appears to have required that a user take any affirmative action at all before having their data handed wholesale to a third party. Inaction or failure to read the notice was simply treated as an 'opt-in'.

It is important to note that nearly every ISP that responded mentioned that they run their own websites, and use traditional tracking methods such as cookies to observe and record the behavior of their customers on their sites, much like Google, Yahoo, Microsoft, and many other web service providers do. Likewise, many ISPs also use what is called a "DNS redirect," which, rather than returning an error to a user's web browser when he or she types in an incorrect web address, redirects the user to another web page which may have related suggestions, advertisements, or other information.

These non-DPI practices have privacy implications that overlap with the ones being discussed today, but which are different in kind and scope. It is the difference between you writing down what I tell you on the phone and my phone company recording my conversation with you because unlike my phone company, you cannot record what I've said on my phone calls to other people. Nonetheless, the privacy practices of and personal information available to application providers raise their own serious questions of legal policy, and any regulatory regime we consider must be comprehensive and attempt to ensure the protection of Internet users against privacy invasions from all such sources.

V. Current Law

Independent analysis by the Center for Democracy and Technology suggests that although it is far from clear, despite ISP claims,[20] past experiments with DPI and behavioral advertising of the type engaged in by Knobbed may run afoul of existing law. Critically, however, some of the laws in question might not apply if the ISP

---

[17] Response Letter of CenturyTel 3. 18 *Id.* 3 (emphasis added).
[18] *Id.* 3.
[19] *Id.* 3–4.
[20] *See* Center for Democracy and Technology, *An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the Knobbed System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising,* (July 8, 2008), available at *http://www.cdt.org/privacy/20080708ISPtraffic.pdf* [hereinafter CDT Behavioral Advertising Overview].

engaged in this behavior internally, instead of delegating responsibility to a third party.[21] Thus, an ISP might legally be able to read and analyze all of its customers' communications as long as it does so itself—hardly an improvement in privacy.

It is extremely important to note that without apparent exception, every ISP that responded to Chairman Markey's letter concluded that both the tracking and opt-out mechanism were legal, or at the very least, were "not unlawful or impermissible."[22] One ISP even went so far as to claim that it "offered customers easy-to-use opt-out mechanisms *as recommended by the FTC.*"[23] However, even the "opt-out" method was questionable, as the act of opting out did not stop the delivery to and monitoring by the third-party partner but only the presentation of targeted ads and stored profiles.[24]

Yet to date, no enforcement actions have been taken against a practice that is of significant concern to citizens and lawmakers alike. Regardless of whether or not the actions taken by ISPs are technically legal, the existing legal regime is clearly not effective at preventing such privacy violations. And if ISPs believe they can legally and profitably engage in this behavior with only a minimal effort made to notify and protect users, they will continue to do so.

To the credit of the ISPs here today, several providers have made commitments to ensuring that there is transparency, affirmative consent, and ongoing control by customers. For example, Time-Warner's testimony suggests control, transparency, disclosure, and safeguarding personal information as principles on which to base a privacy framework. AT&T states that the company will not engage in behavioral advertising without affirmative, advance action by the consumer that is based on a clear explanation of how that information will be used. But while these are laudable principles and we applaud the carriers here today for their stated commitment to customer privacy, promises by individual ISPs are not enough and do not obviate the need for a comprehensive governmental policy.

Part of the reason for the current lack of enforcement can be traced to ambiguity in the FCC's authority to protect the privacy of Internet users, despite the FCC's time-honored role in protecting the privacy of communications as a whole. Congress has long recognized that providers of communications services occupy an especially sensitive position in society. As data conduits, communications services are uniquely positioned to track customers and collect information about their daily lives. The Communications Act, which created the FCC, contains provisions designed to protect the privacy of telephone and cable customers. But those same protections have yet to be unambiguously extended to Internet customers. As a result, customers cannot be confident that their sensitive information is protected from unwanted intrusion. In a society where Internet services are increasingly used to transmit personal and sensitive information, this is clearly problematic.

Section 222 of the Communications Act applies to the privacy of customer information collected by common carriers.[25] The statute recognizes that "individually identifiable consumer proprietary network information" is created by, and critical to the functioning of, telecommunications services.[26] However, the statute strictly limits the use of that information to applications that handle tasks like billing and the maintenance of network integrity.[27] Carriers are allowed to provide aggregate consumer information to third parties, but this information must have both "individual customer identities and characteristics" removed.[28] Viewed holistically, this section manifests a Congressional understanding that common carriers have access to sensitive personal information, and that common carriers have legitimate reasons to use that data. However, this understanding is balanced by strict prohibitions against any non-essential use or the disclosure of sensitive data.

---

[21] *See id.* at 6–9.

[22] Response Letter of CenturyTel 2–3 (Aug. 7, 2008). Cable One does describe their disclosures in their Acceptable Use Policies as "opt-in" because the user must check and acceptance box, but this does not qualify as either an affirmative step specific to monitoring or a meaningful opportunity to deny consent, because the alternative is no Internet service at all. *See* Response Letter of Cable One 3 (Aug. 8, 2008).

[23] Response Letter of Charter Communications 2 (Aug. 8, 2008) (emphasis added).

[24] Ryan Singel, *Congressmen Ask Charter to Freeze Web Profiling Plan,* Threat Level from Wired.com (May 16, 2008). *See also* Ryan Singel, *Can Charter Broadband Customers Really Opt-Out of Spying? Maybe Not,* Wired (May 16, 2008).

[25] 47 U.S.C. § 222.

[26] *See* 47 U.S.C. § 222(c)(1).

[27] *See* 47 U.S.C. § 222(d).

[28] *See* 47 U.S.C. § 222(c)(3), (h)(2).

Although many common carriers provide Internet services to consumers,[29] such Internet services are not covered under Section 222.[30] As a result, plain old telephone customers can be confident that sensitive information contained in their phone records will be kept confidential, but they cannot enjoy the same level of confidence when it comes to sensitive information that Verizon might compile using their DSL Internet activity.

Section 631 of the Communications Act also marks an attempt by Congress to protect the privacy of consumers, this time from cable system operators. Again, the statute recognizes the fact that operators will need to collect and use some personally identifiable information in order to operate their systems. However, these operators are required to obtain written permission from consumers in order to collect any personally identifiable information that is not crucial to the operation of the system.[31] Additionally, operators are required to obtain prior written or electronic consent before disclosing any personally identifiable information.[32] The statute does not impose these same protections on aggregate data that does not identify a particular customer,[33] and allows an operator to disclose names and addresses of subscribers as long as that information is not tied to use or transactional information.[34]

As with Section 222, Section 631 specifically protects sensitive information that network operators are uniquely positioned to collect. However, unlike Section 222, which applies to phone customers but not Internet service customers, Section 631 is written to apply to both cable television subscribers and cable Internet subscribers.[35]

Unfortunately, not all customers access the Internet by way of a cable system. In addition to unprotected DSL service, customers can access the Internet via a fiber optic network, a satellite based service, or by using one of many wireless Internet standards. Instead of relying on old categories that may protect some (but certainly not all) consumers, Congress must recognize that all Internet service providers share the same privileged position of access to their users' personal data. As a result, Congress should collectively protect customers with legislation that specifically addresses all Internet service providers, rather than legislation that effectively forces customers to access the Internet via a single, protected pathway.

The time has come for a comprehensive regulatory structure that will ensure that the privacy rights of all Internet users are protected, and one that, like the Telecommunications Act of 1996, "expands very important privacy protections to individuals in their relationships with these very large companies."[36]

VI. Fixing the Law

Given the power of the technology and the scope of possible uses, it is critical that we establish industry guidelines and legal protections for users. And while the use of personal data by application providers is not the focus of our discussion today, as discussed above, any solution should strive to be comprehensive in scope and ensure that the basic principles of privacy protection are applied across the entire Internet ecosystem. These protections should meet three major goals that parallel the privacy inquiries described above:

- They must ensure that the purpose of the use of customer data is one which can be consistent with consumers' privacy expectations.
- They must ensure that the amount and type of data collected is narrowly tailored to the proposed use, and that the data is not kept or disseminated to third parties past what is necessary to that use.
- They must ensure that customers have access to and actually receive adequate information about the proposed use, and have affirmatively and actively consented to any practices which could violate customers' expectations of privacy.[37]

---

[29] *See, e.g.,* Verizon, *http://www.verizon.com/*.

[30] *See National Cable & Telecommunications Assn.* v. *Brand X Internet Services,* 545 U.S. 967 (2005).

[31] *See* 47 U.S.C. § 551(b).

[32] *See* 47 U.S.C. § 551(c)(1).

[33] *See* 47 U.S.C. § 551(a)(2)(A).

[34] *See* 47 U.S.C. § 551(c)(2).

[35] *See* 47 U.S.C. § 551(a)(2)(C)(ii).

[36] Statement of Congressman Edward Markey, 142 Cong. Rec. H1145–06 (Feb. 1, 1996).

[37] The FCC has already presented us with an example of how Commission action and ISP disclosures can be used to help protect Internet users from privacy invasions and impermissible network management practices. In its order finding that Comcast's interference with customer traffic was not reasonable network management, the Commission ordered Comcast to fully disclose the details of its past and planned practices, including use of DPI. *See* Federal Commu-

Continued

In order to achieve these goals, the Committee should seek to pass legislation to encapsulate these requirements and to make it clear that the FCC has the power to enforce them. As the Commission observed in 1998, "The [Communications Act] recognizes that customers must be able to control information they view as sensitive and personal from use, disclosure, and access by carriers."[38] The Committee and Congress need only make it clear that Internet user privacy is another area of communications where the Commission is empowered to protect consumer privacy.

VII. Conclusion

I would like to thank the Committee again for giving me the opportunity to testify today. Public Knowledge is eager to work with the Committee to craft comprehensive privacy legislation that will protect Internet users. I look forward to your questions.

Senator DORGAN. Ms. Sohn, thank you for your testimony.

Why do we not start with where you concluded on deep packet inspection? I know that our colleagues in the House had sent questionnaires to Internet service providers and have received some responses. How extensive do you think is this tactic of deep packet inspection?

Ms. SOHN. Well, it was more extensive than it is now. Because of the scrutiny over on the House side and also over here, several of the ISPs that were using deep packet inspection have ceased using deep packet inspection. There was such an outcry. However, some are still using deep packet inspection.

And as I said before, a number of those—actually all of the providers that were using deep packet inspection who responded to the House said that they believed that they were fully acting within the law and that what they did to protect consumers was adequate. And speaking to some of the folks—I will let them speak for themselves—on my right, I know some of them are considering using DPI as well, albeit with the protections that they have outlined today.

Senator DORGAN. Is there a beneficial use of deep packet inspection, for example, attempting to determine who is out there that is providing viruses? So is deep packet inspection a process that in some cases can be beneficial?

Ms. SOHN. Absolutely. Public Knowledge has been saying in the 7 years of its existence, that you do not outlaw technology. You outlaw bad uses of technology, and DPI, as you stated, can be used for lawful and very beneficial purposes.

Senator DORGAN. But the testimony and knowledge we have, for example, of NebuAd and others says that the purpose of deep packet inspection is to track people's behavior in a wide range of areas and then profile and do targeted advertising to that profile, which is done, I assume, largely without the knowledge of the user, which is very troublesome.

Ms. Attwood, you indicated to me that the fact that the Senate and the House are beginning to evaluate these things was helpful to your company because these are relatively new issues and it

---

nications Commission, *Memorandum Opinion and Order* ¶54–56 (August 1, 2008), available at *http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC–08–183A1.pdf.* Given the authority, the Commission could make this type of disclosure an industry-wide baseline to ensure that customer's decisions about granting consent are based on good, complete information backed the force of law.

[38] Federal Communications Commission, *Common Carrier News Release* (Feb. 19, 1998), available at *http://www.fcc.gov/Bureaus/Common_Carrier/News_Releases/1998/nrcc8019.html* (clarifying permissible uses of Customer Proprietary Network Information).

really caused your company to be thinking what kind of policies do we employ, how do we go through this and develop policies internally. And I think that is commendable.

The question I think for the three providers here is what kind of information do you collect at this point. What kind of movements do you track and for what purpose?

Ms. ATTWOOD. Well, it is a great question. I guess I would elaborate. Here we are talking about behavioral advertising.

Senator DORGAN. Right.

Ms. ATTWOOD. And in that context, we are not engaged in that practice today. And we commend you and this Committee and the attention and the effort to look at the way in which collection of material has affected or prompted our consumers to identify what they are concerned about.

That allows us to actually look as we enter into these phases to say can we use privacy as a design element. Rather than as a regulatory requirement or as something after the fact that we have to look at, let us look and say our products and services—privacy will be by design. And that is what this dialogue allows us to do. It allows us to as an industry galvanize around how we can construct the right framework so that we can bring the benefits of both the advantages of an advertising-supported model, which is really an innovation in the Internet area, as well as the capabilities of protecting the privacy of our customers.

So we have millions of customers, and therefore we have lots of information that we use to improve the services and products of our customers. There is a lot of value that can be created and innovation that can be created in offering additional targeted advertising, as well as additional value propositions to the customer. We think that is something today that has proved itself, whether it is affinity cards or whether it is in some things that you already see. Those are areas where we are hopeful we can help innovate, as long as we consider privacy by design.

Senator DORGAN. As a consumer and an Internet user, I see the value of targeted advertising because if I am on the Internet wanting perhaps buy a pair of shoes and then I see targeted advertising coming at me advertising certain kinds of shoes, perhaps even that same brand, I understand that someone saw I was looking at shoes, and so they were trying to provide additional advertising about shoes. In many ways that is useful, perhaps in some cases annoying, but in many other cases useful.

But the other side of this is that an Internet service provider would have a substantial body of knowledge. Let us assume that my two colleagues, Senator Klobuchar and Senator Thune, are customers of the same provider. You would have a substantial amount of information about each of them, what they have done, what their travels have been on the Internet, where they have visited, and so on. And that could have enormous financial value to a company. And someone comes to your company and says, you know what? That information you are sitting on has great, great value. We will pay a lot of money for it. So that is where the advertising model on the Internet confronts the issue of privacy that is very, very important.

So I appreciate the testimony today. I think all three of you have said that your companies have had to sink their teeth into this question of how do you deal with the privacy issue. You have all talked, I think, about the opt-in strategy doing so in a manner that has a customer that is fully informed.

I have seen a number of opt-in strategies that I think, Mr. Tauke, you mentioned. People do not have the foggiest idea whether they have opted in or opted out. They have simply pushed the "OK" button with the cursor, and so there they are.

This is a really interesting set of issues. I did indicate that if somebody followed you into a mall with a clipboard and traced everything you not just bought or store you visited, but every single item you looked at, you have great angst about that. Who on earth is doing this? And yet, that potential exists. And so that is why we have to try to deal with this tension between constructive advertising models on the Internet and the right to privacy.

Senator Klobuchar is next.

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

Senator KLOBUCHAR. Thank you very much, Chairman Dorgan. Thank you for having this hearing. Thank you to our witnesses.

At the last hearing on this, I expressed my views that Americans have a love-hate relationship with advertising on the Internet. We want to see some of it, and then some of it we do not want.

I made the mistake, Mr. Chair, of using the example at the last hearing of how I liked to see ads pop up for deals on clothes, but I do not like it when my daughter who is 13 sees ads for American Girls. And as a result, I would just like the record to reflect, I got several letters from defenders of American Girl dolls. It was in the Los Angeles Times—my quote. And I just want the record to reflect that I have nothing against the American Girl dolls, including Kirsten, Molly, Kaya, and Kit Kittredge, which movie I just saw. So if you could just make that clear.

Senator DORGAN. Well, the permanent record will reflect——

[Laughter.]

Senator KLOBUCHAR. Thank you very much.

I actually just had some questions looking at your testimony and thinking about what we talked about last time. You know how when you have your credit record, you are able to go back and clear it up and see what information is on there. Do you think you should have the same ability to do that as a consumer with any information that might be on there on your shopping record or the information on you on the Internet? I do not know who wants to take that.

Ms. ATTWOOD. I am happy to address that. I think that is one of the issues that would be interesting to develop, the question of whether the customer not only can control the information that is collected, but also can identify and see what they look like online. And even more to your point—and I do not want letters either, although I do not think I would get them from American Girl.

Senator KLOBUCHAR. These were just consumers for American Girl, not the company.

Ms. ATTWOOD. Maybe ultimately down the line you would be able to have some flexibility in identifying what advertisements you want to see and what you do not want to see. So those could be age-specific. Those could be related to your household, a particular interest in your household.

So the concept of customer control, the concept of using the capabilities and enhancements of the technology to help customize that experience is something of an exciting prospect so long as we protect and really embrace the notion of privacy.

Senator KLOBUCHAR. Mr. Stern?

Mr. STERN. Thank you, Senator.

If I may just add, not only does customer consent allow the consumer to opt in, if they want to have online advertising be targeted, but they can also opt out. And that gives them a unique ability to do something that they cannot do with their credit report, which is to wipe the slate clean. And so we think that that is actually an important part of this, giving customers the ability to make a decision and later change their mind.

Senator KLOBUCHAR. Very good. And the technology is available to do that?

Mr. STERN. Yes, it is.

Senator KLOBUCHAR. If we were to put together some legislation at some point—and I know all three of you would rather have it be self-regulating, but if Federal privacy regulation is considered in Congress, what would you think the key would be to this potential legislation? What do you think should be in that? Are there any models you would look at like the European data privacy law, or what would you look at to do that? Mr. Tauke?

Mr. TAUKE. Well, Senator, first of all, you are right. At this juncture, we are not prepared to embrace legislation. We actually think that there are some models on the books already that could be useful. I mentioned in my testimony the advertising industry's model where the FTC is the enforcing agency.

One of the reasons why we are a little unsure about legislation at this juncture is because this technology is developing so rapidly, and there are different technologies that are being used to do different things. As I think all of us have alluded to in one way or another, the technology is not in and of itself bad. The technology can do terrific things in order to enhance online experiences. It is how it is handled and what the consumer role is.

So having said that, with legislation I believe the notion of meaningful consent and the consumer in charge of their online experience are the two key elements. Exactly how that translates into the technology of today and the technology and practices of tomorrow is a little uncertain yet. That is why I think if the industry could, in a sense, help establish some best practices ourselves, try to keep up to date with that stuff, get all the players involved, because the consumer does not care who is tracking—you know, it is the same impact no matter who is doing it—if we could do that and then that might inform the Committee too of what we are doing and where gaps may be and if you should step forward with some additional legislation.

Senator KLOBUCHAR. Do you think competition could push, though, some of your fellow competitors not to keep up with those regulations?

Mr. TAUKE. Competition works both ways on this issue, Senator. I mean, I think what we have found in our history on some of these issues is being on the side of the consumer and privacy is not a bad deal. We have had some fairly highly publicized lawsuits over the last few years trying to protect our consumers' privacy, and we think that benefited us in the marketplace.

When we have dealt with issues like—I remember a couple decades ago now, I guess, when we were dealing with caller ID. In other words, there were a lot of fits and starts with caller ID. Initially it was thought to be a great privacy protector because you could see who is calling you. Then, of course, there was concern that, oh, now the estranged husband knows something about who is calling the wife and various other things that happened. And so there was concern from a domestic violence perspective and so on. Then we had blocking that came into play and various other things happened with the technology.

So we evolved to the place today I think where most consumers really like the technology, the information it provides. They know how to protect themselves if they do not want their number following their call.

So I think it is the same thing here. We have to, over time, figure out how to do this the right way.

But I think it is in our company's interest to be on the side of privacy. I think that is a marketing advantage. I think that for the industry as a whole, it is essential that we get there. The worst thing for our industry is the consumers are afraid to use the Internet.

Senator KLOBUCHAR. And I would agree with you, especially from larger, mainstream companies that do not want to be tarred with having not protected privacy rights. But not all the companies in the game might care about that as much. And that is why I am looking at some rules that could maybe protect your own industry if you had some rules that you already believe are in your best interest that could protect the consumers from other companies which might not share your interests in protecting privacy as a marketing and as a good thing to do as a company.

Ms. ATTWOOD. Yes. I would like to underscore that because not all folks in this space have consumers that they answer to. We fully agree with Verizon's position about this being a marketing advantage. AT&T views that absolutely as a great opportunity here. But right now there is behavioral targeting in the online environment, and it is by web actors who do not have direct customers to answer to.

The beauty of an advertising-supported model is that it is free. The disadvantage is that your customer is your advertising industry. It is not retail. It is not our customers. So while I think that there is a direct advantage that we have to our customers, I think we would, at AT&T, say another key element to any legislative proposal would be that it apply to all actors because that is really the only way. I mean, we talk a lot about from a competitive point of view, and clearly that is of interest to AT&T.

But I would say from a customer confusion question, without really addressing this issue holistically, when the customer turns on the computer and goes to a web page and on that web page there is advertising and on that advertising, that customer has indicated to AT&T that they do not want to be tracked, I cannot do anything to protect that customer from being tracked by other entities that are, in fact, appearing in that advertising space.

So until we address this holistically, even efforts from companies such as ours suggesting that there ought to be control and ought to be affirmative selection by the customer cannot be implemented fully, and the customer can be confused.

Senator KLOBUCHAR. Thank you.

Senator DORGAN. We had other companies testifying at the first hearing, and at that point we did not have the Internet service providers, which is why we wanted to have Internet service providers at this hearing. I understand the point you are making.

Senator Thune?

STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA

Senator THUNE. Thank you, Mr. Chairman.

And that was an interesting hearing, and this is an issue that is getting a lot of attention, as you would expect. And I do not think there is any question that online advertising is the fuel for this economic engine that is really driving the world right now. It has resulted in substantial access to free content for people on the worldwide Web.

But I do want to pick up on the previous discussion here because I think, Mr. Tauke, you had mentioned in your remarks that the industry is working to develop self-regulating privacy standards for online advertising. And to get back to Ms. Attwood's point, one entity cannot do this. There has got to be some sort of an agreement, I think, within the industry.

So I guess my question is, what is the time line for those standards? Who is participating in developing those standards? What are those standards going to look like? And will you keep us updated as you progress down that road?

Mr. TAUKE. First, we have signed some nondisclosure agreements with some other companies that would not permit me to today publicly disclose who all the players are. But I think it is fair to say that there are ISPs, there are representatives of other online types of activities. So I think we are seeing people from all parts of the online sector, the search engines, the browsers, and so on, who are interested in participating in this kind of thing.

We also have talked to and engaged with some in the advertising industry who also have an interest.

I cannot tell you we will get there, but I am encouraged by the progress so far. And I think it is feasible that in over a matter of a few months we would be able to get a pretty strong group of players in the industry to move forward with best practices.

Then the question becomes how do you enforce those. First, there is a lot to be said for shining the light of day on a lot of practices, and if industry is focused on doing that, it is able to do that, and force change. That happened with this Committee. This Committee

held a hearing, and as the witnesses have pointed out, people stopped their behavior because the light of day was shined upon it. That is what an industry group can do.

Second, as we have alluded to earlier, the Federal Trade Commission also has jurisdiction in this area, has indicated it intends to assert jurisdiction, and if informed by good industry practices and standards, then I think the FTC would have greater ability to act appropriately.

Senator THUNE. Do you have a time line for when all this might——

Mr. TAUKE. What I would like to say to you is it will all happen in 2 months. I do not know that I can say that. I think this is a process. You are familiar with that, of course, in the Senate. It is a process. I think we have made good progress. I think as you have heard this morning, several companies are endorsing very similar principles here. So I think that there is a consensus developing. And I hope by the end of the year, certainly by the time you come back, that we can report back to you and give you progress on where we are. I think we will have something fairly good to say.

Senator THUNE. That would be really helpful because I think that that is a preferable solution to having us try and legislate something in this area. But it has to be at least, I think, somewhat comprehensive in terms of the scope of those from industry who are participating in order to make it effective. So I would encourage you as you continue down that track.

And I would direct this, I guess, to any of our panelists. But you talk about sensitive information deserving a greater degree of protection than regular online uses. And I guess the question would be, what is considered sensitive personal information? Is that a health record? Is that a credit card history, e-mails? What qualifies in your judgment in that category of sensitive information?

Mr. STERN. Senator, all of those could count as sensitive information. Certainly medical information is sensitive. And we believe that this opt-in framework ensures that we will protect those forms of sensitive information.

We also think that there are certain types of information—and medical information may be one of those—that merits a dialogue between policymakers and participants in industry that would put even more stringent controls around certain types of information, including making it possibly entirely off limits for activities like targeted online advertising.

Ms. SOHN. I think it is critical that it is the Internet user who makes that choice as to what is sensitive. Right now with deep packet inspection, sometimes it is a third party or the NebuAd that is deciding what is sensitive and not. As you point out, there is not a commonly understood definition of what sensitive is. So that is, to me, a critical part of putting control back in the Internet users' hands. They decide what is sensitive as opposed to a third party with whom they are not even contracting.

Mr. TAUKE. Let me just say first this is a tough area. It is hard to define exactly what the sensitive information is and precisely how you handle it.

So, for example, we all agree, I think, that medical records would be sensitive information. Yet, I get my prescriptions online. I do not

know about the rest of you. And I want my online pharmacist to keep track of what I have. I am happy when they send me a notice saying, you know, it is time to renew your prescription. If I would get another prescription that interacted inappropriately with what I have today, I would hope that they would notify me and tell me that. So that means we are asking them, on the one hand, to keep track of some of these things. On the other hand, this is certainly information that most of us would say should not be tracked.

So there are some fine lines here to draw. It is tough, but I think that this is part of what we hope we can make progress on in an industry process.

Ms. ATTWOOD. I would also underscore what Gigi said, which is absolutely creating tools to enable our users to be able to individually assess what is sensitive will be a critical thing, again, another potentially wonderful advance that we could use the technology to actually empower the customer to orient themselves around what is sensitive.

The last thing that the provider wants to do is make that judgment. I can tell you whether Government makes it or the user makes it, the last thing that we want to do is try to make some judgment as to what is important to our customers when it comes to sensitive information.

Senator THUNE. Mr. Chairman, I have one more question. My time is expired.

Senator DORGAN. Why don't you proceed?

Senator THUNE. OK. I would like to have you describe—Mr. Stern, you mentioned the difference between relevant online advertising and targeted online advertising. Could you elaborate on the difference between those two, and from your perspective, are those different types of targeted online advertising that are more problematic for consumer privacy?

Mr. STERN. Ads can be relevant for a number of reasons, Senator. For example, when customers come to a Website and they go to the sports page of that Website and then they see advertisements for team memorabilia, that context was used in order to make the ad relevant. However, if the relevance is based on the customer's behavior on other unrelated Websites, then we would consider that targeted online advertising, the type of advertising that should be governed under the four principles that we talked about earlier, informed consent, plus safeguarding consumer privacy, and value.

Senator THUNE. Thanks, Mr. Chairman. Thank you all very much for your testimony.

Senator DORGAN. Senator Wicker?

STATEMENT OF HON. ROGER F. WICKER, U.S. SENATOR FROM MISSISSIPPI

Senator WICKER. Thank you, Chairman Dorgan, for having this follow up hearing.

You know, I was sitting here thinking John Thune came to the House of Representatives in 1996. I got here in 1994. We were talking about this thing called the worldwide Web. If we had a little time during the orientation, we could go to a room and surf the

worldwide Web. And to think how far this industry has come in 12 or 14 short years is just breathtaking.

I pay my bills. I check my balance. I make purchases. And it is the engine that is largely driving the international economy, and we want to be able to facilitate that for the economy and for job creation and for consumers' convenience.

So I appreciate the fact that there seems to be a feeling that the Congress should defer perhaps and see if these issues of privacy and behavioral advertising can be worked out among the participants rather than as a result of legislation.

I will begin with Mr. Tauke. Maybe within 2 months, we might have an agreement announced among the providers. How will they compare to the proposed behavioral advertising guidelines of the FTC?

Mr. TAUKE. I think all of the companies that are engaged in discussion on this issue are well aware of the FTC's principles. And of course, you never know the outcome of a discussion until it is completed. But I think what the FTC laid out has been very helpful and informative, and in turn, we would hope what the industry could come up with would also be helpful and informative to the FTC.

Senator WICKER. OK. Other panelists?

Mr. STERN. Senator, we think the principles that we have proposed are very similar to what was laid out by the FTC, but they actually go one step further in protecting consumer privacy. And that is that we are seeking affirmative customer consent for the use of any type of information for the purposes of targeted online advertising, not just personally identifiable information.

Senator WICKER. And would you explain what you mean by that to a layman?

Mr. STERN. Absolutely. When you held your testimony in July and met with NebuAd, they talked about the ability that they had with their technology to anonymize the data that they received so that they would track the customer's behavior, but it could not be attributed to any individual. It would be used to deliver relevant ads to that individual while they browsed, but they could not tie it back to a person. They could not tell that that browsing behavior was your browsing behavior, although they could change your browsing experience based on the information.

What we are proposing is that we would not even do what NebuAd talked about, absent affirmative customer consent. In other words, we would not use your information whether or not we could attribute it to you personally to deliver targeted online advertising to you.

Senator WICKER. I see.

Other members of the panel?

Ms. ATTWOOD. Well, I would just say I think that the FTC process has greatly informed our industry discussions. They were able to, along with great work that has been done in the privacy consumer community by Ms. Sohn's group, by CDT, others that have helped shed light on the issue, helped identify the practices that are most concerning to consumers, and have through the imprimatur of the FTC and its process created importance, as has this Committee, creating the incentive for the industry to come together

to talk, to make sure that we understand how we can, in fact, achieve ultimately a greater sense of privacy assurance for consumers so that they use our services and use the Internet even more. I think that there is no question that the FTC process has been quite involved in the development of that.

Ms. SOHN. Can I be the skunk at the self-regulatory party? Because——

Senator WICKER. That would be a lot of fun.

Ms. SOHN. I want to make two points.

Number one is to address something that Senator Klobuchar said about competition. The problem is that, at least in broadband, there is not that much competition. This is something my organization has talked about for a long, long time. And a lot of the ISPs that were using deep packet inspection and NebuAd were not subject to great competition. A lot of them were rural ISPs. So the notion that there is going to be this competitive pressure, I'm dubious.

The second thing—and this is the point that I discussed in my oral testimony but discuss in more detail in my written testimony—is that the Communications Act already does cover some ISPs. There is a lot of talk about a level playing field, but right now cable Internet services are covered by stricter privacy regulation than broadband telephone information ISP services. So there is already in the law gaps where Mr. Tauke's company is being treated differently than a Comcast. So I do think that at a minimum you need to amend the Communications Act to fix those gaps because right now you do not have a level playing field between broadband ISPs.

Senator WICKER. Response?

Mr. TAUKE. Part of that highlights the point. Yes, there are all kinds of rules that apply to all different companies differently. If you guys could take on the Communications Act and level the playing field, most of us would applaud heartily. But rewriting that act—it has been a long process and it is very hard to get anything to fruition when you take on that major a task.

So we are not saying that we are opposed to the Committee addressing the issue, but what you are doing here, having a hearing, forcing industry to address the issue is helpful. We have the FTC that has some authority already. We have an industry that I think wants to get its act together. It is in our own interest to clean up the act. Right? So I think that can help.

If all that should happen, if the Senate—God bless you if you go forward and do your thing. That is terrific. But in the meanwhile, I think there is a need for this other activity to go on. That will inform what you do. It may turn out this is not such a big issue, or it may turn out there are other problems that arise as this goes on. But we ought to go forward with the self-regulatory approach, try to use what is there, and that will help inform you, I think, what the challenges are and where we may need additional legislation.

Senator WICKER. Thank you.

Senator DORGAN. Senator Wicker, thank you.

This issue of self-regulation—I think the process that is ongoing is very valuable. But in the ultimate, self-regulation works if there

is, number one, adequate criteria established, and number two, if it is enforceable. And one of my concerns is that what is happening now and what will happen in the future with respect to Internet advertising is various entities, content providers, Internet service providers, and others, have information that is going to become increasingly valuable, and it is tempting product to sell to someone who would like to purchase it. And so the question is under what conditions does that happen.

I want to come back to this question. Mr. Stern, you talked about when NebuAd appeared before this Committee and the anonymizing of information. It seems to me, however, that if NebuAd gathers all of this information and develops the strategies for targeted advertising and profiling, that if they are able to deliver that advertisement back to the Internet address, it is really not anonymous, is it?

Mr. STERN. Senator, there is a separation between the information that NebuAd has, which is a profile attached to an anonymous identifier, and the information that the ISP has, which is the connection between that anonymous identifier and the individual. As a consequence, there is—and I am not an expert on NebuAd's technology, given that we have not engaged in targeted online advertising and we have not done any sort of a deal with NebuAd or anyone like that—but there is, in fact, a set of technologies that are used in that approach to protect the customer's identity and anonymity.

Senator DORGAN. But there has to be a string somewhere from the information gathered and then ultimately delivered to the Internet address of the person whose tendencies on the Internet have been profiled. I mean, this reminds me of the discussion I sat in last night for 2 hours on the financial rescue issue, the discussion about firewalls that exist. It turns out the firewalls were not so fireproof.

Mr. STERN. That is correct, Senator. There is no perfect technology here.

But the principles that we have outlined ensure that targeted online advertising would only take place if consumers affirmatively consent after being informed of how their information will be used. As a consequence, we think that the harm that you have raised is one that customers will be able to evaluate and weigh against the benefits that they will enjoy by being able to see more relevant ads.

Senator DORGAN. It is interesting. I was just looking at a report that was released this morning. The information was provided me last evening of what was to be released this morning. It is a poll released today by Consumer Reports' National Research Center, and it has a lot of interesting information in it. There is a lot of misinformation out there and a great deal of lack of information.

Consumers are aware that information about their surfing habits, that is, movements on the Web, is being collected online. And here is what they believe.

Sixty-one percent of consumers are confident that what they do online is private and not shared without their permission. That is what people now believe.

Fifty-seven percent believe that companies must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations.

Forty-eight percent believe that their consent is now required for companies to use personal information they collect from online activities.

Forty-three percent believe a court order is now required to monitor activities online.

I only describe that to you because this is just released this morning. What it does show is while people, I think almost all of us would understand, are very concerned about privacy, they have very little understanding about what exists or what might not exist to create fences or gates or protections for their online privacy.

I think that the work that our colleagues in the House have done with their data gathering and hearings, the work that we have done, and the work that the FTC is now doing and the efforts by people in your industry to come together and develop approaches—again, I think in many ways these hearings kind of provoke and require people to be thinking what are we doing and how does it relate to what our responsibilities are and what the law is. I think all of this is constructive for us, as we move down the road here, to understand what is necessary. Is this something that can be self-regulated with enforcement capabilities, or will there need to be, both at the FTC and also will there need to be here in the Congress, some legislative guidelines developed that will inform us as we move forward.

I do not think any of us fully know the answer to that, but we are now learning a great deal more than we knew, which I think is progress.

I want to thank the three Internet service providers for making themselves available for this hearing. Your testimony, I think, is instructive for us.

Ms. Sohn, the title of your organization is Public Knowledge, which is pretty all-encompassing I was thinking, as I read that last evening. So we thank you for providing public knowledge about these issues from your perspective, which I think is also very valuable to this Committee.

This hearing is adjourned.

[Whereupon, at 11:10 a.m., the hearing was adjourned.]

A P P E N D I X

Prepared Statement of Hon. Daniel K. Inouye, U.S. Senator from Hawaii

For the American people, privacy is a treasured right, but it is also a right under regular attack. In this digital age, commercial forces can amass treasure troves of data about each and every one of us. This is especially true when it comes to where we go and what we do on the Internet.

Today we focus on the on-ramps to the Internet, and explore in greater depth the consumer privacy policies of our Nation's largest broadband providers. We will consider the abilities these providers have to view our online behavior and discuss what notice they should provide to consumers when they seek to do so. Further, we must examine whether our communications laws governing consumer privacy have kept up with rapidly changing technology or require adjustment.

I look forward to hearing from our witnesses.