WHAT YOUR BROADBAND PROVIDER KNOWS ABOUT YOUR WEB USE: DEEP PACKET INSPECTION AND COMMUNICATIONS LAWS AND POLICIES

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

JULY 17, 2008

Serial No. 110–137

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

58–071 PDF WASHINGTON : 2008

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

COMMITTEE ON ENERGY AND COMMERCE

JOHN D. DINGELL, Michigan, *Chairman*

HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
Vice Chairman
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
DARLENE HOOLEY, Oregon
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
JOHN BARROW, Georgia
DORIS O. MATSUI, California

JOE BARTON, Texas
Ranking Member
RALPH M. HALL, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING,
Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

PROFESSIONAL STAFF

DENNIS B. FITZGIBBONS, *Chief of Staff*
GREGG A. ROTHSCHILD, *Chief Counsel*
SHARON E. DAVIS, *Chief Clerk*
DAVID L. CAVICKE, *Minority Staff Director*

SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

EDWARD J. MARKEY, Massachusetts, *Chairman*

MIKE DOYLE, Pennsylvania
Vice Chairman
JANE HARMAN, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
BARON P. HILL, Indiana
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
GENE GREEN, Texas
LOIS CAPPS, California
HILDA L. SOLIS, California
JOHN D. DINGELL, Michigan (ex officio)

CLIFF STEARNS, Florida
Ranking Member
FRED UPTON, Michigan
NATHAN DEAL, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSELLA, New York
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
JOE BARTON, Texas (ex officio)

CONTENTS

WHAT YOUR BROADBAND PROVIDER KNOWS ABOUT YOUR WEB USE: DEEP PACKET INSPECTION AND COMMUNICATIONS LAWS AND POLICIES

THURSDAY, JULY 17, 2008

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TELECOMMUNICATIONS
AND THE INTERNET,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 9:40 a.m., in room 2123 of the Rayburn House Office Building, Hon. Edward J. Markey (chairman) presiding.

Members present: Representatives Markey, Doyle, Gonzalez, Inslee, Eshoo, Stupak, Green, Solis, Stearns, Radanovich, and Walden.

Staff present: Amy Levine, Mark Seifert, Tim Powderly, David Vogel, Philip Murphy, Neil Fried, and Garrett Golding.

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

Mr. MARKEY. Good morning, and welcome to the Subcommittee on Telecommunications and the Internet and our hearing on deep packet inspection technology and consumer privacy and issues that are related to it.

Privacy is a cornerstone of freedom. Without question, the digital era in communications technologies will heighten concern about the sensitivity of personal information that can be collected or disclosed about individual citizens and the ever-increasing pervasiveness of such data collection. Obviously this is happening across our society, from video cameras at crosswalks and federal buildings, checkout scanners in supermarkets to the collection of information by national security entities and the gleaning of information from a consumer's Web use. I have long fought for privacy provisions to be added to our Nation's communications statutes to keep pace with changes in technology and markets. I successfully offered amendments that became law in previous Congresses to protect children's online privacy, to extend the privacy provisions of the Cable Act to direct broadcast satellite television providers, to add privacy protections for wireless location information and to strengthen telemarketing privacy protections. In previous Congresses, I also offered legislative proposals to establish a privacy bill of rights for Internet users that would have covered Web sites like Google,

eBay, Amazon, and others, as well as separate legislation that required search engine sites to destroy data collected from users that was no longer needed for any legitimate purpose, and so I obviously have long supported the idea of legislating where needed and to do so in a way that strengthened and harmonized our Nation's communications privacy laws. In this subcommittee, we have direct jurisdiction over the Federal Communications Commission and providers of telecommunications capabilities and services. As such, providers of broadband access to the Internet fall squarely into our oversight role.

Today we look at how so-called deep packet inspection technologies affect consumer privacy and related issues following up on letters that ranking Republican Joe Barton, Chairman John Dingell, and I have recently sent raising questions about these technologies. There are a couple of notable differences between the data-gathering that individual Web sites can and do conduct and that posed by the deployment of deep packet inspection technologies in broadband networks. First, there is a distinction in the detail, the type and the amount of data collected. As opposed to individual Web sites that know certain information about visitors to its Web sites and affiliates, deep packet inspection technologies can indicate every Web site a user visits and much more about a person's Web use. Second, there is already an array of laws on the books that arguably address a broadband provider's treatment of these technologies and services, including the Cable Act, the Electronic Communications Privacy Act, and the Communications Act, among other laws.

From a privacy perspective, given the sheer sophistication of the technology capability and the obvious sensitivity of the personal information that can be gleaned from a consumer's Web use, I believe broadband providers deploying deep packet inspection technologies must adopt clear privacy policies. In my view, consumers deserve, at the least, at the minimum, one, clear, conspicuous and constructive notice about what broadband providers' use of deep packet inspection will be; two, meaningful opt-in consents for such use; and three, no monitoring or data interception of those consumers who do not grant consent for such use.

Deep packet inspection technologies can be deployed not only with the intent to serve targeted advertisements tailored to a user's Web habits, they can also be utilized to manage traffic on the network, detect network threats, and discover the presence of copyrighted or illegal material and other applications. As a result, these technologies raise not only significant privacy concerns, but also highlight broader policy questions, including how they impact the evolution of the Internet itself and its future prospects for driving innovation and fostering competition and job creation. Today's hearing will allow the subcommittee to better understand the implications of deep packet inspection technologies on consumers, broadband providers, and the broader Internet.

We welcome our witnesses to the subcommittee. We thank them for their willingness to be here today.

Mr. MARKEY. Now I turn and recognize the ranking member of the Subcommittee on Telecommunications and the Internet, the gentleman from Florida, Mr. Stearns.

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

Mr. STEARNS. Good morning, and thank you, Mr. Chairman. The use of consumer Internet information for marketing purposes is not a new issue to all of us. Both the Energy and Commerce Committee and, of course, this subcommittee have previously held hearings to examine a multitude of concerns under the broad banners of online privacy and marketing, including the online collection of personally identifiable information and the use of cookies and other tracking tools.

My colleagues, our goal today should be to broadly examine how companies are using consumer Internet behavior to tailor online advertising; both the benefit to consumers, as well as any potential concerns that have not already been addressed by industry. Why then are we just focusing on broadband providers? Why are we not talking about search engines and Internet advertising networks as well? Wouldn't we have the same concerns with those folks?

Broadband providers are considering limited trials of tailored Internet advertising, but companies such as Google and Yahoo and Microsoft all have search engines, have long used tailored Internet advertising. Certainly we cannot have this discussion without addressing them as well. Whatever the appropriate standards are, I think everybody agrees they should apply to everyone.

We can all agree that consumers should be notified, but one of the questions is whether we should require explicit consent through opt-in procedures or whether opt-out procedures are sufficient. That is the core question. Whatever we decide, we need to be consistent. Consumers don't care if you are a search engine or a broadband provider. They want to ensure you are not violating their privacy either way.

I am particularly interested in learning from the witnesses the ways in which the use of behavioral information for marketing has been shown to have already harmed the consumers. It is imperative that there be some evidence of harm if we are going to regulate this practice or we run the risk of prematurely restricting the latest technological advancements that are related to online marketing.

As the overall economy continues to take a significant downturn, the government should not be contemplating how to make it harder for small businesses to succeed. Targeted advertising may be essential for small businesses to compete with larger ones. They don't have the budget of General Motors or Ford. Small businesses don't have hundreds of millions of dollars to spend on this advertising. So being able to target their ads on the Internet to consumers most likely to use their products gives them a better chance to succeed.

Overreaching privacy regulation at this time could possibly do more damage to this fragile economy. Companies should be as transparent as possible about what information they collect and how they are using it. That way, consumers will be empowered with better information to make obviously better decisions.

The Federal Trade Commission began inquiring into targeted online advertising practices with workshops. This effort culminated with it publishing proposed industry self-regulatory principles. Those principles were designed to ensure that companies that en-

gage in behavioral targeting voluntarily adopt best practices that provide increased transparency and choice to consumers about these practices. This approach seemed to be working. In fact, the FTC testified in a Senate Commerce Committee hearing just last week that it continues to believe we have not reached the point where legislation to address online behavioral targeting is immediately necessary.

I have a long track record of talking very seriously about this committee's mandate to consider online privacy and marketing issues, which was evidenced by the many hearings I helped organize in my former role as chairman and ranking member of the Subcommittee on Commerce, Trade, and Consumer Protection. I look forward to working with the chairman and continuing that work on privacy issues as a member and ranking member of this subcommittee. I think the hearing is important. I look forward to its results.

As we examine these issues today, I hope this panel can keep in mind that premature regulation of such practices, particularly in the absence of evidence of consumer harm, could have a significant negative economic impact at a time that many businesses, and particularly small businesses, are struggling, so I will look very closely at these issues before we leap to legislative proposals that even the FTC is not calling for at this time.

And with that, Mr. Chairman, thank you.

Mr. MARKEY. I thank the gentleman. The chair recognizes the gentleman from Michigan, Mr. Stupak. I apologize. I should have recognized the gentleman from Texas, Mr. Green, first. Excuse me.

OPENING STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. GREEN. Thank you, Mr. Chairman, for holding this hearing on the deep packet inspection technology, and I want to thank you and Chairman Dingell and Ranking Member Barton for your leadership and action on this issue over several months.

It is important we look at this issue in light of recent news regarding Embarq and Charter Communications. The potential for invasion of privacy posed by DPI technology if used in the wrong way is extremely troubling. There are necessary and legitimate uses for DPI, specifically for quality of service reasons, monitoring for worms or viruses, use by law enforcement and using it to monitor traffic to the extent necessary to maintain network integrity and prevent congestion in the last mile of the network. Use of DPI by a service provider network operator to protect network infrastructure and systems is one thing; using DPI to monitor Web users' patterns and habits by a third party to direct advertising or other content their way is a separate and troubling issue.

I am most concerned about the privacy implications of targeted advertising based on data collected on Internet users without their knowledge, and our subcommittee has a history of being concerned about it, whether a few years ago it was called a cookie or whatever. At the minimum, this should be something that a consumer is notified of and must opt into specifically outside of agreeing to some service terms and conditions, and I can't imagine most of my constituents agreeing to have their activities monitored. Some peo-

ple may want this kind of information directed toward them, but I and I imagine most of my folks, want to know if data being collected on us and should not have to opt out or install a cookie on our own Web site browser to prevent the collection of data. The idea that this would take place without the affected consumers or Web sites knowing it, without consumers having to specifically agree to have their information collected and analyzed for uses other than for the network operator to ensure quality service, is contemptible.

I am aware Google and Yahoo and others do similar targeting using other technology, and I believe this should be looked into as well, but primary jurisdiction for that falls under another subcommittee. To the extent we can address privacy issues under this subcommittee's jurisdiction, I believe we can and should.

Again, Mr. Chairman, I want to thank you for the hearing today on deep packet inspection, and I look forward to hearing more about the various uses and impacts it has both in improved network performance but also the potential privacy implications. Thank you.

Mr. MARKEY. The gentleman's time has expired. The chair recognizes the gentleman from Michigan, Mr. Stupak.

OPENING STATEMENT OF HON. BART STUPAK, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. STUPAK. Thank you, Mr. Chairman, and thank you for holding this hearing on deep packet inspection technology. It is important that we discuss the policy implications of this newest advancement in network technology.

Applications of DPI technology provide a number of benefits. Internet users are protected from the latest viruses through better filtering security, network administrators have more efficient means of managing traffic, and law enforcement can use these powerful tools to combat cybercrime. However, while we stand to gain from DPI technology, we need to ensure the protections Congress has put in place on behalf of a consumer's personal information are upheld. One of our witnesses today, NebuAd, offers targeted and behavioral advertising services by taking information from the network to create detailed profiles of the Internet service provider subscribers. While NebuAd has stated that the information they collect is completely anonymous, there are legitimate consumer privacy questions. The ISPs that partner with NebuAd should be offering consumers an option to opt in for having their data collected, not opt out. If the hardware of the network is configured to collect their data, they are only opting out of having their information sold while it continues to be collected. This is especially important to broadband subscribers with only one choice for an ISP. They do not have the option to choose a different ISP if they feel uncomfortable knowing that the network they are accessing tracks their every move. As broadband providers continue to integrate this technology, will future application of DPI technology be as transparent to the public?

Mr. Chairman, thank you again for holding today's hearing. I look forward to hearing from our witnesses about the application

of DPI technology and its implications, good and bad, for the future of the Internet.

Mr. MARKEY. The gentleman's time has expired. The chair recognizes the gentleman from Pennsylvania, Mr. Doyle.

Mr. DOYLE. Thank you. Mr. Chairman. I am going to waive an opening statement and just add it on to my questions.

Mr. MARKEY. The gentleman from Pennsylvania will have that time added to his question period, and seeing no other members here to make opening statements, we will turn to our panel, and we will recognize our first witness, Alissa Cooper, who is the chief computer scientist for the Center for Democracy and Technology. Her work focuses on the intersection of computer and networking technologies with consumer privacy. We welcome you, Ms. Cooper. Whenever you are ready, please begin.

STATEMENT OF ALISSA COOPER, CHIEF COMPUTER SCIENTIST, CENTER FOR DEMOCRACY AND TECHNOLOGY

Ms. COOPER. Chairman Markey and members of the subcommittee, on behalf of the Center for Democracy and Technology, I thank you for the opportunity to testify today. CDT is a nonprofit public policy organization dedicated to keeping the Internet open, innovative and free. The legal and policy implications of the technique known as deep packet inspection are of great importance to us.

The Internet was built on the principle that data could travel from one end of the network to the other, largely without interference along the way. Likewise, privacy laws in this country were crafted to protect our communications, whether they be phone calls, e-mails, or Web site visits, from being intercepted in transit. The confluence of technology and policy in this respect was no accident, and it has resulted in the emergence of the Internet that we know and love today, a trusted platform that supports astounding levels of economic activity and individual expression. Deep packet inspection, or DPI, could be used in ways that upend this paradigm by giving network operators the ability to intercept and analyze the Internet communications of their subscribers. While some uses of DPI technology are benign and even beneficial, others raise serious questions about the future of privacy, innovation and openness online. Though all these issues are near and dear to CDT, today I will focus specifically on privacy.

The bottom line is this: Certain uses of DPI allow consumers' communications to be centralized, scrutinized, and monetized. Absent careful privacy safeguards, DPI systems run the risk of damaging the consumer confidence in the Internet that has allowed the medium to flourish. DPI has recently been put to a new use: the tracking of consumers' online activities for the purpose of showing them targeted ads. Traditionally, ad network companies have contracted with Web sites to collect data about consumers. In the new model, ad networks partner instead with Internet service providers and do their collection using DPI.

As it has been implemented thus far, this model poses unique risks to consumer privacy. CDT values advertising as potent fuel for Internet growth, and we all cherish the free content that it supports, but ad networks that use DPI may gain access to the bulk

of consumers' Web-browsing activities, including visits to political, religious, and government Web sites. While traditional ad networks may be large, few, if any, provide the opportunity to collect information as comprehensively as with DPI. Furthermore, most consumers would be quite surprised to find a middleman lurking between them and the Web sites they visit. The DPI model defies consumer expectations.

As several members of this subcommittee have rightly pointed out, the Cable Act prohibition against collecting or disclosing personally identifiable information without consent is relevant here. We believe that a view into most everything a person does on the Web constitutes personally identifiable information, PII, under the statute. So far, cable ISPs have not only failed to obtain consent, but also they have not even told their subscribers that their Internet communications will be captured and shared with a third party.

The Federal Wiretap Act is also applicable. The Wiretap Act prohibits the interception and disclosure of electronic communications without consent. Importantly, the Act applies regardless of whether communications are highly personal and sensitive or completely anonymous. Think of it this way: if an eavesdropper were listening in on your phone calls but didn't know your identity or record the calls, you would likely still feel that your privacy had been violated. The same logic applies to DPI systems.

Though consent is merely one of many critical factors in designing a DPI system, these laws raise the question: how should consent be obtained? Notice must be uncomplicated and unavoidable, and it should mention the third party if one is involved. Consent should be expressly provided, not assumed. If a consumer does not consent, her communication should not be intercepted, and consumers should have the opportunity to change their minds, revoking their consent at any time through an easy-to-find, simple-to-use process. DPI has not emerged in a vacuum but rather in a digital environment where more data is collected and retained for longer periods than ever before. Although our communications privacy laws apply to the model I have described today, our Nation still has no comprehensive consumer privacy law to protect personal data across the board.

Congress needs to take a broad look at both DPI and online privacy concerns at large. Among other recommendations, my written statement suggests that, one, the subcommittee should urge the Federal Trade Commission to address DPI in its proposed privacy guidelines and to exercise its full enforcement authority over online advertising, and two, the subcommittee should set a goal of enacting in the next year baseline consumer privacy legislation that would protect consumers from inappropriate collection and misuse of their information.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Cooper follows:]

Statement of Alissa Cooper
Chief Computer Scientist, Center for Democracy & Technology

Before the House Committee on Energy and Commerce,
Subcommittee on Telecommunications and the Internet

" What Your Broadband Provider Knows About Your Web Use:
Deep Packet Inspection and Communications Laws and Policies"

July 17, 2008

I. Summary

Chairman Markey and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today. We applaud the Subcommittee's leadership and foresight in examining the emerging policy and legal implications of the technique known as "deep packet inspection."

Preserving the Internet as a trusted open platform for speech and innovation, without gatekeepers or central control, has been a defining issue for CDT since its inception. The Internet was built around the "end-to-end" principle: the notion that applications are better left to be implemented at the Internet's endpoints rather than its core, leaving the network itself unfettered by any particular party's interests.[1] Pursuant to this end-to-end design, data has traditionally traversed the Internet without interference from intermediaries. Legislative and legal decisions protecting Internet service providers from intermediary liability (*i.e.*, liability for content that originates with users) have been founded on the principle that the network operator is not manipulating the content that passes through its network. For decades, adherence to the end-to-end principle has preserved the Internet as a trusted platform and has supported astounding levels of innovation, economic activity, and individual expression.

---

[1] J.H. Saltzer, D.P. Reed & D.D. Clark, *End-to-End Arguments in System Design*, 2 ACM Transactions on Computer Sys. 277 (1984).

In recent years, however, massive growth in data processing power has spurred the development of new "deep packet inspection" (DPI) equipment that potentially allows ISPs and other intermediaries to collect and analyze all of the Internet transmissions of millions of users simultaneously. The use of DPI technology, though still in somewhat limited deployment, raises serious questions about the future of trust, openness, and innovation online.[2]

The ultimate implications of DPI depend largely on both how it is implemented and the purposes for which it is used. DPI applications range from managing network congestion to detecting network threats to monetizing individual Internet data streams through targeted advertising. Some of these applications are likely unobjectionable, while others raise far-ranging policy and legal questions affecting everything from privacy and intellectual property rights to freedom of expression and Internet innovation. Although CDT views all of these as core Internet policy issues,[3] my testimony today will focus on the privacy implications of DPI, as nearly every context in which DPI may be used raises substantial privacy concerns.

---

[2] Packet inspection or data analysis that a user conducts on his or her own data stream is a different matter and does not raise the same questions. There are many reasons why a user may want to conduct such analysis, and the ability to do so empowers users to better understand their own Internet service plans. This testimony focuses exclusively on packet inspection and analysis by intermediaries at the middle of the network rather than at the endpoints.

[3] CDT has a long history of opposing government mandates that require ISPs to filter content at the middle of the network, which is certainly one potential use of DPI. *See, e.g.*, CDT, *Summary and Highlights of the Philadelphia District Court's Decision in* Center for Democracy & Technology v. Pappert *(Case No. 03-5051 (E.D. Pa. Sept. 10 2004)* (Sept. 15, 2004), http://www.cdt.org/speech/pennwebblock/20040915highlights.pdf. CDT has also been an active participant in policy debates surrounding Internet neutrality and network congestion management, both of which potentially implicate DPI as a tool that can be used to distinguish certain Internet data streams from others. We have called for focused Internet neutrality legislation that, if enacted, would likely have the effect of restricting certain uses of DPI that facilitate discrimination between Internet data streams. *See* CDT, PRESERVING THE ESSENTIAL INTERNET (2006), http://cdt.org/speech/20060620neutrality.pdf. More recently, we recommended to the Federal Communications Commission that ISPs' endeavors to manage congestion on their networks – which may include the use of DPI – be transparent, evenly applied to all services and applications, and consistent with core internetworking standards. *See* Comments of CDT, *In the Matter of Broadband Industry Practices*, WC Docket No. 07-52 (Feb. 13, 2008), http://cdt.org/speech/20080213_FCC_comments.pdf.

In part because of the Internet's history of decentralized control and unfettered communications, consumers are not accustomed to having their Internet transmissions intercepted or analyzed en route by an intermediary. Depending on how they are deployed, DPI systems can defy this expectation, threatening the basis for consumer trust online. Certain aspects of DPI are also at odds with well accepted "fair information practices," can be disruptive to Internet and Web functionality, and may run afoul of communications privacy laws.

Those who use DPI for the purpose of tracking consumers' online activities to serve targeted advertisements stress the anonymous and limited nature of the profiles they compile. However, the main focus of our privacy concern with this model as it exists today is not on the profiles themselves but rather on what is required to compile those profiles, namely the diversion or copying of substantially all of the Web traffic of all subscribers. The fact that as of now the advertising networks use only a small portion of what is captured and do not store other information does not diminish the intrusiveness of the initial data capture. We are concerned with the interception and analysis of data in transit for purposes having nothing to do with the delivery of that data or the security or integrity of the Internet service. Moreover, as the existing models are now configured, no one can opt-out of that diversion or copying of their Internet traffic; existing opt-outs merely discontinue the creation of behavioral profiles for use in delivering ads.

DPI systems should not be viewed in isolation. They are being deployed within the context of an online environment where more data is being collected – and retained for longer periods – than ever before. Yet our nation still has no basic consumer privacy law and existing sectoral privacy protections have been far outpaced by technological innovation.

Recently, the FTC has begun crafting self-regulatory principles for privacy protection in online advertising.[4] We applaud the FTC for taking this step, but the principles do not

[4] *See* FTC, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles* (Dec. 20, 2007), http://ftc.gov/os/2007/12/P859900stmt.pdf (proposal).

address DPI,[5] and online privacy concerns are not limited to online advertising. Although CDT generally supports self-regulation, it has proven to be insufficient in the online privacy context. For all of these reasons, Congress needs to take a comprehensive look not only at the current and emerging practices associated with DPI, but also at online privacy concerns at large. We recommend that Congress take the following steps:

- The Subcommittee should seek additional information directly from ISPs and their partners about how they are using DPI.

- The Subcommittee should set a goal of enacting in the next year a simple, flexible baseline consumer privacy law that would protect consumers from inappropriate collection and misuse of their personal information, both online and offline.

- The Committee should strongly urge the Federal Trade Commission to address DPI in its proposed guidelines and exercise its full enforcement authority over online advertising practices.

- Congress should examine and strengthen existing communications privacy laws to cover new services, technologies and business models with consistent rules.

II. Understanding Deep Packet Inspection

A. An Analogy to the Postal System

The easiest way to understand deep packet inspection is to consider an analogy to the postal mail system. In the postal system, letters travel through the system in envelopes, each of which is addressed to its appropriate recipient and contains the return address information of the sender. On the Internet, data is broken into "packets." This is true for

[5] *See* Center for Democracy & Technology et al., *Comments of the Center for Democracy & Technology, Consumer Action, and Privacy Activism In Regards to the FTC Staff Statement, "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles"* (Apr. 11, 2008), http://www.cdt.org/privacy/20080411bt_comments.pdf at 18.

all kinds of Internet communications: Web browsing, email, voice-over-IP (VoIP) phone calls, peer-to-peer (p2p) file transfers, online gaming and so on. A single packet consist of two parts: a "payload," which is the actual data inside the packet, like the letter inside an envelope; and a "header," which contains the routing information that directs the packet to its destination (or back to the sender in case of errors), like the address and return address on the outside of an envelope. For an Internet packet, the IP addresses of the recipient and sender, respectively, are equivalent to the address and return address on an envelope in the mail.

As postal employees and equipment move mail through the system, they inspect the addressing information on the outside of each envelope to determine the next step in directing the mail to its final destination. The same is true for the Internet – the devices in the middle of the network responsible for routing data (known as "routers") inspect packet headers to decide where each packet should go next. This is called "shallow packet inspection" because the analysis is limited to the header information that is automatically exposed (by necessity) to every router on the Internet. Just as the postal mail simply cannot be delivered without postal employees and equipment inspecting addresses, neither can Internet communications be delivered without routers inspecting packet headers. But this shallow sort of inspection does not reveal the actual content of the Web browsing session, email, or VoIP call that a particular packet may contain, just as looking at an address on an envelope reveals nothing about the content of the letter inside.

Deep packet inspection is the equivalent of postal employees opening envelopes and reading the letters inside. To do DPI, network devices examine the payload of a packet – the actual data the packet carries – in addition to the packet header. To inspect a packet deeply means to examine the contents of the Web browsing session, email, instant message, or whatever other data the packet contains. Unless the content of the packet is encrypted (as with most online purchases and bank transactions), the entirety of the packet can be analyzed with DPI.

One slight complexity of Internet packets is that a packet payload itself may contain some additional addressing information that is supplemental to the IP addresses available in the packet header. When sending an email, for example, the email address of the recipient appears in the packet payload, not in the packet header. Likewise for Web browsing, the name of the Web site that a user is trying to reach appears in the payload, not the header. These kinds of additional addressing information are sometimes referred to as "application headers" because they are specific to particular Internet applications (Web browsing, email, or VoIP, for example).

Although some may claim that examining such application headers does not constitute deep packet inspection,[6] CDT disagrees. Application headers have the potential to reveal much more about a communication than packet headers, and the task of determining where an application header stops and actual data content begins often necessitates the inspection of the data content itself. Therefore, we believe the line between shallow and deep inspection lies between the packet header and the packet payload, regardless of whether the payload contains these additional "application headers."

DPI may be done in real-time as the data is in transmission, or it may be done afterward if the data is retained. ISPs may house DPI equipment and conduct the packet inspection themselves, or they may allow a third party intermediary to attach equipment to collect and inspect the Internet transmissions of their subscribers.

B. Uses of Deep Packet Inspection

Deep packet inspection is a generic technique that can be used for a wide variety of purposes. Examples include:

- *Behavioral advertising* – As we discuss in great detail in Section IV, DPI is currently being used by advertising companies to analyze individuals' Web

[6] *See, e.g.*, Declan McCullagh, *Q&A with Charter VP: Your Web activity, logged and loaded*, C|Net, May 15, 2008, http://news.cnet.com/8301-13578_3-9945309-38.html.

browsing habits, create profiles of their interests and behaviors, and use those profiles to serve them targeted advertisements.

- *Detection of network attacks* – ISPs and other network operators can sometimes use DPI to detect network threats like spam and viruses, since these kinds of attacks may exhibit well known data "signatures" that ISPs can recognize by inspecting packet payloads.[7]

- *Network congestion management* – DPI can help ISPs manage the volume of data on their networks. For example, inspecting packets may allow an ISP to identify certain kinds of communications (p2p file transfers, for example) that it may decide to "throttle" or process more slowly at times when the network is congested.[8]

- *Service tiering* – An ISP that wants to charge different prices for the use of different Internet services – say Web browsing, online gaming, or VoIP – can use DPI to distinguish one service from another on the network and charge its customers accordingly.[9]

- *Detection of intellectual property* – Some ISPs and content identification companies have begun using DPI to attempt to identify copyrighted works as they flow across their networks for the purpose of enforcing intellectual property rights.[10]

---

[7] *See, e.g.*, Sandvine DPI-Based Policy Solutions, http://sandvine.com/general/getfile.asp?FILEID=17 at 6 (last visited July 14, 2008); Thomas Porter, *The Perils of Deep Packet Inspection*, SecurityFocus, Jan. 1, 2005, http://securityfocus.com/infocus/1817.

[8] *See, e.g.*, Nate Anderson, *New Filings Reveal Extent, Damage of Bell Canada Throttling*, Ars Technica, June 2, 2008, http://arstechnica.com/news.ars/post/20080602-new-filings-reveal-extent-damage-of-bell-canada-throttling.html.

[9] *See* Nate Anderson, *Deep Packet Inspection Meets 'Net Neutrality, CALEA*, Ars Technica, July 24, 2007, http://arstechnica.com/articles/culture/Deep-packet-inspection-meets-net-neutrality.ars.

[10] *See, e.g.*, Audible Magic CopySense Appliance, http://audiblemagic.com/products-services/copysense/ (last visited July 14, 2008); *see also* Rob Frieden, *Internet Packet Sniffing and Its Impact on the Network*

Like most other technologies, DPI is neutral – its benefits and risks to both consumers and the Internet at large vary widely depending upon the particular purpose for which it is used and how it is deployed on the network. Each possible use of DPI has its own unique policy and legal implications, and the ultimate analysis of whether the benefits of DPI outweigh its risks will turn on the context of a particular DPI application. However, we believe DPI in nearly every context raises substantial privacy concerns because it potentially allows for the content of consumers' Internet communications to be captured and analyzed.

III. The Privacy Risks of Deep Packet Inspection

In part because the Internet was developed around the end-to-end principle, consumers have come to expect that their Internet communications pass through the network without being snooped on the way. DPI dramatically alters this landscape by providing an ISP or its partners with the ability to inspect consumer communications en route. Thus, deploying a DPI system likely defies the expectations consumers have built up over time. Absent unmistakable notice, consumers simply do not expect their ISP or its partners to be looking into the content of their Internet communications.

Many companies at every level of the Internet value chain have worked to build trust in the medium to the point where millions of consumers feel comfortable engaging in a wide range of personal and commercial communications and transactions online. ISPs are a critical part of that chain of trust. If consumers find reasons to question what their ISPs are doing with their Internet data, they may become reluctant to use the Internet as openly and frequently as they do today. Unless it is carefully deployed, DPI runs the risk of damaging consumer confidence in the medium.

Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers, 18 Fordham Intell. Prop. Media & Ent. L.J. 633 (2008).

Certain characteristics of DPI also seriously challenge traditional notions of "fair information practices," a generally accepted set of principles for protecting privacy.[11] Consider the fair information principle of limiting data collection to what is necessary to complete the task at hand. How can this idea be squared with existing DPI equipment that has the capability to collect and analyze every single Internet packet for millions of Internet users at once?[12] Although DPI can be implemented with limits on the types of data collected, the trend is toward more data collection and processing power, not less.

Transparency is another core fair information principle that DPI would appear to challenge. DPI equipment vendors compete on how small of an impact they can have on overall network operations.[13] Vendors seek to ensure that DPI equipment, even as it processes masses of Internet data from millions of subscribers, will not slow down network operations and will in fact be as invisible as possible on the network. This means ISPs and others may be able to deploy DPI systems that have few noticeable effects on consumers. With DPI hidden from view, those doing the packet inspection may have little incentive to fully disclose their practices.

In many cases, DPI equipment will automatically collect personally identifiable information (PII), even if the ISP or its partners have no intentions of using such data. Consider a third-party vendor using a DPI system to analyze the Web browsing activities of an ISP's subscribers. Although the vendor may not care to know the home address of a subscriber, the DPI equipment surely collects PII when that subscriber conducts Web searches to obtain online driving directions from his or her own home address. Furthermore, DPI systems automatically collect IP addresses, which can sometimes be

---

[11] *See, e.g.*, Organisation for Economic Co-operation and Development, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (Sept. 23, 1980), http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[12] *See* Procera PacketLogic PL10000 Datasheet, http://www.proceranetworks.com/images/documents/ds-pl10000-05-21-08_4p_web.pdf (last visited July 14, 2008).

[13] *See, e.g.*, The Tolly Group, Procera PacketLogic 7600 Evaluation of Accuracy and Scalability of Network Traffic and Service Management System (May 2007), http://www.proceranetworks.com/images/documents/tolly207173procerapacketlogic7600may2007.pdf (highlighting the fact that the Procera DPI device "generates less than 1 millisecond of one-way average latency").

used to re-identify individuals when combined with other information. In this way, DPI tends to sweep in personal information even when such information is not sought by the party doing the packet inspection.

Similarly, sensitive information may be unintentionally collected in a DPI system. Personal health data, for example, is migrating online through an ever-expanding array of health information and search sites, online support groups, and personal health record sites. Although the operator of a DPI system may not care to store or analyze such information, a packet containing sensitive data must first be inspected to determine its contents before the DPI system operator can decide what to do with it. In short, DPI technology may look at all information, including sensitive information; what is then done with that information can vary widely and is unlikely to be directly observable by consumers.

For DPI to operate in a truly privacy-protective way, data collection and retention need to be limited and those limits should be tied to the original purposes for collecting the data. Consumers need to be informed about what data is being collected about their Internet activities, how the information will be used, whether the information will be shared with others, and what measures are being taken to ensure that any transfer of data remains secure. They should be presented with this information in a manner that supports informed choice concerning their information and that choice should honored persistently over time. Consumers must also have opportunities for legal redress for misuse of the data. As a recent D.C. District Court opinion established, data leakage and the concern for potential abuses of that data are recognizable harms standing alone, without any need to show misuse of the data.[14] Consumers do not need to become victims of identity theft to suffer from an invasion of privacy.

[14] *Am. Fed'n of Gov't Employees v. Hawley*, 543 F. Supp. 2d 44, 50–51 (D.D.C. 2008) (ruling, *inter alia*, that concerns about identity theft, embarrassment, inconvenience, and damage to financial suitability requirements after an apparent data breach constituted a recognizable "adverse effect" under the Privacy Act, 5 U.S.C. § 552a (citing *Kreiger v. Dep't of Justice*, 529 F. Supp. 2d 29, 53 (D.D.C. 2008)).

Although DPI in a generic sense raises the privacy concerns described above, the use of DPI for behavioral advertising has its own unique privacy implications. These are explored in the next section.

IV. The Emerging Use of Deep Packet Inspection for Behavioral Advertising

Behavioral advertising, which involves the collection and aggregation of consumers' Web browsing activities for the purpose of serving them targeted advertisements, has not traditionally made use of DPI. For nearly a decade, behavioral advertising has been undertaken by ad networks – companies that contract with Web sites to be able to collect data about the consumers who visit those sites. A traditional behavioral ad network builds up profiles of individual consumers by tracking their activities on sites participating in the network. Ad networks usually accomplish this tracking by placing a cookie with a unique identifier on a consumer's computer and tying the consumer's behavioral profile to that identifier. Consumers' profiles are later used to serve targeted ads to those consumers on other Web sites. If a consumer visits a series of sports Web sites and later visits a news site, for example, he or she may be shown an ad for golf clubs or baseball tickets on the news site.

Over the past year, a new kind of ad network that makes use of DPI for behavioral advertising has emerged. In this model, the ad network partners with an ISP to do its data collection, rather than with a network of participating Web sites. The ISP allows the ad network to conduct DPI on the individual Web browsing activities of each of the ISP's customers. This means that the ad network receives an individual's Web browsing stream directly from the ISP and analyzes the content of that packet stream in order to create a profile of the individual's online behaviors and interests. As customers of the ISP surf the Web and visit other Web sites, the ad network serves them ads targeted based on their behavioral profiles.

The use of DPI for behavioral advertising is one area that we believe requires close scrutiny from lawmakers. As it has been implemented thus far, the use of DPI for

behavioral advertising poses risks to consumer privacy, defies reasonable user expectations, can be disruptive to Internet and Web functionality, and may run afoul of communications privacy laws.

A. Privacy Implications of the Use of DPI for Behavioral Advertising

1. Privacy Implications of Behavioral Advertising at Large

Even when it does not involve DPI, behavioral advertising poses a growing risk to consumer privacy. Consumers are largely unaware of the practice and are thus ill equipped to take protective action. They have no expectation that their browsing information may be tracked and sold, and they are rarely provided sufficient information about the practices of advertisers or others in the advertising value chain to gauge the privacy risks and make meaningful decisions about whether and how their information may be used. In a recently released Harris Interactive/Alan F. Westin study, 59% of respondents said they were not comfortable with online companies using their browsing behavior to tailor ads and content to their interests even when they were told that such advertising supports free services.[15] A recent TRUSTe survey produced similar results.[16] It is highly unlikely that these respondents understood that this type of ad targeting is already taking place online every day.

In most cases, data collection for behavioral advertising operates on an opt-out basis. Opt-out mechanisms for online advertising are often buried in fine print, difficult to understand, hard to execute and technically inadequate. Only the most sophisticated and technically savvy consumers are likely to be able to successfully negotiate such opt-out

---

[15] Alan F. Westin, *How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings* (Mar. 2008).

[16] TRUSTe, "TRUSTe Report Reveals Consumer Awareness and Attitudes About Behavioral Targeting" (Mar. 28, 2008), http://marketwire.com/press-release/Truste-837437.html ("71 percent of online consumers are aware that their browsing information may be collected by a third party for advertising purposes . . .. 57 percent of respondents say they are not comfortable with advertisers using that browsing history to serve relevant ads, even when that information cannot be tied to their names or any other personal information.").

processes. Moreover, in most cases, opt-out mechanisms offered for behavioral advertising only opt the user out of receiving targeted ads, but do not opt the user out of data collection about his or her Internet usage.

There is also a risk that profiles for behavioral advertising may be used for purposes other than advertising. For example, ad networks that focus on "re-targeting" ads may already be using profiles to help marketers engage in differential pricing.[17] Behavioral profiles, particularly those that can be tied to an individual, may also be a tempting source of information in making decisions about credit, insurance, and employment. While the lack of transparency makes it almost impossible to know whether behavioral profiles are being used for other purposes, the lack of enforceable rules around the collection and use of most personal information leaves the door wide open for a myriad of secondary uses.

Finally, because the legal standards for government access to personal information held by third parties are extraordinarily low, these comprehensive consumer profiles are available to government officials by mere subpoena, without notice to the individual or an opportunity for the individual to object.[18]

2. Deep Packet Inspection Exacerbates and Introduces Its Own Privacy Concerns

The privacy implications of behavioral advertising at large are amplified when DPI is the data collection mechanism. Ad networks that partner with ISPs and use DPI may potentially gain access to substantially all of an individual's Web browsing data as it traverses the ISP's infrastructure, including traffic to all political, religious, and other non-commercial sites. While traditional ad networks may be large, few if any provide the opportunity to collect information about an individual's online activities as

[17] *See* Louise Story, *Online Pitches Made Just for You*, N.Y. TIMES, Mar. 6, 2008, http://nytimes.com/2008/03/06/business/media/06adco.html.

[18] *See* CDT, *Digital Search and Seizure: Updating Privacy Protections to Keep Pace with Technology* (Mar. 2006), http://cdt.org/publications/digital-search-and-seizure.pdf at 7-9; Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1135 (2002).

comprehensively as in the DPI model, particularly with respect to activities involving non-commercial content. And although these ad networks currently inspect predominantly Web traffic, ISPs carry emails, chats, file transfers and many other kinds of data that they could decide to pass on to behavioral ad networks for inspection in the future.

Moreover, the use of DPI for behavioral advertising defies user expectations about what happens when they surf the Web and communicate online. Most Internet users would be surprised to find a middleman lurking between them and the Web sites they visit. Giving an unknown third party broad access to most consumer Web communications may undermine the trust that consumers have in their ISPs.

B. Current Implementations May Interfere With Normal Internet Use

Despite these concerns, several ad network companies are moving forward with plans to use DPI for behavioral advertising. The two most prominent ad networks engaged in this practice are NebuAd in the United States and Phorm in the UK. Charter Communications, a cable broadband ISP, recently announced – and then delayed – a plan to conduct trials of the NebuAd behavioral advertising technology.[19] Several other ISPs, such as Wide Open West (WOW!), CenturyTel, Embarq and Knology also announced plans with NebuAd to trial or deploy its behavioral advertising technology. Although a number of these ISPs have put their plans on hold in the wake of a firestorm of criticism, NebuAd continues to work with U.S. ISPs and seek new ISP partners. Phorm, which originally announced deals with three of the UK's largest ISPs and has sought partnerships with U.S. ISPs, is also now encountering hesitation from some of its UK partners.[20]

---

[19] Saul Hansell, *Charter Suspends Plan to Sell Customer Data to Advertisers*, N.Y. TIMES: BITS BLOG, Jun. 24, 2008, http://bits.blogs.nytimes.com/2008/06/24/charter-suspends-plan-to-sell-customer-data-to-advertisers.

[20] Chris Williams, *CPW builds wall between customers and Phorm*, REGISTER, Mar. 11, 2008, http://theregister.co.uk/2008/03/11/phorm_shares_plummet.

Independent analyses of both companies' systems have revealed that by virtue of their ability to intercept Internet traffic en route – and based on their desire to track individual Internet users – they engage in an array of practices that are inconsistent with the usual flow of Internet traffic. NebuAd reportedly injects computer code into Web traffic streams that causes numerous cookies to be placed on users' computers for behavioral tracking, none of which are related to or sanctioned by the Web sites the users visit.[21] When a user navigates to a particular Web site, Phorm reportedly pretends to be that Web site so that it can plant a behavioral tracking cookie linked to that site on the user's computer.[22] In addition to the privacy implications of tracking all of an individual's Web activities, this kind of conduct has the potential to create serious security vulnerabilities in the network,[23] hamper the speed of users' Internet connections, and interfere with ordinary Web functionality. At a time when many different kinds of companies are working to build a trusted computing platform for the Internet, having ISPs work with partners whose practices undermine trust raises future cyber-security concerns.

C. Current Implementations May Violate Federal Law

Behavioral advertising networks using DPI stress that the profiles they compile are anonymous and contain only generic marketing classifications. That may well be true, and such profiles would not be the focus of serious privacy concerns. Rather, our concern is with what it takes to compile such profiles: the disclosure, copying and analysis of substantially all of an Internet user's Web traffic. That advertising networks today use only a portion of what they collect and discard the raw data after analyzing it offers small

---

[21] Robert M. Topolski, *NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking* (June 2008), http://publicknowledge.org/pdf/nebuad-report-20080618.pdf.

[22] Richard Clayton, *The Phorm "Webwise" System* (May 18, 2008), http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf.

[23] These types of behaviors have much in common with well-understood online security threats, and parts of the Internet security community are already investigating how to respond. *See* Anti-Spyware Coalition, *Anti-Spyware Coalition Aims to Address Behavioral Targeting* (Apr. 2008), http://antispywarecoalition.org/newsroom/20080425press.htm.

comfort to what they or their potential competitors might do with the data in the future. Nor do current claims about the anonymity of stored profiles overcome the fact that the initial capture and disclosure of substantially all of a person's Web traffic defies reasonable expectations and may violate wiretapping laws.

The federal Wiretap Act, as amended by the Electronic Communications Privacy Act (ECPA), prohibits the interception and disclosure of electronic communications – including the content of Internet packets – without consent.[24] Although exceptions to this rule permit interception and disclosure without consent, we seriously doubt that any of them apply to the use of DPI for behavioral advertising purposes. Accordingly, we believe that the Wiretap Act requires consent before the content of Internet packets may be used for behavioral advertising purposes, and furthermore that such consent should be obtained on an opt-in basis after unavoidable notice. Certain state laws may take this one step further, requiring consent from both parties to the communication: the consumer and the Web site he or she is visiting. A detailed CDT legal memorandum on the application of the Wiretap Act, ECPA and relevant state wiretap laws to the use of Internet data content for behavioral advertising is attached as Appendix A.

Importantly, federal and state wiretap laws make no distinction between PII and non-PII, and rightly so: eavesdropping on phone calls, for example, is an obvious privacy violation even when the eavesdropper does not know the identity of the caller. Existing legal prohibitions against interception and disclosure of electronic communications apply whether or not those communications contain PII.

As Congressmen Markey, Barton and Dingell have noted, the Cable Communications Policy Act also applies here.[25] The law prohibits cable operators from collecting or

---

[24] 18 U.S.C. § 2511.

[25] Reps. Edward Markey and Joe Barton, *Letter to Charter Communications CEO in Regards to the Charter-NebuAd Data Collection Scheme* (May 2008), http://markey.house.gov/docs/telecomm/letter_charter_comm_privacy.pdf; Reps. Edward Markey, John Dingell, and Joe Barton, *Letter to Embarq CEO* (July 2008), http://markey.house.gov/index.php?option=content&task=view&id=3410&Itemid=125.

disclosing personally identifiable information without prior consent.[26] While the term "personally identifiable information" in the law is defined by what it does not include – "any record of aggregate data which does not identify particular persons"[27] – we doubt that a user's entire Web browsing data stream, unique to that individual, often containing both PII and non-PII, would be considered aggregate data as that term is commonly understood.

We do not believe that it is possible to shoehorn the collection and disclosure of a subscriber's entire browsing history for advertising purposes into the statute's exception for collection or disclosure of information that is necessary to render service.[28] Thus, we conclude that cable-based ISPs that wish to disclose the content of Internet packets to advertising networks would also have to meet the consent requirements of the Cable Communications Policy Act.

The DPI models that have been deployed thus far have failed to obtain affirmative, express opt-in consent required by law. In fact, they have failed to meet even relatively lax standards of implied consent. Several small U.S. ISPs, for example, have buried vague information about their deals with NebuAd in the ISPs' terms of service.[29] Charter Communications, the largest U.S. ISP that had planned to partner with NebuAd, notified its subscribers that they would be receiving more relevant ads, but did not explain its plans to intercept subscribers' traffic data and did not provide a way for subscribers to give or withhold consent to having their communications intercepted and disclosed. Charter has since suspended its plans.

---

[26] 47 U.S.C. § 551(b)-(c). A 1992 amendment adding the phrase "other services" to the Cable Act's privacy provision made it clear that the law covers Internet services provided by cable operators.

[27] *Id.* § 551(a)(2)(A).

[28] *Id.* § 551(a)(2)(B).

[29] *See* Mike Masnick, *Where's The Line Between Personalized Advertising And Creeping People Out?*, TECHDIRT, Mar. 11, 2008, http://techdirt.com/articles/20080311/121305499.shtml; Peter Whoriskey, *Every Click You Make*, WASH. POST, Apr. 3, 2008, http://washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html.

Designing a robust opt-in consent system for DPI-based behavioral advertising presents a formidable challenge. We are less than sanguine that such a system can be easily designed, particularly since it must not only provide a way for consumers to give affirmative consent, but it must also provide a method for them to revoke that consent. The burden is on those who wish to move forward with the model to demonstrate that an express notice and consent regime can work in this context.

V. The Role of Congress

Congress should take action to address the significant privacy concerns raised by DPI and broader online privacy issues:

- As a first step, we urge the Subcommittee to seek additional information directly from ISPs and other companies about their use of DPI technology in order to better assess the associated technological, legal and policy implications.

- This Subcommittee should set a goal of enacting in the next year general privacy legislation covering both the online and offline worlds. CDT has long argued for simple, flexible baseline consumer privacy legislation that would protect consumers from inappropriate collection and misuse of their personal information while enabling legitimate business use to promote economic and social value. In principle, such legislation would codify the fundamentals of "fair information practices:" requiring transparency and notice of data collection practices, providing consumers with meaningful choice regarding the use and disclosure of that information, allowing consumers reasonable access to personal information they have provided, providing remedies for misuse or unauthorized access, and setting standards to limit data collection and ensure data security. Although we believe communications privacy laws already apply to some applications of DPI, enacting baseline privacy legislation would further clarify consumers' privacy

rights and create protections for other forms of data collection not covered under current law.

- The FTC's draft proposed principles for online advertising fail to address issues specific to the DPI-based advertising model. It is also unclear whether the FTC will formally adopt the principles or put its enforcement power behind them. We ask the Subcommittee to urge the FTC to address DPI in its guidelines and exercise the full measure of its enforcement authority over online advertising practices.

- Congress should examine and strengthen existing communications privacy laws to cover new services, technologies and business models with consistent rules. ECPA was passed more than 20 years ago, long before there was a World Wide Web and the Internet became integrated into Americans' daily lives. The application of the law to common online activities including Web search remains unclear and the legal protections it provides for the enormous amounts of personal data stored online are far too low. Congress should also consider clarifying that the Cable Communications Policy Act's privacy provisions apply to broadband Internet service.

VI. Conclusion

CDT would like to thank the Subcommittee again for holding this important and forward-looking hearing. We believe that Congress has a critical role to play in ensuring that privacy is protected as deep packet inspection and other new technologies contribute to an increasingly complex online environment. CDT looks forward to working with the Subcommittee as it pursues these issues further.

Appendix A: An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising

July 8, 2008

Much of the content on the Internet (just like content in newspapers, broadcast TV, radio and cable) is supported in whole or part by advertising revenue. The Internet offers special opportunities to target ads based on the expressed or inferred interests of the individual user. There are various models for delivering targeted ads online. These range from the purely contextual (everyone who visits a travel site sees the same airline ad) to models that involve compiling information about the online behavior of individual Internet users, to be used in serving them advertisements. For years, Web sites have entered into agreements with advertising networks to use "cookies" to track individual users across Web sites in order to compile profiles. This approach has always been, and remains, a source of privacy concern, in part because the conduct usually occurs unbeknownst to most Internet users. Recent developments, including the mergers between online service providers and some of the largest online advertising networks, have heightened these concerns. The Center for Democracy & Technology has been conducting a major project on behavioral advertising, in which we have been researching behavioral advertising practices, consulting with Internet companies and privacy advocates, developing policy proposals, filing extensive comments at the FTC, and analyzing industry self-regulatory guidelines.

This memo focuses on the implications of a specific approach to behavioral advertising being considered by Internet advertising networks and Internet Service Providers (ISPs). This new approach involves copying and inspecting the content of each individual's Internet activity with the cooperation of his or her ISP.[1] Under this new model, an advertising network strikes a deal with an ISP, and the ISP allows the network to copy the contents of the individual Web traffic streams of each of the ISP's customers. The advertising network analyzes the content of these traffic streams in order to create a record of each individual's online behaviors and interests. Later, as customers of the ISP surf the Web and visit sites where the advertising network has purchased advertising space, they see ads targeted based on their previous Internet behavior.

NebuAd is one such advertising network company operating in the United States. In the past few months, it has come to light that NebuAd was planning to partner with Charter Communications, a cable broadband ISP, to conduct trials of the NebuAd

[1] *See, e.g.*, Peter Whoriskey, *Every Click You Make*, WASH. POST (Apr. 3, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html?nav=hcmodule; Saul Hansell, *I.S.P. Tracking: The Mother of All Privacy Battles*, N.Y. TIMES: BITS BLOG (Mar. 20, 2008), http://bits.blogs.nytimes.com/2008/03/20/isp-tracking-the-mother-of-all-privacy-battles/?scp=1-b&sq=the+mother+of+all+privacy+battles&st=nyt.

behavioral advertising technology. Several other smaller ISPs, such as Wide Open West (WOW!), CenturyTel, Embarq, and Knology, have also announced plans with NebuAd to trial or deploy its behavioral advertising technology. In response to concerns raised by subscribers, privacy advocates, and policymakers, Charter, CenturyTel and Embarq have delayed these plans, but NebuAd and other similar companies are continuing to seek new ISP partners.

The use of Internet traffic content from ISPs for behavioral advertising is different from the "cookie"-based model in significant ways and raises unique concerns.[2] Among other differences, it copies all or substantially all Web transactions, including visits to sites that do not use cookies. Thus, it may capture not only commercial activity, but also visits to political, advocacy, or religious sites or other non-commercial sites that do not use cookies.

In this memo, we conclude that the use of Internet traffic content from ISPs may run afoul of federal wiretap laws unless the activity is conducted with the consent of the subscriber.[3] To be effective, such consent should not be buried in terms of service and should not be inferred from a mailed notice. We recommend prior, express consent, but we do not offer here any detailed recommendations on how to obtain such consent in an ISP context. Also, we note that that the California law requiring consent of all the parties to a communication has been applied by the state Supreme Court to the monitoring of telephone calls when the monitoring is done at a facility outside California. The California law so far has not been applied to Internet communications and it is unclear whether it would apply specifically to the copying of communications as conducted for behavioral monitoring purposes, but if it or another state's all-party consent rule were applied to use of Internet traffic for behavioral profiling, it would seem to pose an insurmountable barrier to the practice.

---

[2] Privacy concerns also apply to advertising-based models that have been developed for services, such as email, that ride over ISP networks. *See* CDT Policy Post 10.6, *Google GMail Highlights General Privacy Concerns*, (Apr. 12, 2004), http://www.cdt.org/publications/policyposts/2004/6 (recommending express prior opt-in for advertising-based email service).

[3] Additional questions have been raised under the Cable Communications Policy Act. *See* Rep. Edward Markey and Rep. Joe Barton, *Letter to Charter Communications CEO in Regards to the Charter-NebuAd Data Collection Scheme* (May 2008), http://markey.house.gov/docs/telecomm/letter_charter_comm_privacy.pdf. In this memo, we focus on issues arising under the federal Wiretap Act, as amended by the Electronic Communications Privacy Act.

I. Wiretap Act

A. Service Providers Cannot "Divulge" The Contents of Subscriber Communications, Except Pursuant to Limited Exceptions

The federal Wiretap Act, as amended by the Electronic Communications Privacy Act, protects the privacy of wire, oral, and electronic communications.[4] "[E]lectronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system . . . ."[5] Web browsing and other Internet communications are clearly electronic communications protected by the Wiretap Act.

In language pertinent to the model under consideration, § 2511(3) of the Act states that "a person or entity providing an electronic communication service to the pubic shall not intentionally divulge the contents of any communications . . . while in transmission on that service to any person or entity other than an addressee or intended recipient . . . ."[6]

There are exceptions to this prohibition on disclosure, two of which may be relevant here. One exception specifies that "[i]t shall not be unlawful under this chapter for an . . . electronic communication service, whose facilities are used in the transmission of a[n] . . . electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a *necessary incident to the rendition of his service* or to the protection of the rights or property of the provider of that service."[7] We will refer to this as the "necessary incident" exception. The second exception is for disclosures with the consent of one of the parties.[8] We will discuss both exceptions below. We conclude that only the consent exception applies to the disclosure of subscriber content for behavioral advertising, and we will discuss preliminarily what "consent" would mean in this context.

---

[4] 18 U.S.C. §§ 2510-2522.

[5] *Id.* § 2510(12).

[6] *Id.* § 2511(3)(a). Lest there be any argument that the disclosure does not occur while the communications are "in transmission," we note that the Stored Communications Act (SCA) states that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." *Id.* § 2702(a)(1). We do not comment further here on the SCA because, in our judgment, the approach that has been described so far clearly involves the divulging of communications "while in transmission."

[7] *Id.* § 2511(2)(a)(i) (emphasis added). This analysis focuses on the capture of electronic communications and definitions are abridged accordingly.

[8] *Id.* § 2511(3)(b)(ii).

B. With Limited Exceptions, Interception Is Also Prohibited

The Wiretap Act regulates the "interception" of electronic communications. The Act defines "intercept" as the "acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical, or other device."[9]

The Wiretap Act broadly bars all intentional interception of electronic communications.[10] The Act enumerates specific exceptions to this prohibition.[11] Law enforcement officers, for example, are authorized to conduct interceptions pursuant to a court order. For ISPs and other service providers, there are three exceptions that might be relevant. Two we have mentioned already: the "necessary incident" exception and a consent exception.[12]

A third exception, applicable to interception but not to disclosure, arises from the definition of "intercept," which is defined as acquisition by an "electronic, mechanical, or other device," which in turn is defined as "any device or apparatus which can be used to intercept a[n] . . . electronic communication *other than*—(a) any telephone or telegraph instrument, equipment or facility, or any component thereof . . . (ii) being used by a provider of . . . electronic communication service in the *ordinary course of its business* . . . ."[13] This provision thus serves to limit the definition of "intercept," providing what is sometimes called the "telephone extension" exception, but which we will call the "business use" exception.

---

[9] *Id.* § 2510(4).

[10] *Id.* § 2511(1).

[11] *Id.* § 2511(2).

[12] Separate from the consent provision for disclosure, the consent exception for interception is set forth in 18 U.S.C. § 2511(2)(d): "It shall not be unlawful under this chapter for a person not acting under color of law to intercept a[n] . . . electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception . . . ."

[13] *Id.* § 2510(5) (emphasis added).

C. The Copying of Internet Content for Disclosure to Advertising Networks Constitutes Interception

When an ISP copies a customer's communications or allows them to be copied by an advertising network, those communications have undoubtedly been "intercept[ed]."[14] Therefore, unless an exception applies, it seems likely that placing a device on an ISP's network and using it to copy communications for use in developing advertising profiles would constitute illegal interception under § 2511(1)(a); similarly, the disclosure or use of the intercepted communications would run afoul of § 2511(1)(c) or § 2511(1)(d), respectively.

D. The "Necessary Incident" Exception Probably Does Not Permit the Interception or Disclosure of Communications for Behavioral Advertising Purposes

The Wiretap Act permits interception of electronic communications when the activity takes place as "a necessary incident to the rendition of [the ISP's] service or to the protection of the rights or property of the provider of that service."[15] The latter prong covers anti-spam and anti-virus monitoring and filtering and various anti-fraud activities, but cannot be extended to advertising activities, which, while they may enhance the service provider's revenue, do not "protect" its rights. Courts have construed the "necessary incident" prong quite strictly, requiring a service provider to show that it *must* engage in the activity in order to carry out its business.[16] It is unlikely that the copying, diversion, or disclosure of Internet traffic content for behavioral advertising would be construed as a "necessary incident" to an ISP's business. Conceivably, an ISP could argue that its business included copying its subscribers communications and providing them to third parties for purposes of placing advertisements on Web sites unaffiliated with the ISP, but the ISP would probably have to state that that business existed and get the express agreement of its customers that they were subscribing to that business as well as the basic business of Internet access, which leads anyhow to the consent model that we conclude is necessary.

---

[14] *See, e.g.*, United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992) (holding in context of telephone communications that "when the contents of a wire communication are captured or redirected in any way, an interception occurs at that time" and that "[r]edirection presupposes interception"); *In re* State Police Litig., 888 F. Supp. 1235, 1267 (D. Conn. 1995) (stating in context of telephone communications that "it is the act of diverting, and not the act of listening, that constitutes an 'interception'").

[15] 18 U.S.C. § 2511(2)(a)(i).

[16] *See* United States v. Councilman, 418 F.3d 67, 82 (1st Cir. 2005) (en banc) (holding that service provider's capture of emails to gain commercial advantage "clearly" was not within service provider exception); Berry v. Funk, 146 F.3d 1003, 1010 (D.C. Cir. 1998) (holding in context of telephone communications that switchboard operators' overhearing of a few moments of phone call to ensure call went through is a "necessary incident," but anything more is outside service provider exception).

E. While It Is Unclear Whether the "Business Use" Exception Would Apply to the Use of a Device Installed or Controlled by a Party Other than the Service Provider, the Exception Does Not Apply to the Prohibition Against Divulging a Subscriber's Communications

The "business use" exception, § 2510(5)(a), constricts the definition of "device" and thereby narrows the definition of "intercept" in the Wiretap Act. There are two questions involved in assessing applicability of this exception to the use of Internet traffic content for behavioral advertising: (1) whether the device that copies the content for delivery to the advertising network constitutes a "telephone or telegraph instrument, equipment or facility, or any component thereof," and (2) whether an ISP's use of the device would be within the "ordinary course of its business."

We will discuss the "business use" exception at some length, because there has been considerable discussion already about whether copying of an ISP subscriber's communications for behavioral advertising is an "interception" under § 2511(1) of the Wiretap Act. However, even if the business use exception applied, an ISP would only avoid liability for the *interception* of electronic communications. It would still be prohibited from divulging the communications of its customers to an advertising network under the separate section of the Wiretap Act, § 2511(3), which states that a service provider "shall not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient . . . ."[17] The business use exception does not apply to this prohibition against divulging.[18]

At first glance, it would seem that the business use exception is inapplicable to the facilities of an ISP because the exception applies only to a "telephone or telegraph instrument, equipment or facility, or any component thereof." However, the courts have recognized that ECPA was motivated in part by the "dramatic changes in new computer and telecommunications technologies"[19] and therefore was intended to make the Wiretap Act largely neutral with respect to its treatment of various communications technologies. The Second Circuit, for example, concluded in a related context that the term "telephone" should broadly include the "instruments, equipment and facilities that ISPs use to

---

[17] 18 U.S.C. § 2511(3)(a).

[18] By adopting two different exceptions—"necessary incident" and "ordinary course"—Congress apparently meant them to have different meanings. Based on our reading of the cases, the necessary incident exception is narrower than the ordinary course exception. It is significant that the "necessary incident" exception applies to both interception and disclosure while the "ordinary course" exception is applicable only to interception. This suggests that Congress meant to allow service providers broader latitude in examining (that is, "intercepting" or "using") subscriber communications so long as they did not disclose the communications to third parties. This permits providers to conduct a range of in-house maintenance and service quality functions that do not involve disclosing communications to third parties.

[19] S. Rep. No. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555.

transmit e-mail."[20] Therefore, as a general matter, it should be assumed that the business use exception is available to ISPs.

However, it is not certain that the device used to copy and divert content for behavioral advertising would be considered to be a component of the service provider's equipment or facilities. In some of the behavioral advertising implementations that have been described, the monitoring device or process is not developed or controlled by the ISP but rather by the advertising network.

The second question is whether an ISP's use of a device to copy traffic content for behavioral advertising falls within the "ordinary course of its business." There are a number of cases interpreting this exception, but none of them clearly addresses a situation where a service provider is copying all of the communications of its customers. Many of the cases arise in situations where employers are monitoring the calls of their employees for purposes of supervision and quality assurance. "These cases have narrowly construed the phrase 'ordinary course of business.'"[21] Often such cases also involve notice to the employees and implied consent.[22] One court has stated that, even if an entity could satisfy the business use exception, notice to one of the parties being monitored would be required.[23] Other cases involve the monitoring of prisoners.

Some cases have interpreted "ordinary course" to mean anything that is used in "normal" operations. The D.C. Circuit, for instance, has suggested that monitoring "undertaken normally" qualifies as being within the "ordinary course of business."[24] In the context of law enforcement taping of the phone calls of prisoners, the Ninth and Tenth Circuits have concluded that something is in the "ordinary course" if it is done routinely and consistently.[25] It might be that courts would give equal or greater latitude to service providers in monitoring their networks than they would give to mere subscribers or users.

Other circuit courts have used a more limited interpretation, concluding that "ordinary course" only applies if the device is being used to intercept communications for "legitimate business reasons."[26] Although the courts have not been entirely clear as to

---

[20] Hall v. Earthlink Network, Inc., 396 F.3d 500, 505 (2d Cir. 2005) (quoting S. Rep. No. 99-541 at 8).

[21] United States v. Murdock, 63 F.3d 1391. 1396 (6th Cir 1995).

[22] *E.g.*, James v. Newspaper Agency Corp., 591 F.2d 579 (10th Cir. 1979).

[23] *See, e.g.*, Adams v. City of Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001).

[24] Berry v. Funk, 146 F.3d 1003, 1009 (D.C. Cir. 1998) (workplace monitoring).

[25] *See* United States v. Van Poyck, 77 F.3d 285, 292 (9th Cir. 1996); United States v. Gangi, 57 Fed. Appx. 809, 814 (10th Cir. 2003).

[26] *See* Arias v. Mutual Central Alarm Serv., Inc., 202 F.3d 553, 560 (2d Cir. 2000) (monitoring calls to an central alarm monitoring service).

what that means, some have suggested that it is much closer to necessity than to mere profit motive.[27] One frequently-cited case explicitly holds that the business use exception does not broadly encompass a company's financial or other motivations: "The phrase 'in the ordinary course of business' cannot be expanded to mean anything that interests a company."[28]

Normal principles of statutory interpretation would require that some independent weight be given to the word "ordinary," so that the exception does not encompass anything done for business purposes. It is unclear, however, how much weight courts would give to the word "ordinary" in a rapidly changing market. It does not seem that the phrase "ordinary course of business" should preclude innovation, but courts might refer to past practices and normal expectations surrounding a line of business and specifically might look to what customers have come to expect.

Viewed one way, it is hard to see how the copying of content for behavioral advertising is part of the "ordinary course of business" of an ISP. After all, the ISP is not the one that will be using the content to develop profiles of its customers; the profiling is done by the advertising network, which does not even disclose to the ISP the profiles of its own subscribers. (The profiles are proprietary to the advertising network and it is careful not to disclose them to anyone.) Very few (if any) of the ads that are placed using the profiles will be ads for the ISP's services; they will be ads for products and services completely unrelated to the ISP's "ordinary course of business." Moreover, the ads will be placed on Web sites having no affiliation with the ISP. On the other hand, the ISP could argue that part of its business model—part of what keeps its rates low—is deriving revenue from its partnership with advertising networks.

The legislative histories of the Wiretap Act and ECPA weigh against a broad reading of the business use exception. Through these laws, Congress intended to create a statutory regime generally affording strong protection to electronic communications. Congress included limited, specific and detailed exceptions for law enforcement access to communications, and other limited, specific and detailed exceptions to allow companies providing electronic communications service to conduct ordinary system maintenance and operational activities. Congress gave especially high protection to communications content. If the business use exception can apply any time an ISP identifies a new revenue

---

[27] *See id.* (concluding that alarm company had legitimate reasons to tap all calls because such businesses "are the repositories of extremely sensitive security information, including information that could facilitate access to their customers' premises"); *see also* First v. Stark County Board of Comm'rs, 234 F.3d 1268, at *4 (6th Cir. 2000) (table disposition).

[28] Watkins v. L.M. Berry & Co., 704 F.2d 577, 582 (11th Cir. 1983). Watkins states: "We hold that a personal call may not be intercepted in the ordinary course of business under the exemption in section 2510(5)(a)(i), except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not. In other words, a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents." 704 F.2d at 583. This language supports the conclusion that the business use exception could not cover wholesale interception of ISP traffic, no more than switchboard operators can perform wholesale monitoring of telephone traffic.

stream that can be tapped though use of its customers' communications, this careful statutory scheme would be seriously undermined.

F. The Consent Exception: The Context Weighs Heavily in Favor of Affirmative, Opt-In Consent from ISP Subscribers

Consent is an explicit exception both to the prohibition against intercepting electronic communications under the Wiretap Act and to the Act's prohibition against disclosing subscriber communications. The key question is: How should consent be obtained for use of Internet traffic content for behavioral advertising? Courts have held in telephone monitoring cases under the Wiretap Act that consent can be implied, but there are relatively few cases specifically addressing consent and electronic communications. However, in cases involving telephone monitoring, one circuit court has stated that consent under the Wiretap Act "is not to be cavalierly implied."[29] Another circuit court has noted that consent "should not casually be inferred"[30] and that consent must be "actual," not "constructive."[31] Yet another circuit court has stated: "Without actual notice, consent can only be implied when the surrounding circumstances *convincingly* show that the party knew about and consented to the interception."[32] Furthermore, "knowledge of the *capability* of monitoring alone cannot be considered implied consent."[33] The cases where consent has been implied involve very explicit notice; many of them involve the monitoring of prisoners' phone calls.[34]

Consent is context-based. It is one thing to imply consent in the context of a prison or a workplace, where notice may be presented as part of the daily log-in process. It is quite another to imply it in the context of ordinary Internet usage by residential subscribers, who, by definition, are using the service for personal and often highly sensitive communications. Continued use of a service after a mailed notice might not be

---

[29] Watkins. 704 F.2d at 581 ("Consent under title III is not to be cavalierly implied. Title III expresses a strong purpose to protect individual privacy by strictly limiting the occasions on which interception may lawfully take place.").

[30] Griggs-Ryan v. Smith, 904 F.2d 112, 117 (1st Cir. 1990).

[31] *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 20 (1st Cir. 2003); *see also* United States v. Corona-Chavez, 328 F.3d 974, 978 (8th Cir. 2003).

[32] Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (internal quotation omitted).

[33] Watkins, 704 F.2d at 581; *see also* Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992) (holding that consent not implied when individual is aware only that monitoring might occur, rather than knowing monitoring is occurring).

[34] "The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private. And the ultimate determination must proceed in light of the prophylactic purpose of Title III-a purpose which suggests that consent should not casually be inferred." Griggs-Ryan, 904 F.2d at 117.

enough to constitute consent. Certainly, mailing notification to the bill payer is probably insufficient to put all members of the household who share the Internet connection on notice.

Thus, it seems that an assertion of implied consent, whether or not users are provided an opportunity to opt out of the system, would most likely not satisfy the consent exception for the type of interception or disclosure under consideration here. Express prior consent (opt-in consent) is clearly preferable and may be required. While meaningful opt-in consent would be sufficient, courts would likely be skeptical of an opt-in consisting merely of a click-through agreement—i.e., a set of terms that a user agrees to by clicking an on-screen button—if it displays characteristics typical of such agreements, such as a large amount of text displayed in a small box, no requirement that the user scroll through the entire agreement, or the opt-in provision buried among other terms of service.[35]

In regards to consent, the model under discussion here is distinguishable from the use of "cookies," which were found to be permissible by a federal district court in a 2001 case involving DoubleClick.[36] In that case, the Web sites participating in the DoubleClick advertising network were found to be parties to the communications of the Internet users who visited those sites. As parties to the communications, the Web sites could consent to the use of the cookies to collect information about those communications. Here, of course, the ISPs are not parties to the communications being monitored and the interception or disclosure encompasses communications with sites that are not members of the advertising network. Therefore, the source of consent must be the IPS's individual subscribers, as it would be impossible to obtain consent from every single Web site that every subscriber may conceivably visit.

II. State Laws Requiring Two-Party Consent to Communication Interception

A. Summary

In addition to the federal Wiretap Act, a majority of states have their own wiretap laws, which can be more stringent than the federal law. Most significantly, twelve states[37] require all parties to consent to the interception or recording of certain types of communications when such interception is done by a private party not under the color of law.

---

[35] *See, e.g.*, Specht v. Netscape Commc'ns Corp., 306 F.3d 17 (2d Cir. 2002) (rejecting online arbitration agreement because, among other things, site permitted customer to download product without having scrolled down to arbitration clause and agreement button said only "Download"); United States v. Lanoue, 71 F.3d 966, 981 (1st Cir. 1995) ("Deficient notice will almost always defeat a claim of implied consent.").

[36] *In re* DoubleClick Inc. Privacy Litig., 154 F.Supp.2d 497 (S.D.N.Y. 2001).

[37] The twelve states are California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington.

In several of these states—for example, Connecticut—the all-party consent requirement applies only to the recording of oral conversations. In others, the all-party consent rule extends to both voice and data communications. For example, Florida's Security of Communications Act makes it a felony for any individual to intercept, disclose, or use any wire, oral, or electronic communication, unless that person has obtained the prior consent of all parties.[38] Similarly, the Illinois statute on criminal eavesdropping prohibits a person from "intercept[ing], retain[ing], or transcrib[ing an] electronic communication unless he does so . . . with the consent of all of the parties to such . . . electronic communication."[39]

The most important all-party consent law may be California's, because the California Supreme Court held in 2006 that the law can be applied to activity occurring outside the state.

B. California

The 1967 California Invasion of Privacy Act makes criminally liable any individual who "intentionally taps, or makes any unauthorized connection . . . or who willfully and without the consent of all parties to the communication . . . reads, or attempts to read, or to learn the contents or meaning of any message . . . or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place" in California.[40] It also establishes liability for any individual "who uses, or attempts to use, in any manner . . . any information so obtained" or who aids any person in doing the same.[41] The law has a separate section creating liability for any person eavesdropping upon or recording a confidential communication "intentionally and without the consent of all parties," whether the parties are present in the same location or communicating over telegraph, telephone, or other device (except a radio).[42]

Consent can be implied only in very limited circumstances. The California state Court of Appeals held in *People v. Garber* that a subscriber to a telephone system is deemed to have consented to the telephone company's monitoring of his calls if he uses the system in a manner that reasonably justifies the company's belief that he is violating his subscription rights, and even then the company may only monitor his calls to the

---

[38] Fla. Stat. § 934.03(1).

[39] Ill. Comp Stat. 5/14-1(a)(1).

[40] Cal. Pen. Code § 631(a).

[41] *Id.*

[42] *Id.* § 632(a). The statute explicitly excludes radio communications from the category of confidential communications.

extent necessary for the investigation.[43] An individual can maintain an objectively reasonable expectation of privacy by explicitly withholding consent for a tape recording, even if the other party has indicated an intention to record the communication.[44]

In *Kearney v. Salomon Smith Barney, Inc.*, the state Supreme Court addressed the conflict between the California all-party consent standard and Georgia's wiretap law, which is modeled after the federal one-party standard.[45] It held that, where a Georgia firm recorded calls made from its Georgia office to residents in California, the California law applied. The court said that it would be unfair to impose damages on the Georgia firm, but prospectively the case effectively required out-of-state firms having telephone communications with people in California to announce to all parties at the outset their intent to record a communication. Clear notice and implied consent are sufficient. "If, after being so advised, another party does not wish to participate in the conversation, he or she simply may decline to continue the communication."[46]

C. The Implications of *Kearney*

The Kearney case arose in the context of telephone monitoring, and there is a remarkable lack of case law addressing whether the California statute applies to Internet communications. If it does, or if there is one other state that applies its all-party consent rule to conduct affecting Internet communications across state lines, then no practical form of opt-in, no matter how robust, would save the practice of copying Internet content for behavioral advertising. That is, even if the ISP only copies the communications of those subscribers that consent, and the monitoring occurs only inside a one-party consent state, as soon as one of those customers has a communication with a non-consenting person (or Web site) in an all-party consent state that applies its rule to interceptions occurring outside the state, the ISP would seem to be in jeopardy. The ISP could not conceivably obtain consent from every person and Web site in the all-party consent state. Nor could it identify (for the purpose of obtaining consent) which people or Web sites its opted-in subscribers would want to communicate with in advance of those communications occurring.

A countervailing argument could be made that an all-party consent rule is not applicable to the behavioral advertising model, since the process only copies or divulges one half of the communication, namely the half from the consenting subscriber.

---

[43] 275 Cal. App. 2d 119 (Cal. App. 1st Dist. 1969).

[44] Nissan Motor Co. v. Nissan Computer Corp., 180 F. Supp. 2d 1089 (C.D. Cal. 2002).

[45] 39 Cal. 4th 95 (2006).

[46] Id. at 118.

Conclusion

The practice that has been described to us, whereby an ISP may enter into an agreement with an advertising network to copy and analyze the traffic content of the ISP's customers, poses serious questions under the federal Wiretap Act. It seems that the disclosure of a subscriber's communications is prohibited without consent. In addition, especially where the copying is achieved by a device owned or controlled by the advertising network, the copying of the contents of subscriber communications seems to be, in the absence of consent, a prohibited interception. Affirmative express consent, and a cessation of copying upon withdrawal of consent, would probably save such practices under federal law, but there may be state laws requiring all-party consent that would be more difficult to satisfy.

Mr. MARKEY. Thank you, Ms. Cooper, very much.

Our second witness is Mr. Robert Dykes. He is the founder, chairman, and chief executive officer of NebuAd, a behavioral advertising firm. Prior to forming NebuAd, Mr. Dykes held senior positions with Symantec Corporation and the Ford Motor Company. We welcome you, sir. Whenever you are ready, please begin.

STATEMENT OF ROBERT R. DYKES, CHAIRMAN AND CEO, NEBUAD, INC.

Mr. DYKES. Thank you, Mr. Chairman, Mr. Stearns, and other members of the committee. My name is Bob Dykes, CEO of NebuAd, a recent entry into the online advertising industry.

My objectives today are to recognize that our business process, which involves partnering with the Internet Service Providers, the ISPs, raises legitimate privacy issues, but also I want to explain how we have addressed those issues and continue to do so and to enlighten the members of the subcommittee in as much detail as possible within the time allotted about NebuAd's service and technology. In doing so, I hope to dispel the many myths and misconceptions that have surfaced about our company.

In many ways, I feel like Galileo when he was viewed with skepticism on demonstrating that the earth revolved around the sun. Members of the subcommittee, the science exists today, and NebuAd is using it to create truly anonymous profiles that cannot be hacked or reverse-engineered, and it is possible to provide ISP subscribers prior robust notification and a meaningful opportunity to express their informed choice whether to participate in NebuAd's targeted advertising so that they are in control of their online experience.

I come from a security background, serving for many years as executive vice president of Symantec Corporation. When we launched NebuAd several years ago, it was a time when many people had particularly heightened concerns about data security. As part of its mission, NebuAd sought to address these privacy and security concerns. As you will see, NebuAd systems are designed so that no one, not even the government, can determine the identity of our users.

Currently, online advertising solutions and data collection methods operate in many locations throughout the Internet ecosystem, from users' computers to individual Web sites to networks of Web sites. The NebuAd service, in partnership with ISPs, provides consumers with significant benefits, serving them with more relevant ads, which they want, while ensuring they have robust privacy protections and control over their online experience.

NebuAd's ad network also is designed to benefit two groups that provide substantial value on the Internet, the many smaller Web sites and general use sites that have difficulty maintaining free access to their content and the ISPs who need to upgrade their infrastructure to provide increased bandwidth for consumers who increasingly want access to Internet-delivered videos. NebuAd creates these benefits by using a select set of a user's Internet activities to construct anonymous inferences about likely interests, which are then used to select and serve the most relevant advertisements.

We appreciate that there are groups who would like the Internet service providers to be like the post office, but ISPs and the many other entities that operate the Internet are in fact commercial enterprises, not nonprofit, quasi-government organizations. As such, they can see that much of the Internet is well supported by advertising revenue, and it is legitimate for them to seek ways to also increase their advertising revenues. NebuAd enables that endeavor while allowing its ISP partners to maintain their subscribers' trust by giving them control over their online experience. The NebuAd service is architected and its operations are based on principles central to strong privacy protection. That is, we provide users with prior robust notice about the service and the opportunity to express informed choice about whether to participate both before the service takes effect and persistently thereafter. We do not collect or use personally identifiable information, that is PII. We do not store raw data linked to identifiable individuals, and we provide state-of-the-art security for the limited amount of information we do store.

I listened to comments from members of the Senate Commerce Committee last week and the CDT's testimony during that hearing. Immediately after the Senate hearing last week, I made plans to sit down with the CDT to discuss practical solutions to issues they and Members of Congress have raised around notice and informed choice. We met yesterday with staff of the CDT for a few hours and believe that a common ground can be reached on a framework that involves prior and unavoidable, simple, but complete notice to ISP subscribers about NebuAd's operations and an easy and obvious means for consumers to express their informed choice both before NebuAd's behavioral advertising takes effect and thereafter. We also reached a high level of understanding of how a mechanism can be designed that would honor consumers' choice not to participate in NebuAd's targeted advertising and not to have information about their browsing behavior flow to our service. I am extremely encouraged by this and have set a goal of being a privacy leader since I started NebuAd. I will continue to work with CDT on the framework we discussed yesterday, and I am happy to keep members of this committee informed of our progress.

In the meantime, we continue to innovate on privacy. NebuAd last week announced that it was enhancing the industry standard notice options of regular mail and e-mail with a new interstitial or online service, which would appear on a user screen prior to the NebuAd service being enacted. We have designed this notice to be easily readable and understandable, so that users can exercise informed choice. In addition, we are working with our ISP partners to make users' choice of participating in the service more persistent. The NebuAd opt-out system is a more robust mechanism than traditional cookie-based opt-out systems, and as a default, users are considered opted out of the NebuAd system until such time that the system can confirm the consumer has not opted out. So for example, if your Web browser blocks cookies, the NebuAd system will consider you to be an opted-out user and will exclude you from NebuAd's information collection and targeted ads. Further, we are developing a network-based opt-out and working with ISPs on other mechanisms that can be offered to users to honor even more robust and persistent choice, and these will be able to

be configured to ensure that traffic from opted-out users is not diverted.

We understand that to gain the public's trust, we need to adopt strong privacy protections. Ours have been reviewed by such entities as the Ponemon Institute, and we are engaging a Big Four audit firm to conduct an audit to verify that we do what we say we do.

This committee has long been involved with the creation of privacy statutes covering the cable and telecommunications industries, as well as specific statutes addressing online privacy for children and telemarketing. Yet even these and other privacy statutes have been developed one at a time. There is a common thread running through them all, that is, the more sensitive data that is collected and when the collection or disclosure of the data could harm or embarrass a consumer, more rigorous disclosure and consent requirements tend to be imposed. When raw data is linked to identifiable individuals, there is an emerging trend that more rigorous disclosure, consent, and security requirements should be imposed.

NebuAd supports this privacy paradigm, which provides users with consistent expectations and substantial protections. This paradigm also is technology and business neutral, and it is the basis on which NebuAd built its technology and operations. NebuAd urges the committee to maintain both the paradigm and the principle of technology and business neutrality, and we are in favor or a baseline privacy law consistent with that principle. Thank you.

[The prepared statement of Mr. Dykes follows:]

SUMMARY OF TESTIMONY OF BOB DYKES, CEO NEBUAD, INC.
BEFORE THE HOUSE SUBCOMMITTEE ON
TELECOMMUNICATIONS AND THE INTERNET
WHAT YOUR BROADBAND PROVIDER KNOWS ABOUT YOUR WEB USE:
DEEP PACKET INSPECTION AND COMMUNICATIONS LAWS AND POLICIES
July 17, 2008

My name is Bob Dykes, CEO of NebuAd, Inc., a recent entrant into the online advertising industry that partners with Internet Service Providers (ISPs). I come from a security background, serving for many years as Executive Vice President of Symantec Corporation. When we launched NebuAd several years ago, it was at a time when many people had particularly heightened concerns about data security. As part of its mission, NebuAd sought to address these privacy and security concerns, ensuring it was in compliance with both the letter and spirit of the law. Appended to my testimony is a memorandum discussing in greater detail NebuAd's compliance with the law, including the cable privacy statute.

Currently, online advertising solutions operate in many locations throughout the Internet ecosystem – from users' computers to individual web-sites to networks of web-sites. NebuAd system uses a select set of a user's Internet activities to construct anonymous inferences about likely interests, which are then used to select and serve the most relevant advertisements. In operating this service, NebuAd:

- Provides users with prior, robust notice and the opportunity to express informed choice about whether to participate, both before the service takes effect and persistently thereafter;
- Does not collect or use personally-identifiable information ("PII");
- Does not store raw data linked to identifiable individuals; and
- Provides state-of-the art security for any information stored.

As a result, NebuAd's service is designed so that no one – not even the government – can determine the identity of our users.

In the US, privacy statutes have been developed in a largely sector-specific fashion. This Subcommittee has long been part of that trend, having overseen the creation of privacy statutes covering the cable and telecommunications industries. Yet, even though these and other privacy statutes have been developed one at a time, there are common threads running through them:

- When more sensitive data is collected, and when the collection and disclosure of the data could harm or embarrass a consumer, more rigorous disclosure and consent requirements tend to be imposed.
- When raw data linked to an identifiable individual is stored for longer periods, there is an emerging trend that more rigorous disclosure, consent, and security requirements should be imposed.

NebuAd supports this privacy paradigm, which provides users with consistent expectations and substantial protections. This paradigm also is technology and business-neutral, and it is the basis upon which NebuAd built its technology and operations. NebuAd urges the Committee to maintain both the paradigm and the principle of technology and business-neutrality.

TESTIMONY OF BOB DYKES, CEO NEBUAD, INC.
BEFORE THE HOUSE SUBCOMMITTEE ON
TELECOMMUNICATIONS AND THE INTERNET

WHAT YOUR BROADBAND PROVIDER KNOWS ABOUT YOUR WEB USE:
DEEP PACKET INSPECTION AND COMMUNICATIONS LAWS AND POLICIES
July 17, 2008

Chairman Markey, Ranking Member Stearns, and Members of the Subcommittee, thank you for inviting me to appear today to discuss the privacy implications of online advertising solutions in which Internet Service Providers (ISPs) participate. My name is Bob Dykes, CEO of NebuAd, Inc., a recent entrant into the online advertising industry that partners with ISPs. I have spent considerable time over the past year with federal policymakers at the Federal Trade Commission, Federal Communications Commission, and in Congress – as well as with consumer and privacy advocates – discussing NebuAd's technology, operations, and privacy protections and welcome the opportunity to discuss all of this further with the Subcommittee.

The NebuAd service in partnership with ISPs provides consumers with significant benefits, serving them with more relevant ads, which they want, while ensuring they have robust privacy protections and control over their online experience.

NebuAd's Ad Network also is designed to benefit two groups that provide substantial value on the Internet:

- The many smaller web sites and general news sites that have difficulty maintaining free access to their content;
- The ISPs who need to upgrade their infrastructure to provide increased bandwidth for consumers, who increasingly want access to Internet-delivered videos.

INTRODUCTION

Online advertising is a phenomenon of the Internet age. It permits advertisers to provide more relevant messages to consumers and in turn fuels the development of website publishers, both large and small. In fact, advertising is the engine for the free Internet. Within this world of online advertising, NebuAd and its ISP partners are newcomers, just entering among industry giants like Google, Yahoo!, Microsoft, Amazon, and countless website publishers. That means we have a steep hill to climb, but it also means we have great opportunities. We are able to learn the lessons of the industry and construct state-of-the-art technology that delivers ads that are more relevant to users and that provide them with robust and industry-leading privacy protections. Indeed, as I will discuss, these privacy protections are built into our technology and designed into our policies from the ground up.

Let me explain our privacy motivation more fully. I come from a security background, serving for many years as Executive Vice President of Symantec Corporation, a global leader in providing security solutions for computers and computer networks. When we launched NebuAd several years ago, it was at a time when many people had particularly heightened concerns about data security. Hackers were piercing firewalls, seeking to capture seemingly random strands of data to find the identity of users. The government was ordering ISPs and other network providers to turn over data on their users. As part of its mission, NebuAd sought to address these privacy and security concerns, ensuring it was in compliance with both the letter and spirit of the law. I am appending to my testimony a memorandum discussing in greater detail NebuAd's compliance with the law, including the cable privacy statute over which this Subcommittee has jurisdiction.

The NebuAd service is architected and its operations are based on principles essential to strong privacy protection:

- Provide users with prior, robust notice and the opportunity to express informed choice about whether to participate, both before the service takes effect and persistently thereafter;
- Do not collect or use personally-identifiable information ("PII");[1]
- Do not store raw data linked to identifiable individuals; and
- Provide state-of-the art security for any information stored.

As a result, NebuAd's service is designed so that no one – not even the government – can determine the identity of our users. That means our service for ISP users, including the ad optimization and serving system, does not collect or use any PII. In addition, NebuAd requires its ISP partners to provide robust, advance notice about our operations and our privacy protections to their subscribers, who at any time can exercise their choice not to participate. And, finally, we have located our servers in highly secure data centers.

THE NEBUAD TECHNOLOGY AND ITS ADVERTISING OPERATIONS

Currently, online advertising solutions operate in many locations throughout the Internet ecosystem – from users' computers to individual web-sites to networks of web-sites. When an Internet user visits the sites of web publishers, like Yahoo! or Amazon, these sites typically collect information about the user's activities to target ads based on that information. When an

[1] NebuAd does not collect or use personally identifiable information about Internet consumers, and it ensures the anonymous information that its systems infer cannot be used to identify any individual. None of the anonymous information NebuAd stores can be compiled together and somehow reverse engineered to identify any individual. In other words, the information is not "pseudo-anonymous." NebuAd is able to ensure this critical privacy protection by building many safeguards into its system including: completely anonymous user profiles which only store levels of qualifications for market segment categories; market segment categories that are kept sufficiently broad and aged sufficiently rapidly; no connection or link between the ISP's registration data systems and NebuAd; and, no collection of information from any small, identifiable group (such as by specific 9-digit zip-code information).

Internet user conducts a search, the search company may collect information from the user's activity, which in turn may be used to improve the relevance of the ads shown. And when a user visits a web-site within an online advertising network, some of which include thousands of sites, the visits help the network advertising company categorize a user for targeted advertising. All of these activities are well-entrenched in the Internet and, given the enormous and growing use of the Internet, have proven to have mutual benefits for users, publishers – large and small – advertisers, and ad-networks.

NebuAd provides online advertising in partnership with ISPs. The NebuAd advertising service – part of which is collocated with, but operates separate and apart from, an ISP's facilities – has been architected to use only a select set of a user's Internet activities (that is, only a subset of HTTP traffic) to construct anonymous inferences about the user's level of qualification for a predefined set of market segment categories ("anonymous user profiles"), which are then used to select and serve the most relevant advertisements to that user. The NebuAd advertising service does not collect or use any information from password-protected sites (*e.g.*, HTTPS traffic), web mail, email, instant messages, or VOIP traffic. Using only non-PII, NebuAd constructs and continuously updates these unique and anonymous user profiles.[2]

In the course of these business operations, NebuAd's ad optimization and serving system does not collect PII or use information deemed to be sensitive (*e.g.*, information involving a user's financial, sensitive health, or medical matters). In addition, NebuAd requires its ISP partners to provide robust disclosure notices to users prior to initiating any service and permits them to opt-out of having their data collected and receiving targeted ads. Once a user opts-out,

---

[2] The anonymous user profiles do not contain any original raw data, such as URLs navigated, but only consist of a set of numbers that represent the anonymous inferences about the user's level of qualification for a predefined set of market segment categories.

NebuAd deletes that user's anonymous user profile and will ignore the user's subsequent web navigation activity.[3]

Finally, NebuAd's ad optimization and serving system operates similar to traditional ad networks. It makes standard use of cookies for accepted ad serving purposes. It makes standard use of pixel tags that operate only within the security framework of the browser to invoke the placement of ad network cookies and that contain no uniquely identifying number, subscriber identifier, or any other subscriber information. In sum, NebuAd's code used for standard ad serving purposes is both clean in its purpose and function.

THE PRIVACY PARADIGM IN THE UNITED STATES AND NEBUAD'S PRIVACY PROTECTIONS

In contrast to the European Community, where omnibus privacy law covers all industries, in the United States, privacy statutes have been developed in a largely sector-specific fashion. This Subcommittee and the larger Energy and Commerce Committee have long been part of that trend, having overseen the creation of privacy statutes generally covering the cable and telecommunications industries, as well as specific statutes addressing online privacy for children, telemarketing, and spam. Yet, even though these and other privacy statutes have been developed one at a time, there are common threads running through them:

- When more sensitive data is collected, and when the collection and disclosure of the data could harm or embarrass a consumer, more rigorous disclosure and consent requirements tend to be imposed.

- When raw data linked to an identifiable individual is stored for longer periods, there is an emerging trend that more rigorous disclosure, consent, and security requirements should be imposed.

---

[3] NebuAd has enhanced the industry-standard opt-out "cookie" based system with the use of proprietary techniques. This enables the opt-out to be more persistent. NebuAd's entire enhanced opt-out system is linked to individual computers and browsers, and it informs users of this fact in assisting them in understanding the nature of their opt-out choice.

NebuAd supports this privacy paradigm, which provides users with consistent expectations and substantial protections. This paradigm also is technology and business-neutral, and it is the basis upon which NebuAd built its technology and operations. NebuAd urges the Committee to maintain both the paradigm and the principle of technology and business-neutrality.

In implementing this privacy paradigm, NebuAd not only relied on the expertise of its own personnel, it turned to leading privacy experts, including Fran Maier, Executive Director and President of TRUSTe, the consumer privacy organization, Dr. Larry Ponemon of the Ponemon Institute, and Alan Chapell of Chapell & Associates. These experts provided important input into NebuAd's initial privacy program. They were particularly stringent in recommending that NebuAd should not collect PII or sensitive information and that it provide consumers with robust notice and choice. NebuAd followed that guidance in developing our privacy program.[4]

The following summarizes the key privacy protections upon which NebuAd has architected into its technology and based its operations and which ensure its activities and that of its ISP partners are in compliance with federal and state laws:

> **1. NebuAd's service does not collect or use PII from ISP subscribers.** The entire ad optimization and serving system does not collect or use any PII, nor does it collect any information from password-protected sites, web mail, e-mail, instant messages, or VOIP traffic.
>
> **2. NebuAd stores only a set of numbers that represent the user's level of qualification for a predefined set of market segment categories ("anonymous user profiles").** NebuAd does not store raw data such as URLs navigated or IP addresses associated with an identifiable individual. Rather, the NebuAd service constructs

[4] A just released survey of U.S. Internet users by TRUSTe showed that 71% of online consumers are aware their web-surfing information may be collected for the purpose of advertising and 91% wanted to have the tools to assure they could protect their privacy. NebuAd has strived to provide users with this transparency by educating users about its activities and their choices regarding whether to participate in NebuAd's services.

anonymous inferences about the user's level of qualification for a predefined set of market segment categories, and then discards the raw data that was used to create or update a user's anonymous profile. This mechanism of constructing anonymous inferences about the user's level of qualification and not storing raw data provides a strong additional layer of privacy protection that goes beyond the standards used by many Internet companies today.

3. NebuAd's ISP Partners are required to provide robust, direct notice in advance of launch of the service. The notice discloses to the user that the ISP is working to ensure that advertisements shown will be more relevant advertisements, that to deliver these ads its partner creates anonymous profiles based on part of the user's web-surfing behavior, which does not include the collection of PII, and that the user may opt-out of the service. For existing subscribers, the notice is required to be delivered 30-days prior to the launch of the service by postal mail, e-mail, or both.[5] For new subscribers, the notice is required to be placed clearly and conspicuously in the new subscriber sign-up flow and outside the privacy policy. All subscribers can opt-out at any time, and on-going disclosure and opportunity to opt-out is required to be provided within the ISP's privacy policy.

4. NebuAd and its ISP partners offer users advance and on-going choice of opting-out of the service. Users are provided with a clear statement of what opt-out means and the way it operates. Once the opt-out option is chosen, NebuAd honors that choice and ignores the user's subsequent web surfing activity and thus does not serve the user with behaviorally targeted ads.[6]

5. NebuAd's service only creates anonymous user profiles, which contain no PII and no raw data, and its placement of ads is completely anonymous. NebuAd uses proprietary algorithms and techniques, including one-way encryption of data, so that no one – not even NebuAd's engineers who designed the system – can reverse-engineer an anonymous identifier, or the anonymous user profile associated with it, to an identifiable individual.

6. NebuAd avoids any sensitive websites or product categories. NebuAd does not track or serve ads based on visits related to adult content, sensitive medical information, racial or ethnic origins, religious beliefs or content of a sexual nature, and does not have market segment categories for illegal products.

7. NebuAd does not permit either complexity of data or narrowness of data to be reverse-engineered into PII. This protection is accomplished because anonymous user profiles are constructed by anonymous inferences about the consumer's level of qualification for a predefined set of market segment categories. Raw data is simply not

---

5 NebuAd seeks to ensure that users are fully informed of its activities and are given full opportunity to choose whether to participate. To that end, we are developing enhanced notification mechanisms.

6 The user, of course, will continue to receive ads.

stored as part of the anonymous user profile. In addition, the NebuAd service does not have narrowly-defined segments. Finally, the anonymous profile identifier is the result of multiple encryptions, and based on multiple data elements including the hashed IP address.

8. There is no connection or link between the ISP's registration data systems and NebuAd. That means that no user-specific data is exchanged between NebuAd and ISP data systems. This boundary is preserved further and inadvertent disclosure is prevented because NebuAd immediately performs a one-way encryption of the IP address and other anonymous user identifiers used within the NebuAd system.

9. NebuAd installs no applications on users' computers, has no access to users' hard drives, and has no access to secure transactions. As such, NebuAd does not control a user's computer or web-surfing activity in any way (*e.g.*, by changing computer settings or observing private or sensitive information).

10. NebuAd's Data Centers are professionally operated and secured. NebuAd's servers are located at secure sites with state-of-the-art protections against any intrusion, electronic or physical.

NebuAd is proud of these protections – all of which were adopted to comply with both the spirit and letter of the government's privacy paradigm – and, it continuously seeks to enhance them.

CONCLUSION

As I stated at the outset, I have spent years seeking to ensure that users have robust and transparent privacy protections. In a very real sense, NebuAd is the product of that work. It has adopted and implemented state-of-the-art privacy protections, and, equally as important, it has established a process to continuously improve on them. The Internet is a highly dynamic environment, where new technologies are constantly developed to address new challenges, and we both want and need to take advantage of them. NebuAd and its ISP partners take their responsibilities to Internet users very seriously. NebuAd looks forward to continuing to work with government policymakers as they examine online advertising and privacy issues.

MEMORANDUM

JULY 17, 2008

FROM: NEBUAD, INC.

RE: LEGAL AND POLICY ISSUES SUPPORTING NEBUAD'S SERVICES

I. Introduction to NebuAd

NebuAd is an online media company founded by Internet security experts in 2006. It provides online advertising in partnership with ISPs, using a select set of a user's Internet activities (only a subset of HTTP traffic) to construct anonymous inferences about the user's level of qualification with respect to a predefined set of market segment categories ("anonymous user profiles"), which are then used to select and serve the most relevant advertisements to that user.

NebuAd is a newcomer to the world of online advertising. This world of Internet companies includes several industry giants, behavioral advertising networks, and countless website publishers. Currently, online advertising solutions operate in many locations throughout the Internet ecosystem – from users' computers to individual websites to networks of websites. When an Internet user visits the sites of web publishers, like Yahoo! or Amazon, these sites typically collect information about the user's activities to target ads based on that information. When an Internet user conducts a search, the search company may collect information from the user's activity, which in turn may be used to improve the relevance of the sponsored search results and ads shown. When a user visits websites within an online advertising network, some of which include thousands of sites, the visits help the advertising network track the user for the purpose of serving higher-value targeted advertising. All of these activities are well-entrenched in the Internet and have become fundamental to the economic model that underpins the wide availability of content and services on the Internet today. These advertising capabilities, have proven to have mutual benefits for users, publishers – both large and small – and advertisers.

NebuAd offers a unique business model that allows ISPs to participate in the online advertising ecosystem, while not only adhering to industry-standard privacy policies but also establishing new state-of-the-art privacy protections and user choice policies that go far and beyond those used on the Internet today.

Given the background of its founders, NebuAd architected its service and its policies to adhere to very strict privacy principles. These include:

1. NebuAd's service does not collect or use PII from ISP subscribers. The entire ad optimization and serving system does not collect or use any Personally Identifiable Information (PII), nor does it collect any information from password-protected sites, web mail, email, instant messages, or VOIP traffic.

2. NebuAd stores only a set of numbers that represent the user's level of qualification for a predefined set of market segment categories ("anonymous user profiles"). NebuAd does not store raw data such as URLs navigated or IP addresses associated with an identifiable individual.

Rather, the NebuAd service constructs anonymous inferences about the user's level of qualification for a predefined set of market segment categories, and then discards the raw data that was used to create or update a user's anonymous profile. This mechanism of constructing anonymous inferences about the user's level of qualification and not storing raw data provides a strong additional layer of privacy protection that goes beyond the standards used by many Internet companies today.

3. NebuAd's ISP Partners are required to provide notice to users in advance of launch of the service. The notice, which must be direct and robust, discloses to the user that the ISP is working to ensure that advertisements shown will be more relevant advertisements, that to deliver these ads its partner creates anonymous profiles based on part of the user's web surfing behavior, which does not include the collection of PII, and that the user may opt-out of the service. For existing subscribers, the notice is required to be delivered 30 days prior to the launch of the service by postal mail, email, or both. For new subscribers, the notice is required to be placed clearly and conspicuously in the new subscriber sign-up flow and outside the privacy policy. All subscribers can opt-out at any time, and on-going disclosure and opportunity to opt-out is required to be provided within the ISP's privacy policy.

4. NebuAd and its ISP partners offer users advance and on-going choice of opting-out of the service. Users are provided with a clear statement of what the opt-out means and the way it operates. Once the opt-out option is chosen, NebuAd honors that choice and ignores the user's subsequent web surfing activity and thus does not serve the user with behaviorally targeted ads.[1]

5. NebuAd's service only creates anonymous user profiles, which contain no PII and no raw data, and its placement of ads is completely anonymous. NebuAd uses proprietary algorithms and techniques, including one-way encryption of data, so that no one – not even NebuAd's engineers who designed the system – can reverse-engineer an anonymous identifier, or the anonymous user profile associated with it, to an identifiable individual.

6. NebuAd avoids any sensitive websites or product categories. NebuAd does not track or serve ads based on visits related to adult content, sensitive medical information, racial or ethnic origins, religious beliefs or content of a sexual nature, and does not have market segment categories for illegal products.

7. NebuAd does not permit either complexity of data or narrowness of data to be reverse-engineered into PII. This protection is accomplished because anonymous user profiles are constructed by anonymous inferences about the user's level of qualification for a predefined set of market segment categories. Raw data is simply not stored as part of the anonymous user profile. In addition, the NebuAd service does not have narrowly-defined segments. Finally, the anonymous profile identifier is the result of multiple encryptions, and based on multiple data elements including the hashed IP address.

8. There is no connection or link between the ISP's registration data systems and NebuAd. That means that no user-specific data is exchanged between NebuAd and ISP data systems. This

---

[1] The user, of course, will continue to receive ads.

boundary is preserved further, and inadvertent disclosure is prevented, because NebuAd immediately performs a one-way encryption of the IP address and other anonymous user identifiers used within the NebuAd system.

9. NebuAd installs no applications of any type on users' computers, has no access to users' hard drives, and has no access to secure transactions. As such, NebuAd does not control a user's computer or web-surfing activity in any way, e.g., by changing computer settings or observing private or sensitive information.

10. NebuAd's Data Centers are professionally operated and secured. NebuAd's servers are located at secure sites with state-of-the-art protections against any intrusion, electronic or physical.

II. The Federal Wiretap Act

As a threshold matter, it is important to note that the federal Wiretap Act[2] was last amended in 1986 before the widespread adoption of personal computing and online communications.[3] When the Wiretap Act was enacted, and amended, the focus was on telephone communication and other similar technology. Case law is rich with examples of claims involving a tapped phone line.[4] Notably, these cases primarily involve direct, one-on-one communication between the parties. The content is personal to the speakers, such that if one of the parties was replaced, the communication would not contain the same content. Although secrecy or confidentiality was not expressly built into the Wiretap Act, the Act was enacted at a time when the focus was on individual communications—likely as a result of the limitations of then-existing technology.

The environment that has since evolved for online communications is markedly different. While online communications are still carried by *wire,* there are important policy distinctions between the types of communications that the Wiretap Act was enacted to address, and the types of communications present in the online environment today. Internet users are not engaged in a personal, direct conversation with non-secure website publishers.[5] Such publishers provide online content indiscriminately to all users. As stated below, even under the Wiretap Act, courts look to the circumstances surrounding a communication.[6] Yet, the evaluation of circumstances

[2] 18 U.S.C. §§ 2510-2522.

[3] The Wiretap Act was amended by the Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986). While the Wiretap Act is Title I of the ECPA, it was first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and is generally known as "Title III."

[4] *See, e.g., United States v. Foster,* 580 F.2d 388 (10th Cir. 1978) (telephone company taps phone line of user suspected of defrauding the telephone company out of long-distance charges); *United States v. Harvey,* 540 F.2d 1345 (8th Cir. 1976) (same); *United States v. Auler,* 539 F.2d 642 (7th Cir. 1976) (same).

[5] There are always exceptions to this statement, such as online purchases, encrypted communication, and other secured data transactions, but notably, these private communications are the exact types of information that NebuAd's services do not collect. NebuAd's services personalize generic content rather than intruding upon private communications.

[6] *See United States v. Amen,* 831 F.2d 373, 378 (2d Cir. 1987).

that surround a telephone communication between two parties is not analogous to an online communication between a party and a website. To date, there are no litigated decisions directly addressing the application of the Wiretap Act to a URL provided as part of a consumer's online navigations or provided via publicly available search request and response. Therefore, it is still an open question as to whether these types of communications are even covered by the Wiretap Act.[7]

Assuming, for the purposes of this memorandum, that the Wiretap Act applies to NebuAd's services, the Act expressly prohibits the intentional interception of an electronic communication[8] unless "one of the parties to the communication has given prior consent to such interception."[9] The legislative history of the Wiretap Act clearly indicates "that Congress intended the consent requirement to be construed broadly."[10] As a result, "courts have resoundingly recognized the doctrine of implied consent."[11] The Court of Appeals for the Second Circuit stated that the Wiretap Act "affords safe harbor not only for persons who intercept calls with the explicit consent of a conversant but also for those who do so after receiving implied consent."[12]

To determine whether a party has impliedly consented to an interception under the Wiretap Act, courts examine the totality of the circumstances and "imply consent in fact from surrounding circumstances indicating that the [party] knowingly agreed to the surveillance."[13] In such evaluations, courts have found that parties impliedly consented to an interception in various fact patterns. The federal district court for the Southern District of New York found implied consent when an employer circulated memoranda regarding telephone monitoring and recording.

---

[7] *See* Patricia L. Bellia, *Spyware: The Latest Cyber-Regulatory Challenge,* 20 BERKELEY TECH. L.J. 1283, 1296, 1311-12 (2005). Another law review article described the question as to whether URLs contain contents as "surprisingly difficult" and "quite murky." Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't,* 97 Nw. U. L. REV. 607, 645-46 (2003).

[8] 18 U.S.C. § 2511(1)(a).

[9] *Id.* § 2511(2)(d).

[10] *United States v. Amen,* 831 F.2d 373, 378 (2d Cir. 1987) ("Consent may be expressed or implied. Surveillance devices in banks or apartment houses for institutional or personal protection would be impliedly consented to.'" (quoting S. Rep. No. 1097, 90th Cong. 2d Sess., *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182)).

[11] *George v. Carusone,* 849 F. Supp. 159, 164 (D. Corm. 1994); *see United States v. Faulkner,* 439 F.3d 1221, 1224-25 (10th Cir. 2006) ("We are not persuaded to depart from the unanimous view of the *holdings* by our fellow circuit courts."); *United States v. Corona-Chavez,* 328 F.3d 974, 978-79 (8th Cir. 2003); *Griggs-Ryan v. Smith,* 904 F.2d 112, 118 (1st Cir. 1990); *United States v. Willoughby,* 860 F.2d 15, 19-20 (2d Cir. 1988); *Amen,* 831 F.2d at 378; *United States v. Tzakis,* 736 F.2d 867, 870, 872 (2d Cir. 1984); *Borninski v. Williamson,* No. Civ. A. 3:02CV1014-L, 2005 WL 1206872, at *13 (N.D. Tex. May 17, 2005); *United States v. Rittweger,* 258 F. Supp. 2d 345, 354 (S.D.N.Y. 2003); *Chance v. Avenue A, Inc.,* 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001); *In re DoubleClick Inc. Privacy Litig.,* 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001).

[12] *Griggs-Ryan,* 904 F.2d at 116.

[13] *Amen,* 831 F.2d at 378.

Although the party denied receiving the notice, and evidence proving such receipt was destroyed, the court determined that the party had knowledge of the monitoring and recording and impliedly consented to such monitoring and recording by continuing to use the monitored telephone lines.[14]

Similarly, a Connecticut federal district court found that employees had given their implied consent to the recording of conversations on work telephones, as many of the telephones displayed warning labels, memoranda were circulated to all employees regarding the recording of incoming and outgoing telephone calls.[15] The court stated that employees' "knowledge of the system and subsequent use of the phones is tantamount to implied consent to the interception of their conversations."[16] The Court of Appeals for the First Circuit held that repeated oral statements that all incoming telephone calls would be monitored was sufficient notice, and that the party's taking an incoming phone call was implied consent to the interception." Additionally, a Texas federal district court found that an employee consented to monitoring of Internet communications at work because the employee had signed a form stating that "Internet access should be limited to 'business use only,' and that the company 'logs and archives all incoming and outgoing data communications through its gateway system. Use of the gateway implies consent to such monitoring.'"[18]

Using the framework established by the courts, NebuAd satisfies the implied consent exception to liability for interception under the federal Wiretap Act.[19] NebuAd requires, by contract, that all of its ISP partners give subscribers notice of NebuAd's services, including the collection of anonymous information regarding subscribers' online activities, for use in advertising. This notice must be given directly, and prior to the initiation of the ISP's use of NebuAd's services. The ISP partners are also required, by contract, to alter their privacy policies accordingly. NebuAd further requires that all ISP partners provide users with an option to opt-out of NebuAd's services, initially upon receipt of the direct notice, and in an ongoing manner through the ISP's privacy policy.

---

[14] *Rittweger,* 258 F. Supp. 2d at 354.

[15] *George,* 849 F. Supp. at 164.

[16] *Id.*

[17] *Griggs-Ryan,* 904 F.2d at 117-19.

[18] *Borninski v. Williamson,* No. Civ. A. 3:02CV1014-L, 2005 WL 1206872, at *13 (N.D. Tex. May 17, 2005).

[19] Website publishers may also consent to an interception, as website publishers make web content available for any user. Such posting does not constitute an exclusive communication between the website publisher and the user, but rather it is public communication that is intended to be viewed by any number of simultaneous users. As a result, website publishers have no reasonable expectation that the communication between it and any consumer will remain private or confidential, and thus impliedly consent to the interception by a third party.

III. The Cable Act

The Cable Act[20] was enacted to protect cable subscribers' personal information. Among other things, it requires cable operators to obtain written or electronic consent from a subscriber prior to collecting any PII concerning the subscriber.[21] In addition to the limitations on the collection of subscriber PII, the Cable Act limits the disclosure of subscriber PII by cable operators.[22] The Cable Act sets out multiple standards that a cable operator must satisfy in order to disclose subscriber PII. If the disclosure is necessary for a legitimate business activity, a cable operator is not required to provide the subscriber with any notice.[23] A cable operator may disclose the name and mailing addresses of subscribers if it provides subscribers with the opportunity to opt out of such disclosure.[24] For all other disclosures of subscriber PII, a cable operator must obtain "the prior written or electronic consent of the subscriber"—essentially an opt-in standard.[25]

Notably, under the Cable Act, PII "does not include any record of aggregate data which does not identify particular persons."[26] The Cable Act does not define PII beyond this exclusion. The legislative history expressly states:

> The phrase 'to collect personally identifiable information' covers the various ways that individuals can be identified, including name, address, and social security number. It is not intended to cover the electronic collection process used to produce aggregate records that are not individually identifiable. Such aggregate records indicate how groups of subscribers—such as males or residents of a certain neighborhood—use the system, and therefore pose no perceivable privacy threat to individuals.[27]

Courts have used this legislative history as the foundation to further define the limits of PII under the Cable Act, and the limited number of litigated decisions yield findings consistent with the legislative history and the traditional definitions of PII, such as "specific information about the subscriber, or a list of names and addresses on which the subscriber is included, but does not include aggregate information about subscribers which does not identify particular persons."[28]

[20] Cable Communications Policy Act (1984), 47 U.S.C. §§ 551-561.

[21] *Id.* § 551(b)(1).

[22] *Id.* § 551(c).

[23] *Id.* § 551(c)(2)(A).

[24] *Id.* § 551(c)(2)(C)(i).

[25] /d. § 551(c)(1).

[26] *Id.* § 551(a)(2)(A).

[27] S. REP. No. 98-67, 98th Cong., 1st Sess. 28 (1983).

[28] H.R. REP. No. 934, 98th Cong., 2d Sess. 79 (1984); *see, e.g., Pruitt v. Comcast Cable Holdings, LLC,* 100 F. App'x 713, 2004 WL 1226937, at **2 (10th Cir. 2004) (quoting same language from H.R. REP. No. 934); *Scofield v. Telecable of Overland Park, Inc.*, 973 F.2d 874, 876 (10th Cir. 1992) (same); *Parker v. Time Warner Entm't Co.,* No. 98 CV 4265(ERK), 1999 WL 1132463 (E.D.N.Y. Nov. 8, 1999) (stating that collection of subscriber race, ethnicity, age, income, dwelling type, and telephone number packaged along with individual subscriber name

In *Pruitt v. Cox Cable Communications,* a 2004 case before the Court of Appeals for the Tenth Circuit, the court examined the application of the Cable Act to subscriber data stored in a converter box, which contained a "unit address" that can be matched to a billing system. The court found:

> [T]he converter box code—without more—provides nothing but a series of numbers. . . . Without the information in the billing or management system one cannot connect the unit address with a specific customer; without the billing information, even [the cable operator] would be unable to identify which individual household was associated with the raw data in the converter box. Consequently, it is the billing system that hold the key to obtaining personally identifiable information, not the converter box.[29]

Similar to the court's finding in *Pruitt,* NebuAd's service specifically complies with the Cable Act because NebuAd's service does not collect PII. Instead, using only non-personally identifiable information, NebuAd uses a select set of a user's Internet activities (a subset of HTTP traffic) to construct anonymous inferences about the user's level of qualification for a predefined set of market segment categories, which are then used to select and serve the most relevant advertisements to that user. The use of NebuAd's services certainly does not require a subscriber to opt-in—the strictest notice and consent requirement. Although not an activity conducted by NebuAd, even the disclosure of a subscriber's mailing address, widely recognized as PII, only requires that the subscriber have an opportunity to opt-out. NebuAd's service, on the other hand, does not even collect subscriber PII. Because NebuAd's service does not collect subscriber PII, there is no violation of the Cable Act.

Additionally, a 2002 FCC ruling concluded that "cable modem service, as it is currently offered, is properly classified as an interstate information service, not as a cable service, and that there is no separate offering of a telecommunications service."[30] This determination that cable interne

---

services are not classified as telecommunications services was upheld by the Supreme Court as a

and address is PII); *Nat'l Satellite Sports, Inc. v. Eliadis, Inc.,* No. 5:97CV3096, 1998 WL 695246, at *5 (N.D.Ohio Sept. 10, 1998) (holding that list identifying residential cable subscribers is PII); *United States v. Cox Cable Commc'ns,* No. 98CV118/RV, 1998 WL 656574, at *1 (N.D.Fla. Apr. 28, 1998) (quoting same language from H.R. REP. No. 934, and stating that a customer's cable billing and payment history is PII) *Metrovision of Livonia, Inc. v. Wood,* 864 F. Supp. 675, 681 (E.D. Mich. 1994) (records from a fraud detecting device used by a cable provider are not PII). Several cases also cite the legislative history referencing general privacy interests, and the capability of cable systems to collect information such as bank transactions, viewing habits, and significant personal decisions using subscriber records from the interactive cable systems. Such information may be PII if it is specifically linked to and can be used to identify individual subscribers, but not if it is information contained in an anonymous user profile. While these types of information may be general privacy considerations, of which Congress was expressly aware, Congress chose to enact the definition of PII such that it "does not include any record of aggregate data which does not identify particular persons." 47 U.S.C. § 551(a)(2)(A).

[29] *Pruitt,* 100 F. App'x 713, 2004 WL 1226937, at **3.

30 *In re Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities,* 17 FCCR 4798, 4802 (2002).

lawful interpretation of the Communications Act.[31] A recent decision by the Court of Appeals for the Sixth Circuit upheld this distinction and stated that the plain language of the Cable Act precludes its application to broadband internet services, even those provided by a cable operator.[32] Examining the application of the Cable Act, the court emphasized that as the cable provider was providing broadband internet access and not cable service, the Cable Act was inapplicable.[33]

IV. Policy Implications

NebuAd provides users with a great amount of privacy protection. Unlike many online advertising models today, NebuAd's service does not collect or use any PII. In addition, NebuAd's anonymous user profiles do not contain any original raw data, such as URLs navigated, but only consist of a set of numbers that represent anonymous inferences about the user's level of qualification for a predefined set of market segment categories. (NebuAd does retain some anonymous data for analysis and reporting.) Additionally, NebuAd is one of the only models—if not the only model—that provides users with advance notice of the nature of its services and an opportunity to opt-out *before* the service takes effect. NebuAd's service also complies with the government's consent policy on privacy as NebuAd's service does not collect any PII, and provides users with the opportunity to opt-out.[34] Finally, NebuAd's service does not observe encrypted traffic, does not observe VOIP sessions, does not store raw search queries linked to an identifiable user, and does not track users' IP addresses, thus providing an excellent set of privacy protections. Because of the privacy protections that NebuAd has incorporated into the architecture of its service, it is able to provide users with relevant advertising messages in a safe, secure, and privacy-respecting manner.

---

[31] *Nat'l Cable and Telecomms. Ass 'n v. Brand X Internet Servs.*, 545 U.S. 967 (2005).

[32] *Klimas v. Comcast Cable Commc'ns, Inc.*, 465 F.3d 271 (6th Cir. 2007), *reh'g en banc denied Klimas v. Comcast Cable Commc'ns, Inc.*, 2007 U.S. App. LEXIS 13658 (6th Cir. May 1, 2007).

[33] A few courts have applied the disclosure provisions of the Cable Act to broadband internet services in the limited context of discovery proceedings under the Federal Rules of Civil Procedure. *See, e.g., Warner Bros. Record Inc. v. Does,* No. 07-706 (RJL), 2008 WL 60297 (D.D.C. Jan. 4, 2008); *Arista Records LLC v. John Does 1-19,* 245 F.R.D. 28 (D.D.C. 2007). *But see, Interscope Records v. Does 1-7,* 494 F. Supp. 2d 388, 390 (E.D. Va. 2007) (stating that "only a government entity may obtain personally identifiable information concerning a cable subscriber pursuant to a court order," and denying an *ex parte* subpoena under the Cable Act) (internal quotation omitted). In these cases, the courts compelled ISPs to release PII of otherwise unidentifiable defendants to plaintiffs in the course of litigation unrelated to the ISPs activity. Such disclosure occurred only after the plaintiffs exhausted their ability to identify the defendants, thus requiring information from the ISPs for the suits to progress any further. *Warner Bros.*, 2008 WL 60297, at *1; *Arista Records,* 246 F.R.D. at 28-29. These cases did not recognize a right of action against the providers of broadband internet service under the Cable Act.

[34] Use of a consumer opt out is consistent with other consumer information protection statutes such as the Gramm-Leach-Bliley Act (financial Data), the Health Insurance Portability And Accountability Act (health data), the Fair Credit Reporting Act (consumer reports), the

Telemarketing and Consumer Fraud and Abuse Prevention Act (telemarketing), and the CAN-SPAM Act (email marketing)

Mr. MARKEY. Thank you, Mr. Dykes.

Our next witness, Dr. David Reed, is an adjunct professor of engineering at the Massachusetts Institute of Technology. He is affiliated with MIT's renowned media lab, where he focuses on communications technologies, and he was also a pioneer in the development early on of the Internet. We welcome you, Dr. Reed. Whenever you are ready, please begin.

STATEMENT OF DAVID P. REED, PH.D., ADJUNCT PROFESSOR, THE MEDIA LAB, MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Mr. REED. Thank you. Mr. Chairman and distinguished members, good morning. I want to thank you all for the opportunity to testify on this matter, which I think is very important. I have been involved, as you mentioned, with the Internet's design and development since 1976, when I joined the Internet project as one its architects working with Vint Cerf and Bob Kahn and many others. As one of those who designed the Internet, I feel I have a duty to those who use the Internet today and will use it tomorrow. That personal duty, rather than any commercial interest, is why I am here today.

Though we all use the Internet, let me set some context that relates to its technology and that can explain my testimony. First of all, participating in the Internet as a transport or access provider implies adherence to a set of technical protocols and standards and standard technical practices that are essential for the proper functioning of the collective Internet as a whole. These rules and practices are analogous in many ways to the rules and practices of global banking or international commerce. There is a strong distinction made in the Internet design between information needed to transport Internet datagrams, or packets, and the information that the end users request to be transported. This distinction is crucial to the scalability, innovation rate, and economic impact of the Internet, as well as playing an important role in ensuring the privacy and safety of users of the Internet and limiting liability for the companies that invest in providing the Internet infrastructure.

The speed of digital systems has changed dramatically over the last 30 years and has led to a new, innovative technology that allows the inspection of packets as they transit the Internet at full speed and in complete depth. This set of technologies, often called deep packet inspection, make it possible on a large scale to dig into the content of all end-to-end messages at almost any point in the network, do selective recording and analysis of such messages, and to modify and to inject messages into the Internet that appear to be messages from a particular source but in fact are partially the result of actions by a third party unrelated to that source and without the ability of the end-point system to detect the modifications or insertions.

These technical innovations are being packaged into applications and sold as solutions to Internet access providers and Internet transport providers by a number of vendors, notably Phorm, NebuAd, Sandvine, and Ellacoya Networks, but hardly limited to those vendors. A subset of these technologies, called deep packet inspection technologies, targeted at marketing are particularly worri-

some because they involve inspection of end-user to end-user information content, decoding that content and making of inferences about the meaning of that content and modifying the content in flight without particularly making that inference or the other activities an aspect of the agreement between the end-users on both ends.

In my testimony today I draw several conclusions that Congress may want to consider as it explores use of these technologies. First, and this is most important, that DPI technologies are not at all necessary to operating the Internet or to profitable operation of Internet operators. In fact, they actually violate long-agreed standards and principles of Internet design since the beginning, and these principles that have been around from the beginning have led to the Internet's enormous impact and continued success.

Second, DPI technologies pose major risks to the economic success of the Internet as a whole. They do so by normalizing nonstandard and risky technical activity on the part of telecom operators and broadband operators who may choose to exploit their captive customers rather than transparently deliver the communications services for which their customers have paid.

Third, that protecting themselves from the negative impact of these technologies on their private business imposes significant additional costs on the knowledgeable customers of Internet transport operators and on developers of new Internet services while at the same time exploiting the unwitting and captive customers of service providers who choose to deploy them.

Let me start off by saying, it is best to think of the Internet as a shipping service, in some sense a collection of shipping modes like airplanes and ships and railroads and so forth, that carry packages. The end-users put their information in these packages, which will be called packets, and put addressing information on the outside of the packet, and they present them to a shipping agent, who chooses a path and a set of warehouses along the way, that might be called routers, that deliver these packets. What makes deep packet inspection deep is the use of this technology to collect and modify the internal contents of these packages as if they were a high-speed X-ray technology that was able to examine packets without changing them and also high-speed manufacturing technology that can actually open up the packets, manufacture something new, stick it in, and send it along, and I think that analogy is actually very strong. Note that it is unnecessary for the carriers to look inside the packages to do their job. This separation of concerns that was built into the Internet, that of transport versus packet access, is part of the economic success of the Internet and also part of the privacy functionality that was built in from the beginning. There should be no reason to look inside these packets.

One more thing about the Internet that is different is that the Internet is constructed based on protocols or conversations between the endpoints, and these protocols are an understanding between the end-users, not the end-users and their carrier.

When DPI systems make inferences about packet contents, they do not have access to the meaning that is intended by the endpoints of those protocols, and because of that, it poses signifi-

cant risks, and with that, I will finish here and await your questions.

[The prepared statement of Mr. Reed follows:]

STATEMENT OF DR. DAVID P. REED

Adj. Professor, The Media Laboratory

The Communications Futures Program

Massachusetts Institute of Technology

Weisner Building E15-492

20 Ames Street

Cambridge, Massachusetts 02139

to

Subcommittee on Telecommunications and the Internet

Committee on Energy and Commerce

U.S. House of Representatives

Washington, DC 20515-6115

17 July 2008

Mr. Chairman and Members of the Subcommittee, I thank you for the opportunity to address you on the topic of "What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies." The subject of this hearing is an important one to the country and to society as the use of the Internet becomes, more and more, a central part of every citizen's everyday life, in commerce, political expression, and culture. For the last 35 years, I have been personally involved in developing many of the key technologies of the Internet, distributed personal computing, and information sharing that we now all take for granted.

A brief summary of my main points is in order here.

First, participating in the Internet as a transport or access provider implies adherence to a set of standard technical protocols and technical practices that have been and remain essential for the proper functioning of the world-wide Internet for all its users.

Second, there is a strong distinction made in the Internet's design between information needed for transporting Internet Datagrams, and the information the Internet carries between end-point systems attached to the Internet. This distinction has a major impact on the scalability, innovation rate, and economic impact of the Internet, as well as playing an important role in ensuring privacy and safety of the users of the Internet, and limiting liability for companies that invest in providing the Internet infrastructure.

Third, technical innovations now available at very low cost in the marketplace have started to make it possible on a large scale to dig into the content of end-point to end-point messages at almost any point in the Internet transport, do selective recording and analysis of such messages, and to modify or to inject messages into the Internet that appear to be messages from a particular source, but in fact are from a third party, without the ability of the end-point systems to detect the modifications or insertions.

These technical innovations, which might be called Realtime Packet Inspection and Realtime Packet Updating, are being packaged into applications and sold as "solutions" to Internet Access Providers and Internet Transport Providers by several vendors, notably Phorm, NebuAd, Sandvine, and Ellacoya Networks, but hardly limited to those

vendors. A subset of these technologies, called Deep Packet Inspection technologies, are particularly worrisome, because they involve inspection of end-user to end-user information content, decoding, and the making of inferences about users' personal interests, private activities, etc.

In this statement, based on my expertise and direct experience as a developer and researcher for the last 35 years, a technical and marketplace-oriented discussion of these systems, their capabilities, and the uses advocated for them by their developers and by Internet transport operators, including companies. such as cable, telephone and wireless carriers, that sell high-speed Internet access as part of a "Broadband" offering.

I focus my attention on the uses proposed for Deep Packet Inspection and systems supporting those uses that are being marketed to Broadband Internet Access Providers, since such providers enjoy a strong monopoly or oligopoly position in the Internet's actual deployment.

Following the discussion, I draw several conclusions that Congress may want to consider as it explores the use of these technologies.

First, that such technologies are *not at all necessary to operating the Internet or to profitable operation of an Internet operator*, andin fact that they actually violate long-agreed standards and principles that have been part of the Internet's design from the beginning, and which have led to its enormous impact and continued success.

Second, that deployment of such technologies pose *major risks to the economic success of the Internet* as a whole. They do so by normalizing non-standard and risky technical activity on the part of telecom operators who may choose to exploit captive customers, rather than transparently deliver the communications services for which their customers have paid.

Third, that protecting themselves from the negative impacts of these technologies on their private business i*mposes significant additional costs on the knowledgeable customers* of the Internet transport operators and on the developers of new Internet applications, while at the same time *exploiting the unwitting and captive customers* of service providers who choose to deploy them.

My background

From the title and overview of this hearing, I understand you are interested in technical issues (such as the deployment of these technologies and their potential impact on privacy), in legal issues, and in policy-related issues. Perhaps you are also interested in their impact on innovation of Internet services, and in possible technical and legislative steps that might be taken to mitigate negative impacts on society.

Other witnesses you will hear are far more qualified than I to discuss the applicable laws and the various policy implications of these technologies. My experience and knowledge is largely in the spheres of technology, architecture and applications, based on more than 35 years of activity in computer systems, Internet communications, computer security,

and computer applications design, development, and technology strategy, both in research and industry.

Separation of concerns in the Internet Architecture

Survival of the Internet requires that Internet Access Providers and Transport Providers continue to take a proper, transparent role as participants in the Internet.

Internet Access Providers (and in particular Broadband providers offering so-called high-speed Internet *access* service) do *not* create the Internet for their customers, instead they provide *access* to the larger collective system called the Internet, of which they are a small part.

The Internet itself is the "network of networks" that results from voluntary interoperability among a wide variety of Autonomous Systems – networks that are not owned by each other, and which do not even have contractual obligations to each other in most cases. All it takes to be part of the Internet as an Autonomous System is to agree to participate according to the very simple ground rules of the Internet.[1] These ground rules are directly responsible for the remarkable growth, scalability, and resilient evolution of the Internet itself, and more importantly the growth of the Internet's utility as a backbone of commerce, information exchange, and cultural growth.

The fundamental agreement among Autonomous Systems is that they collectively

---

1 The core ground rules of the Internet were laid out in the original design begun in 1975 by Vint Cerf and Bob Kahn of ARPA. I participated in that original development of, and have since written extensively about, these Internet ground rules.

provide each *host*, that is each computer that is connected to any of the many Autonomous Systems, the ability to send and receive small messages called Internet Datagrams, to any of the other hosts on any Autonomous System in the Internet. I avoid defining a whole collection of technical terms by suggesting that you view these Internet Datagrams as *envelopes* containing messages from one host to another on the Internet. The envelope is stamped on the outside with *only* four things:

- an address,
- a return address,
- a protocol identifier, and
- some marks that indicate how the message is handled as it is carried through the network.

The content of each message is held "inside the envelope." This content is meant to be meaningful only to the sending and receiving hosts, while the envelope exterior is meant to contain all the information needed for that content to be carried from the source to the intended destination.

As a condtion of participation in the Internet, each Autonomous System must agree to provide "best efforts" delivery of these Internet Datagrams (envelopes) without reading or changing their contents – that is, a sender posts an envelope with its return address and a specified destination address, and it expects that the envelope will be routed

through the network and delivered eventually to the specified address.

The concept of "outside the envelope" and "inside the envelope" is a reflection of much effort on the part of the Internet designers when the Internet was first created, and is acknowledged by many as one of the two or three reasons why

1. the Internet has scaled by many orders of magnitude over the past 30 years without a fundamental architectural change,
2. the Internet easily evolved to incorporate technological innovations in digital transport such as optical fiber switching, WiFi, 3G cellular, etc., and
3. the Internet has catalyzed the invention of a wide variety of consumer and business content distribution, communications applications and resource sharing services that range from the World Wide Web to Instant Messaging, Social Networking, business process outsourcing, etc.

It is worth thinking about these points carefully. The core idea of the Internet Datagram is a form of radical simplicity. All the Internet does is carry envelopes of a standard form – in a sense just like the post office.

Scaling: To make a faster Internet, all one need do is process the envelopes faster. To make a larger Internet, all one need to do is improve the processing units that use the address on each envelope to sort the envelope into one of the many outgoing paths from each routing point.

Technology evolution: To incorporate a new technology like optical fiber into the network, all one need do is find a way to put the bits of an Internet Datagram into a sequence of light pulses that travel down the fiber. There are numerous technical details involved in doing so, which are the province of companies like Cisco and other Internet technology providers.

Application/Service innovation: To build a new application or service, all one need do is write a program to run on standard computer servers and standard personal computer clients that communicates using a *protocol* based on Internet Datagrams. A protocol is a set of conventions or rules that specify messages that are sent inside the envelopes, in particular saying what the messages mean to the recipient, and what actions the recipient of a message should take upon the receipt of a message. Each new kind of application or service on the Internet is created by inventing a new protocol.

The Internet transport infrastructure does its job without needing to understand or to generate protocol-required messages in Application or Service protocols. Therefore, applications and services can be invented and deployed without having to negotiate consent or ask for favors from the infrastructure. The infrastructure – all of the AS's – does the same thing for *every* application: transport the envelopes.

It is this separation of concerns that is the essence of the success of the Internet.

Real-Time Packet Inspection and Real-Time Packet Updating

Because silicon computing technology has followed Moore's Law, with the size and

performance of computers improving by a factor of four every three years, the ability to process information carried in messages has improved drastically in the last 35 years. That means that today's silicon chips can, in principle, examine and process a message of a particular size about *8 million* times more efficiently than the silicon chips at the time I began working on research computer networks in 1973.

The result of this technology evolution is that it is now quite reasonable to construct specialized computing devices that can scan tens of millions or even billions of bits of data per second passing through a network switch, running complex pattern matching and decision algorithms on each Internet Datagram during the time the Internet Datagram is received into a network switch and transmitted out over a fiber or cable to the next switch on the path between the source and destination. Since each Internet Datagram is stored in specialized buffer memory before being retransmitted, specialized devices can put put selected Datagrams aside for complex processing and modification before forwarding them on to the destination as desired.

When such devices are produced in volume, the cost per device can be made quite small. Such devices capable of monitoring, decoding, and matching Internet Datagrams are a natural result of the evolution of high performance Internet switches, but are capable of far more general operations than delivering datagrams to their intended destination.

These devices are what I call Real-Time Packet Inspection and Real-Time Packet Updating systems.

Deep Packet Inspection: Inspecting "inside the envelope"

As mentioned earlier, a core element of the Internet architecture is that the content "inside the envelope" of an Internet Datagram is not to be read or modified by any of the AS's that carry the Internet Datagram from source end-point to destination end-point.

The term *Deep Packet Inspection* was invented to describe real-time packet inspection systems that inspect and use content from "inside the envelope." Since that content is intended only for the destination end-point, it is never necessary for AS's to inspect or analyze such content to perform their function of delivery, just as it is never necessary for the Post Office to inspect the contents of a First Class Letter in order to properly deliver the letter to its destination.

Nevertheless, a variety of companies have developed systems based on Deep Packet Inspection and have begun to market them to network transport operators and others. These systems are marketed for a variety of applications, which I will discuss below.

Often lumped into the category of Deep Packet Inspection are other techniques that involve real-time modification of the content "inside the envelope" of Internet Datagrams, and even creation of Internet Datagrams with content not requested by the source whose address appears on the "outside of the envelope".

Though some call this modification or synthesis of Internet Datagrams "forgery" of Internet Datagrams, the legality of performing such operations involves non-technical, legal issues where I am not an expert.

Instead I will point out that the Internet Architecture, as defined by the IETF and other bodies who oversee the Internet's evolution, *neither requires nor allows* Internet Datagrams to be modified or created by AS's in this manner. I will discuss the implications and risks to end-users and the Internet as a whole of such action further below.

Thus Deep Packet Inspection goes against the separation of concerns that has been a hallmark and generator of the Internet's success.

Proposed uses of Deep Packet Inspection

When there is a technical capability of the sort we are discussing that is relatively inexpensive and quite powerful, there are many potential applications. Let me briefly list some of the potential applications where this technology appear to generate interest.

Surveillance by law enforcement and intelligence collection agencies is an application area where there is strong technical value of Deep Packet Inspection, though there is no need for updates or insertion. This application includes highly selective capture and recording of selected packets – often called "lawful intercept" by telecommunications carriers – and broad data recording and capture – often called "data mining." Since this is typically a government function, I believe this application is out of scope for this hearing, but CALEA apparently does require that Internet operators enable the application of some forms of Deep Packet Inspection for this purpose.

Another category of application that has been marketed by vendors such as Sandvine is

"traffic management" by Internet Access Providers, which was the subject of recent hearings by the FCC, where I have testified in regard to the use of such technology by Comcast to disrupt certain categories of traffic on its Internet Access Service. That particular use involves inspection "inside the envelope" of Internet Datagrams and the technique of injecting packets that appear to be generated by the TCP protocol software as if they were sent by end-points intending to cancel the connections, with the result being that certain traffic, including BitTorrent traffic carrying large files, is disrupted severely.

Given that advertising and marketing play a large and extremely valuable part in electronic commerce using the World-Wide Web and electronic messaging, the application of such technology to analyze user behavior in order to target marketing more precisely is a hot application area.

At least two separate companies, NebuAd and Phorm, have developed systems that use Deep Packet Inspection that can be deployed within any AS to scan and analyze all Internet Datagrams, both inside the envelope and outside the envelope. The results are stored in a local database, or sent to a centralized database, recording patterns of access that are analyzed to determine each user's interests, then saved. Each of these systems also provides the ability to modify or synthesize the content of Internet Datagrams containing user-requested information from vendors and information services such as Amazon, Google, and even small business websites in order to insert advertising on the

behalf of the access provider.

It is important to note that the interception of content and modification of returned content in these systems is done under the control of the Internet Access network that installs NebuAd or Phorm. The interception and modification is beyond the control of either the consumer/user or the vendor/service who are the two primary parties. While these systems may incorporate "opt-out" provisions, privacy safeguards of the databases they construct, etc., it is important to know that their service is not a normal or accepted part of the Internet Architecture.

Another proposed use of Deep Packet Inspection technology is the scanning of traffic for undesirable, unwanted, or unlawful content. It has been proposed that Deep Packet Inspection can be used to detect unlicensed distribution of copyrighted content such as digitized movies, unwanted bulk email (spam), computer viruses, pornography, child pornography, etc. between witting and unwitting endpoints. There have been proposals that colleges, universities, and businesses, as well as Internet AS's be mandated to install such systems either by law or by legal precedents making them liable for carrying such traffic between end-points.

Finally, Deep Packet Inspection technologies are used for monitoring the performance and health of Internet operations. With such diagnostic tools, engineers can measure activity on the network, plan for facilities investments, etc. Such tools can be quite helpful in finding faults within the network and predicting areas of growth that support

AS's

This list of potential applications covers the applications of which I am current aware. Since Deep Packet Inspection is a general-purpose capability grounded in Moore's Law and tied to the advancement of the technologies already built into the Internet switching gear being sold to customers, it will always be tempting for entrepreneurs to invent new applications for this general approach of reading, capturing, modifying, and injecting Internet Datagrams as they flow through the network.

Risks associated with Deep Packet Inspection

As noted earlier, a very useful way to think about the how the Internet is structured is to imagine Internet Datagrams as packages or envelopes carried by a sequence of third party delivery services from and end-point computer to another end-point computers. In this analogy, the Autonomous Systems are like individual package delivery services, such as UPS, FedEx, DHL, Yellow Trucking, etc. On the "outside" of packages is a set of labels that are intended for use in forwarding the package on to its destination. A carrier that picks up a package may transfer the package from one carrier to another, choosing the path best suited for timely delivery of the package to its destination.

In this analogy, Deep Packet Inspection technologies can be accurately thought of as devices that are placed in trucks, airplanes, warehouses, etc. of the various forwarding services that very quickly and efficiently examine the contents of the packages (perhaps by X-ray, by actually opening the package and taking pictures of its content, ...), record

the results of that examination in a database held by a third party, and analyze all of the information captured using statistical methods. This information is then used to select particular packages for special handling, discarding, or re-routing, to change, delete, or insert contents into the packages, and to create packages that *appear to be* from a particular source, but which are in fact generated by within the network itself.

A useful example in this analogy would be if all of the packages you ship and receive through an independent shipping agent (such as Mailboxes, Etc.) were scanned, and the contents used to understand your buying habits, and further that the shipping agent had a contract with various companies to insert or replace the contents of your packages with "improved" contents.

I suspect that there may be some users who would be delighted to receive items they did not request in their packages, and that merchants might be happy to find that the computer that they ship to a customer is magically "improved" or replaced by an upgraded model along the way.

However, the normal understanding in dealing with shipping agents is that the contents of packages are not to be examined, studied, reported to third parties, replaced or modified according to the desires of third parties.

There is another problem, however, that to me is more problematic. That is that unlike the shipping agent example above, the Internet is based on end-to-end protocols that are more complex than simply the delivery of packages. In these protocols, the contents of

packages contain requests for remote end-point service systems to perform actions on the user's behalf, which generate responses and then more requests. As an example, consider a user who coordinates his or her finances among of number of banks and brokers via protocols carried in these packages. He or she might first send a deposit to one account, then request a transfer to another bank once the deposit is confirmed, and then send instructions about investing the money to the second bank. This sequence of steps is called a protocol.

What Deep Packet Inspection technologies attempt to do is to *second-guess the intent* of the end-users of these services (the investor and the bank), to draw inferences about the intent of those protocols and to modify (hopefully safely) the packages without causing harm to the protocol transactions.

The source of the problem is that *vendors of Deep Packet Inspection systems cannot presume to understand, merely by looking at the contents of packages what they actually mean or intend to happen at the source and endpoint.*

This is the real risk: an service or technology *unnecessary to the correct functioning of the Internet* is introduced at a place where it cannot function correctly because it does no know the endpoints' intent, yet it operates invisibly and violates rules of behavior that the end-users and end-point businesses depend to work in a specific way.

As a simple example, I cannot send email from many hotels, because of a Deep Packet Inspection technology deployed in many hotels' Internet Access service. That service

(intended to block spammers who might operate from hotel rooms) intercepts my packages intended for my email server, and responds, pretending to be any and all destination email servers, offering to accept my email messages on behalf of the recipients, which it will then scan for evidence of viruses and spam. In my case, I use a special secure, encrypted email delivery service that is more secure than most, so my mail sending software recognizes the deception and refuses to deliver the mail to the deceptive provider that requires me to send my mail "in the clear" so it can be scanned.

Hotel providers claim that they are "doing a service" by blocking spam, but in doing so they reduce my own personal security, both by requiring that my mail be sent in the clear, and by introducing the risk that my mail will be scanned and modified by an interceptor I cannot easily avoid. Some hotel providers even claim that they are legally *mandated by liability law* to inspect my email that originates through the hotel system.

In addition, if my email requests happen to involve the transmission of messages that the operator *deems to be spam*, my message, which may be quite important to my business, will be blocked without my knowledge or any possibility to appeal the erroneous inference.

That example, though a simple example, captures the risks that I want to highlight:

- Systems based on Deep Packet Inspection work by drawing inferences from packet contents that are not intended to be understood by anyone other than the destination host. Deep Packet Inspection systems *cannot* reliably determine the

intent or meaning of those Internet Datagrams.

- Deep Packet Inspection systems work by deliberately interfering with end-to-end communications, but by definition attempt to deceive the endpoint systems about what the original Internet Datagrams contain. The endpoints cannot tell if such systems have either captured their content information, or modified or created information that was not sent or intended by the author of the Internet Datagram.
- Deep Packet Inspection systems cannot be made reliable, either in their inference or in their actions.

Impacts on Users and Services Built on the Internet

In order to block interception and modification of the contents of their Internet Datagrams, end-point hosts can take steps such as encrypting contents of packets, using digital signatures, and choosing providers that vow not to scan or modify packets.

Besides raising the cost of using the Internet for existing and new applications, there are three problems with this.

First, existing applications have been designed with the expectation that Deep Packet Inspection is not a legitimate activity by a service provider.

Second, there is only one Internet, which consists of many Autonomous Systems. Choosing a different point of connection cannot, given the nature of the Internet, ensure that all users one might want to send Internet Datagrams to have successfully chosen

providers that have not deployed Deep Packet Inspection systems that scan or modify Internet Datagrams. Thus, consumer choice is not an option. Since the risks of incorrect operation of Deep Packet Inspection can disrupt critical protocols (including protocols yet to be deployed or invented), mere consumer choice may not be enough to fix the problem.

Third, encryption from end-to-end, while a potential solution, has public policy implications. This committee and Congress have gone through those issues many times. I personally would like to see all communications activities fully protected by strong encryption, but I fear that reaching that point will encounter many obstacles. If the primary problem the encryption is to deal with is an unnecessary technology such as Deep Packet Inspection, a simpler solution would be to bar the use of Deep Packet Inspection systems.

SUMMARY STATEMENT OF DR. DAVID P. REED

Massachusetts Institute of Technology

Weisner Building E15-492

20 Ames Street

Cambridge, Massachusetts 02139

17 July 2008

In Re: What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies

The main points of my statement to the committee hearing are as follows:

First, participating in the Internet as a transport or access provider implies adherence to a set of standard technical protocols and technical practices that have been and remain essential for the proper functioning of the world-wide Internet for all its users.

Second, there is a strong distinction made in the Internet's design between information needed for transporting Internet Datagrams, and the information the Internet carries between end-point systems attached to the Internet. This distinction has a major impact on the scalability, innovation rate, and economic impact of the Internet, as well as playing an important role in ensuring privacy and safety of the users of the Internet, and limiting liability for companies that invest in providing the Internet infrastructure.

Third, technical innovations referred to as Deep Packet Inspection make it possible on a large scale to dig into the content of end-point to end-point messages at almost any point in the Internet transport, do selective recording and analysis of such messages, and to modify or to inject messages into the Internet that appear to be messages from a particular source, but in fact are from a third party, without the ability of the end-point systems to detect the modifications or insertions.

These technical innovations, which might be called Realtime Packet Inspection and Realtime Packet Updating, are being packaged into applications and sold as "solutions" to Internet Access Providers and Internet Transport Providers by several vendors, notably Phorm, NebuAd, Sandvine, and Ellacoya Networks, but hardly limited to those vendors. A subset of these technologies, called Deep Packet Inspection technologies, are particularly worrisome, because they involve inspection of end-user to end-user information content, decoding, and the making of inferences about users' personal interests, private activities, etc.

I draw several conclusions that Congress may want to consider as it explores the use of these technologies:

First, that such technologies are *not at all necessary to operating the Internet or to profitable operation of an Internet operator*, andin fact that they actually violate long-agreed standards and principles that have been part of the Internet's design from the beginning, and which have led to its enormous impact and continued success.

Second, that deployment of such technologies pose *major risks to the economic success of the Internet* as a whole. They do so by normalizing non-standard and risky technical activity on the part of telecom operators who may choose to exploit captive customers, rather than transparently deliver the communications services for which their customers have paid.

Third, that protecting themselves from the negative impacts of these technologies on their private business i*mposes significant additional costs on the knowledgeable customers* of the Internet transport operators and on the developers of new Internet applications, while at the same time *exploiting the unwitting and captive customers* of service providers who choose to deploy them.

Mr. MARKEY. Thank you, Dr. Reed, very much.

And our next witness is Mr. Bijan Sabet. He is a general partner at Spark Capital, a venture capital fund focused on the media, technology, and entertainment industries. Mr. Sabet has led numerous investments in startup technology companies and has worked for Apple Computer. We welcome you, sir. Please begin.

STATEMENT OF BIJAN SABET, GENERAL PARTNER, SPARK CAPITAL

Mr. SABET. Thank you, Mr. Chairman and Ranking Member Stearns, for the opportunity to testify today. I am from Boston, but I am a Yankee fan, so please don't hold that against me.

Mr. MARKEY. Thank for you helping us to win the All-Star Game so the final game in the World Series can be at Fenway Park. We thank all the Yankee players for helping us.

Mr. SABET. All right. Well, my name is Bijan Sabet. I am a general partner at Spark Capital based in Boston, Massachusetts. Spark Capital, as you said, is a venture capital firm, and we are managing and investing in excess of $620 million. We make direct investments in early-stage companies, in the Internet, media and technology industries. To date, we have made 25 investments in this area. We are being very aggressive, and it probably will be over 30 companies next year, and our companies are generating real value, real technology, real revenue, and real jobs.

Deep packet inspection is something I care a great deal about, as well as my partners, and will directly impact the Internet ecosystem, which is beginning to thrive. As a technology, I believe there is nothing wrong with DPI. It is a significant technology breakthrough, and up until fairly recently, DPI could not be achieved at scale at any reasonable cost. So I don't have any criticism about NebuAd specifically or any vendors that have DPI technology. The issue at hand is how DPI is implemented and how it is managed. It is less about whether these vendors have certain features or not. It is about what can and cannot be done with DPI.

So to start off, just a quick definition of DPI. I think Wikipedia cites it well when it states that deep packet inspection, or sometimes complete packet inspection, is a form of computer network packet filtering that examines the data or header form of packets as it passes an inspection point searching for non-protocol compliance, viruses, spam, intrusion, or predefined criteria to decide if the packet can pass or if it needs to be routed to a different destination or for the purpose of collecting statistical information. This is in contrast to shallow packet inspection, usually just called packet inspection, which just checks the header portion of a packet.

So we need to understand the impact of DPI. DPI can provide significant economic and consumer benefit if used correctly, but it can cause significant problems if used incorrectly. There are really two issues to consider. One is privacy, which I think Dr. Reed and Ms. Cooper summarized very well, and I largely agree with them. I think the other issue is how DPI relates to the open Internet.

My interest in providing this testimony is less about privacy per se and more about DPI's impact on the open Internet and the Internet ecosystem. The important question is, do we want an open Internet or a closed Internet, where ISPs can decide what content

and applications should be available? Specifically, should ISPs decide if a competitor's product will be able to flow to the home or not? That is just one example. That is the topic I would very much like to discuss with all of you.

We have all seen the explosion and growth of the Internet in the business and consumer markets. It has been a large success. High-speed Internet to the home has fueled this growth, with applications such as Apple iTunes, Google's YouTube, joint ventures such as Hulu by NBC and Fox. This world is moving quite fast. Consider Netflix, which was once only a mail order DVD rental company. It is now streaming full-length movies on demand over the Internet. Thus, the impact of high-speed Internet has just begun. Hundreds and hundreds of startups by venture capitalists like myself are investing in this space, because entrepreneurs and investors alike see the value in the open Internet.

And while the Internet is growing rapidly and investors are pouring money into the new ideas and new opportunities and new businesses and new jobs funding new technology, U.S. broadband penetration is not as good as it should or could be. The chart I provided in my testimony is from the Organization for Economic Cooperation and Development, and it shows that as recently as 2007, the United States was ranked 15th in terms of broadband penetration, so we are behind many countries such as Canada, France, Germany, Korea, Iceland, Denmark, etc.

The other interesting note here is there is not a very good definition of what high-speed or broadband access is. Up until recently, broadband in this country was defined as 200 kilobits per second, which by today's standards would not be considered high-speed data.

Hopefully, we would all believe that it is in our economic self-interest to explore ways to make the United States a leader in high-speed Internet. We need more applications and consumer benefit to increase broadband adoption in the United States. We need lower cost of service, and we need a national coverage plan. The open Internet and growing broadband penetration are the key economic drivers of the Internet ecosystem and economy from my perspective as a venture capitalist.

And that brings me back to the topic of DPI and its potential negative impact on the open Internet. Many are calling this topic of the open Internet and DPI a discussion around network neutrality, which is the principle about an open network with restrictions potentially only for legal purposes. The danger is that ISPs would and could use DPI as a way to turn off or slow down third-party applications or third-party services. Recently, the FCC discovered that this was happening with a large ISP and a third party. In this case, it was a startup called BitTorrent.

We don't have to imagine what would happen if ISPs continue to do this. We have only to look at the mobile industry. Many venture capital firms like mine are investing in the mobile space, but cautiously compared to the open Internet sector. Why are we doing that? Well, consider the biggest success startup stories in the last 15 years, and the vast majority of them were companies that were a result of the open Internet ecosystem. Ask yourself, which start-up companies have created billions of dollars of value and thou-

sands of jobs in the mobile space? There are few, but these examples are far less than those that are coming from the open Internet ecosystem. That is because the mobile Internet, the mobile system, is closed. There is no ecosystem in the United States. Carriers are able to block Web sites. They are able to block third-party applications and services, and as a result of this closed network, most consumers in the United States are not signing up for Internet access on their mobile phones, which means a less attractive market for innovation, a less attractive market for investors, a less attractive market for entrepreneurs——

Mr. MARKEY. Mr. Sabet, could you summarize, please?

Mr. SABET. So we need a healthy and growing broadband market in the United States. I would like to see our cable companies and telephone companies thrive and grow their businesses with new technology and capabilities and new applications. New applications will help them sell services, too, but it should not be at the consumer's expense or the Internet ecosystem's expense.

Thank you for your time and consideration.

[The prepared statement of Mr. Sabet follows:]

To: Committee on Energy & Commerce, US House of Representatives

Fr: Bijan Sabet

Date: July 18, 2008

Re: Deep Packet Inspection Testimony

My name is Bijan Sabet and I'm a General Partner at Spark Capital. Spark Capital is a venture capital firm based in Boston, MA. We are managing & investing $620M.

We make direct investments in early stage companies in the Internet, media and technology industries. To date we have made 25 investments in this area. It will most likely be over 30 companies by next year. Our companies are generating real value, real technology, real revenue and real jobs.

Deep Packet Inspection is something that I care a great deal about and will directly impact the Internet ecosystem which is beginning to thrive.

As a technology itself, there is nothing wrong with DPI. It's a significant technology breakthrough. Up until fairly recently, DPI could not be achieved at scale at any reasonable cost.

The issue about DPI is how it's implemented. How it's managed.

What is Deep Packet Inspection?

Wikipedia cites it well when it states (http://en.wikipedia.org/wiki/Deep_packet_inspection):

> "Deep packet inspection (DPI) (or sometimes complete packet inspection) is a form of computer network packet filtering that examines the data and/or header part of a packet as it passes an inspection point, searching for non-protocol compliance, viruses, spam, intrusions or predefined criteria to decide if the packet can pass or if it needs to be routed to a different destination, or for the purpose of collecting statistical information. This is in contrast to shallow packet inspection (usually called just packet inspection) which just checks the header portion of a packet.
>
> Deep packet inspection (and filtering) enables advanced security functions as well as Internet data mining, eavesdropping, and censorship."

We need to understand the impact of DPI. DPI can provide significant economic and consumer benefit if used correctly.

But it could cause significant problems if used incorrectly.

Issues to consider:

1. Privacy. What should be disclosed and how.
2. Open or closed Internet.

Privacy.

Companies that benefit from the use of DPI should disclose to consumers what they are doing, how they are doing it and what they will do with information acquired by DPI.

My interest in providing this testimony is less about privacy and more about DPI's impact on the open Internet & the Internet ecosystem.

The important questions is: Do we want an open Internet or a closed Internet where ISPs can decide what content & applications should be available. As an example: should ISPs decide if a competitors product will be able to flow through to the home or not.

That is the topic I want to discuss with all of you.

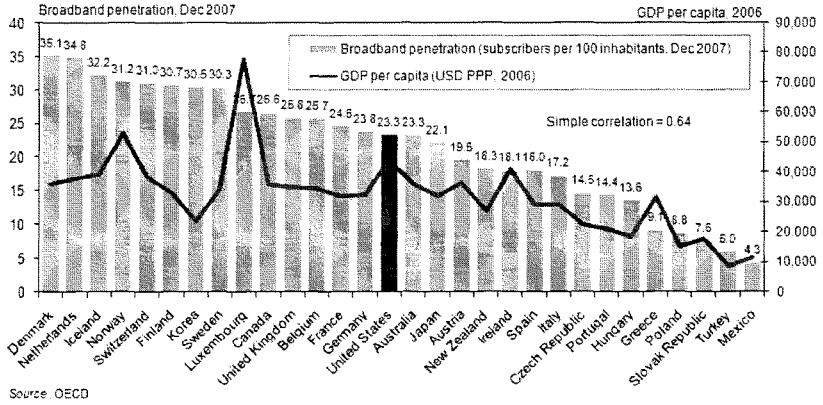
We all have seen the explosion and growth of the Internet in the business and consumer markets. It has been a large success. High speed Internet to the home has fueled this growth with applications ranging from Apple's iTunes, Google's YouTube, NBC/FOX joint venture Hulu. The world and growth is moving fast. Consider Netflix, which was once only a mail order dvd rental company, is now streaming full length movies on demand over the Internet to their subscribers. The impact of high speed Internet has only just begun. Hundreds and hundreds of startups are being funded

by venture capitalist because entrepreneurs and investors see the value in the open Internet.

And while the Internet is growing rapidly and investors are pouring money into new ideas, new opportunities, new businesses, new jobs & funding new technology, US broadband penetration isn't as good as it should or could be.

This chart is from The Organization for Economic Co-Operation and Development (OECD) and shows that in 2007 the United States was ranked 15th in terms of broadband penetration.

OECD broadband penetration and GDP per capita



Source: OECD

Hopefully we would all agree that it is in our economic self interest to explore ways to make the United States a leader in high speed Internet access. We need more

applications and user benefits to increase broadband adoption in the United States. We need lower costs of service. We need national coverage.

The open Internet and growing broadband penetration are the key economic drivers of the Internet ecosystem and economy from my perspective as a venture capitalist.

And that brings me back to the topic of DPI and it's potential negative impact on the open Internet. Many are calling this topic of the open Internet a discussion around network neutrality, which is the principle about an open network with restrictions only for legal purposes.

The danger is that ISPs would & could use DPI as a way to turn off or slow down 3rd party applications or 3rd party services. Recently the FCC discovered that this was happening with a large ISP and a 3rd party. In this case a start up company called BitTorrent.

We don't' have to imagine what would happen if ISPs did this. We have only to look at the mobile industry. Many venture firms like mine are investing in mobile but cautiously compared to the open Internet sector.

Why? Consider the biggest success startup success stories. The vast majority are open Internet companies.

What startup companies have created billions of dollars of value and thousands of jobs in the mobile space. There are some but examples are far less than the open Internet ecosystem. That's because the mobile Internet is closed for the most part in

the United States. Carriers are able to block web sites and 3rd party applications and services. As a result of this closed network, most consumers in the United States aren't signing up for internet access on their mobile phones which means a less attractive market for innovation and the cycle spins downward.

If ISPs do the same for the high speed Internet market to the home it would have a significant long term impact on the economy. Venture firms like ours would look for investments in other areas that had fewer restrictions. Less VC funding means less startups, which means less businesses, less jobs, less innovation. Not a pretty picture.

We need to a healthy and growing broadband market in the United States. I want our cable companies and telephone companies to thrive and grow their businesses with new technology and capabilities. New applications will help them sell more services too. But it should not be at the consumers expense or the internet ecosystems expense.

We are in the early days of the open Internet. We need to support the open ecosystem and support it. Not get in the way.

Thanks for your time & consideration

Regards,

Bijan Sabet

Mr. MARKEY. Thank you, Mr. Sabet, very much.

Our final witness, Mr. Scott Cleland, is a founder and President of Precursor LLC, a research and consulting firm. He blogs and speaks frequently on issues related to the Internet economy. We welcome you, sir.

STATEMENT OF SCOTT CLELAND, PRESIDENT, PRECURSOR LLC

Mr. CLELAND. Mr. Chairman and members, thank you for the opportunity to testify. I am Scott Cleland, President of Precursor LLC, an industry research consulting firm. Full disclosure: I am also chairman of NetCompetition.org, which is a pro-competition e-forum funded by telecom, cable, wireless, and broadband companies. My testimony today reflects my personal views, not those of my clients.

I believe the real problem here is not necessarily the prospect of deep packet inspection but the current patchwork of U.S. privacy laws, a lack of holistic approach to Internet privacy, and selective oversight of privacy problems. I believe they all combine to create perverse incentives for some companies to arbitrage privacy laws and to push the privacy envelope. As a result, abuse of privacy is among the most serious problems that face users of the Internet. I believe the lack of a holistic, comprehensive, and balanced approach to privacy law and oversight is a serious threat to Americans' privacy.

Now, broadband companies have long been subject to strict privacy laws, sections 222, 551, and the ECPA. These laws create serious consequences for the misuse of private information without a user's permission. Consequently, broadband companies have developed extensive policies, practices, and procedures to respect users' privacy and protect private information. Now, the subcommittee's oversight of deep packet inspection for advertising purposes is very appropriate, and existing laws, I believe, appear to cover these practices.

What I am concerned about is that the selective oversight of only broadband privacy matters fosters a blind eye to the arbitrage of privacy laws by companies like Google, Yahoo, and others. This creates perverse incentives for companies not covered by U.S. privacy laws to push the envelope on privacy to gain competitive advantage. Now, Americans' privacy should not be an unrestricted commodity to sell to the highest bidder or to gain competitive advantage. Specifically, I am troubled with the broadband focus of this hearing, because privacy is a cross-cutting, big picture issue that knows no boundaries between the application, the transport or the content layers of the Internet. By turning a blind eye to Google, which I believe is the worst privacy offender on the Internet, it is systematically invading and abusing Americans' expectation of privacy.

Now, my feeling about this hearing is, it is here to create fear about what broadband providers could do while it is ignoring what Google and others are actually doing today that hurts Americans' privacy. Now, the irony here is the worry about whether broadband privacy blinds are perfect when the Internet house has no privacy walls at all. Let us consider the depth and the breadth of the inti-

mate blackmailable information that Google already collects on you: everything you have searched for; everywhere you have gone on the Web; what you watch through YouTube; what you read through Google news Feedburner blogger; what you say in your e-mails; what you produce in Google Docs; what your family and friends look like through Picasa; your medical conditions and history, through Google Health; your purchase habits through Checkout; your call habits and voice prints through Google Talk; your travel habits and interests via Google Maps; your interest in places through Google Earth and StreetView; your personal information through Orca, G-mail, Checkout, and otherplaces where you go and hang out, which will come through Android; where you will be or where you work through Google Calendar.

The scale and scope of Google's unauthorized Web surveillance, and I use that term, that should be as concerning to people as deep packet inspection, unauthorized Web surveillance, and I commend the chairman today in the Washington Post for talking about this. He said surreptitiously tracking individual users' Internet activity cuts to the heart of consumer privacy. I couldn't agree more with the chairman on that. So this is truly Orwellian Big Brother stuff. While Google is not the government, all this information that Google collects is on Google's servers, it is not on your PC where you own it, and it is available to the government via subpoena.

So in sum, information is power. Power corrupts. Absolute power corrupts absolutely. Google's market power over private information is corrupting Google. Just like former FBI Director J. Edgar Hoover was corrupted by his power and mastery of personally sensitive information, Google's unprecedented arbitrage of privacy law combined with its exceptional lack of accountability is fast creating this era's privacy-invading, unaccountable equivalent, which I call J. Edgar Google. Remember the timeless insight: Those who don't learn from the past are doomed to repeat it.

Thank you for the opportunity to testify.

[The prepared statement of Mr. Cleland follows:]

Testimony of Scott Cleland, President, Precursor LLC
"The Blind Eye to Privacy Law Arbitrage by Google -- Broadly Threatens Respect for Privacy"
Before the House Energy & Commerce Subcommittee on Internet Hearing, July 17, 2008

I am Scott Cleland, President of Precursor LLC, an industry research and consulting firm. I am also Chairman of NetCompetition.org, a pro-competition e-forum funded by telecom, cable and wireless broadband companies. My testimony today reflects my own personal views and not the views of any of my clients.

The current patchwork of U.S. privacy laws, the lack of a holistic approach to Internet privacy, and selective oversight of privacy problems – have combined to create perverse incentives for some companies to: arbitrage privacy laws and push the privacy envelope. As a result, invasion/abuse of privacy is among the most serious problems users face on the Internet. **The lack of a holistic, comprehensive and balanced approach to privacy law and oversight is a serious threat to American's privacy**.

Broadband companies, (telecom, wireless and cable) have long been subject to strict privacy laws (sections 222, 551 & the ECPA), which created serious consequences for the misuse of personally identifiable information without a user's permission. Consequently, broadband companies have developed extensive policies, procedures and practices to respect users' privacy and protect personally identifiable information. This Subcommittee's oversight of experimentation by some, with "deep packet inspection" for advertising purposes, is entirely appropriate. Existing laws appear to cover these practices so oversight by Congress is expected.

I am concerned however, that selective oversight of only broadband privacy matters fosters a blind eye to arbitrage of privacy laws by application companies like Google, Yahoo and others. This creates perverse incentives for companies not covered by U.S. privacy laws to push the envelope on privacy to gain competitive advantage. **Americans' privacy should not be an unrestricted commodity to sell to the highest bidder or to gain competitive advantage**.

Specifically, I am troubled with the selective broadband focus of this hearing, because privacy is a cross-cutting, big picture issue that knows no boundaries between the access, application and content "layers' of the Internet. To add balance and to focus on the most serious threat to Americans' privacy, I humbly suggest the Subcommittee hold another hearing entitled: "*Why Google Knows Everything About You: Unauthorized Web Surveillance and Privacy Law Arbitrage.*"

By turning a blind eye to what Google, the worst privacy offender on the Internet, is doing to systematically invade and abuse Americans' expectation of privacy, Congress is perversely encouraging copycat behavior by "deep packet inspection" advertising entrepreneurs who see that there is a huge privacy double standard to arbitrage. Companies like NebuAd are essentially just following the privacy-arbitrage leader – Google.

To illustrate my point of the extreme privacy law arbitrage that is occurring in the U.S. marketplace today, I explain in detail in my written testimony how Google is the single worst arbitrageur of privacy laws and the single biggest threat to Americans' privacy today.

Case Study: How Google Systematically Threatens Americans' Privacy:

1. Google's radical "publicacy" mission is antithetical to privacy.
2. Privacy is not a priority in Google's culture.
3. Google gives privacy "lip service."
4. Google threatens the privacy of more people than most any other entity.
5. Google collects/stores the most potential "blackmail-able" information.
6. Google's track record does not inspire trust.

As others have said, information is power. Power corrupts. Absolute power corrupts absolutely. Google's market power over private information is corrupting Google, just like former FBI Director J. Edgar Hoover was corrupted by his power and mastery of personally-sensitive information. Google's unprecedented arbitrage of privacy law combined with its exceptional lack of accountability is fast-creating this era's privacy-invading, unaccountable equivalent: "J. Edgar Google." Remember the timeless insight, those who don't learn from history -- are doomed to repeat it.

Written Testimony of
Scott Cleland
President, Precursor LLC

"The Blind Eye to Privacy Law Arbitrage by Google
-- Broadly Threatens Respect for Privacy"

Before the
House Energy & Commerce Subcommittee
On Telecommunications and the Internet

Hearing on:
"What Your Broadband Provider Knows About Your Web Use:
Deep Packet Inspection and Communications Laws and Policies"

July 17, 2008

I. Introduction

Mr. Chairman and Members of the Subcommittee thank you for the honor of testifying on the important subject of Internet privacy. I am Scott Cleland, President of Precursor LLC, an industry research and consulting firm, specializing in anticipating the future of the converging techcom industry. I am also Chairman of NetCompetition.org, a pro-competition e-forum funded by telecom, cable and wireless broadband companies. My testimony today reflects my own personal views and not the views of any of my clients.

II. The Problem of Privacy Law Arbitrage and Selective Privacy Oversight:

The current patchwork of U.S. privacy laws, the lack of a holistic approach to Internet privacy, and selective oversight of privacy problems – have combined to create perverse incentives for some companies to:

- Arbitrage privacy laws,
- Try and "fall between the cracks" of privacy oversight, and
- Push the privacy envelope.

As a result, invasion/abuse of privacy is among the most serious problems users face on the Internet. The lack of a holistic, comprehensive and balanced approach to privacy law and oversight is a serious threat to American's privacy.

Broadband companies, (telecom, wireless and cable) have long been subject to strict privacy laws (sections 222, 551 & the ECPA), which created serious consequences for the misuse of personally identifiable information without a user's permission. Consequently, broadband companies have developed extensive policies, procedures and practices to respect users' privacy and protect personally identifiable information. Like medical providers operate under HIPPA privacy protections and financial services providers operate under FCRA/FDCPA privacy protections, broadband providers operate under sections 222, 551 and the ECPA, privacy protections. As a result, the broadband, medical and financial industries have **made respect for privacy an integral part of their business models and cultures**.

This Subcommittee's oversight of experimentation by some, with "deep packet inspection" for advertising purposes, is entirely appropriate. Existing laws appear to cover these practices so oversight by Congress and regulators is appropriate and expected.

I am concerned however, that selective oversight of only broadband privacy matters fosters a blind eye to arbitrage of privacy laws by application companies like Google, Yahoo and others. This creates perverse incentives for companies not covered by U.S. privacy laws to push the envelope on privacy to gain competitive advantage. **Americans' privacy should not be an unrestricted commodity to sell to the highest bidder or to gain competitive advantage.**

- Specifically, I am troubled with the selective broadband focus of this hearing, because privacy is a cross-cutting, big picture issue that knows no boundaries between the access, application and content "layers' of the Internet.
    - If the Subcommittee holds a hearing entitled: "*What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies*" – to add balance and to focus on the most serious threat to Americans' privacy, I humbly suggest the Subcommittee hold another hearing entitled: "*Why Google Knows Everything About You: Unauthorized Web Surveillance and Privacy Law Arbitrage.*"
- By turning a blind eye to what Google, the worst privacy offender on the Internet, is doing to systematically invade and abuse Americans' expectation of privacy, Congress is perversely encouraging copycat behavior by "deep packet inspection" advertising entrepreneurs who see that there is a huge privacy double standard to arbitrage.
    - If you are a broadband provider strict privacy laws apply, if you are an "application" provider like Google, it's the Wild West – there's no privacy protection.
    - Like water seeking its own level, market forces can be expected to arbitrage the huge gaps in privacy protection among companies.
    - Companies like NebuAd are essentially just following in the footsteps of the privacy-arbitrage leader – Google.

To illustrate my point of the extreme privacy law arbitrage that is occurring in the U.S. marketplace today, let me explain in detail how Google is the single worst arbitrageur of privacy laws and the single biggest threat to Americans' privacy today.

III. Case Study: How Google Systematically Threatens Americans' Privacy:

To begin, I am not alone in believing Google's privacy practices are a particularly serious consumer protection problem.

- **Privacy watchdog, Privacy International, ranked Google worst in its world survey on privacy in 2007 and described Google as "hostile to privacy."**
- EPIC, CDD, and USPIRG filed suit with the FTC last year challenging Google's privacy practices as deceptive trade practices.
- Recently, a broad coalition of privacy advocates pressured Google to finally comply with California privacy law and put a link to their privacy policy on their home page.

1. Google's mission is antithetical to privacy.

- Google's megalomaniacal "*mission is to organize the world's information and make it accessible and useful.*"
    - **Google's mission is so uniquely antithetical to privacy – it actually warrants the creation of a new term: "publicacy."**
    - Google's unique and radical "publicacy" mission believes "the world's information," is, and should be public not private. (Note the mission statement puts no qualifier on "information" other than "the world's.")
- The fact that most of the world's most valuable information is *copyrighted or owned by others* hasn't stopped Google from making other's property universally available – without permission or compensation. As a result, several different content industries are suing Google for theft. Google supports radical copyright reform to remake the Internet

into a less-propertied, "information commons" where most all content is free to the user and supported by Internet advertising -- the business that Google dominates.

- The fact that much of the world's information is also *private*, or enables privacy because it is not easily accessible publicly by anyone, hasn't stopped Google from trying to make this *private* information *publicly* accessible. The business reason for this is that Google knows that the most valuable information is private (scarce) information that was not available before. Google also knows that its competitive advantage is its world-leading "database of user intentions," i.e. search histories on several hundred million Google users worldwide. Google also understands that it can earn a premium because it knows more private information on users' intentions, preferences and secrets than any other company in the world – by far. Simply, Google's business edge is that it collects, stores and uses more private information than any other entity in existence, which enables it to "target" "relevant" advertising better than anyone else.
- The fact that Google's web "crawlers" are the world's most pervasive and invasive, Google indiscriminately searches websites for whatever it can find, and automatically assumes if their crawlers can find it, it must be "public" information. This indiscriminate web crawling has resulted in Google exposing private information like social security numbers, as Google did in making hundreds of California university students' social security numbers public -- as reported by the Sacramento Bee (3-7-07.)

2. Privacy is not a priority in Google's culture.

- Google celebrates an "innovation without permission" culture. Google's obsession with innovation comes at a cost, because it comes with a cultural disdain for internal controls, management supervision, and internal vetting of issues for privacy concerns. Let me illustrate this cultural disdain for privacy with three high-profile examples of Google proceeding full-speed-ahead with "beta" releases -- without regard to privacy implications of their actions.
    - Google introduced gmail, which enables Google to automatically read the content of users' private gmail messages in order to send them "relevant" advertising –

without meaningful internal privacy review. This caused a widely reported public uproar over users' privacy being abused.

- Google introduced Google Earth, which exposed the roof tops of the White House, public buildings and military installations, without meaningful internal review of the privacy, safety, or national security implications. The uproar that ensued over this suggests Google learned little from the gmail incident about the importance of internal review to address external concerns like privacy.
- Google then introduced StreetView, which is video of people's homes, apartments and neighborhoods, without meaningful internal review of the privacy or safety concerns involved. The uproar over this invasion of privacy is so significant that Google is very secretive about where and when Google's "spycars" will be videoing a particular neighborhood in order to protect the safety of the Google drivers from irate residents.

- The inescapable conclusion from this pattern of behavior is that Google's culture exhibits a fundamental and sustained disdain for privacy.

3. Google gives privacy "lip service."

- Only this month did Google begrudgingly comply with longstanding California Privacy law to post a link to their privacy policy on their webpage. Google's founders did not want to "clutter" the signature simplicity of their homepage with the addition of another word. Google's leaders spoke loudly on their assessment of the value of privacy policies with their stubborn recalcitrance on this most basic of privacy compliance. The message internally is that privacy is not a priority to the founders. We also know that organizations listen and follow the cues from their leaders about which values to follow in conducting business.
- Google has not bothered to update its privacy policy since October 14th, 2005 despite a number of major external developments that objective observers would think would merit an update or a change in their privacy policy.
  - Since the last update, Google has entered several new businesses which operate under very different privacy laws:

- YouTube – viewing habits;
- Feedburner – reading habits;
- GrandCentral – voiceprints and wiretapping;
- DoubleClick – ad viewing
  - (Note: a few years ago the FTC sanctioned DoubleClick for its privacy practices.);
- Google Health (which arbitrages HIPPA); and
- FriendConnect (after state Attorney Generals acted on privacy/safety related issues of minors.)

  - In the fall of 2007, Privacy International ranked Google worst in its world survey, and called the company "hostile to privacy."
  - In 2007, privacy watchdog EPIC, sued Google via the FTC review of the Google-DoubleClick merger, for deceptive trade practices.
  - In late 2007, the FTC staff proposed new behavioral advertising privacy principles that run counter to Google's current privacy practices.

- If Google really cared about privacy and it was an important priority, wouldn't Google have updated its privacy policy to adapt to any of the above mentioned developments? Not only does Google not a lead by example on privacy matters, it doesn't even follow others lead.

4. Google threatens the privacy of more people than most any other entity.

- Google-DoubleClick track the search histories and ad-viewing habits of an estimated 90% of global Internet users, approaching a billion people worldwide.
- Google has the largest network of advertisers, ~1,000,000 compared to Yahoo's ~300,000 and Microsoft's ~75,000.
- Google has relationships with over 1 million websites, orders of magnitude more content relationships than its competitors.
- What this means is that **Google has both the means and the business model to learn more private information about more people than any other company in the world**.

5. Google collects/stores the most potential "blackmail-able" information.

- Consider the depth and breadth of intimate information Google collects:
  - *What you search for*;
    - (a Ponemon Institute survey of 1,000 Google users found that 89% thought that their searches were private and 77% thought Google searches could not reveal their personal identities – wrong on both accounts.)
  - *Where you go on the web*;
    - Google has pervasive unauthorized-web-surveillance capability (web tracking/stalking) through a combination of Google's search, Google's cookies, DoubleClick's ad-view recording capability, Google's extensive content affiliate network of hundreds of thousands of sites, and the wide variety of Google apps.
  - *What you watch* -- through YouTube;
    - (Remember Supreme Court nominee Robert Bork was politically attacked for the videos he rented.)
  - *What you read* -- through Google News, Feedburner and Blogger.
  - *What you say* -- in your emails through gmail's automated reader.
  - *What you produce* -- in Google Docs or spreadsheets.
    - (In return for the free Google Apps like Docs and spreadsheets, users grant Google some search rights in perpetuity to any content a user produces using Google's Apps.)
  - *What your family and friends look like* -- through Picassa images.
  - *Your medical conditions, medications, and medical history* -- through Google Health.
  - *Your purchase habits* -- through Google Checkout.
  - *Your call habits and voiceprint* -- through Google Talk.
  - *Your travel habits and interests* -- via Google Maps.
  - *Your interest in other people/places* -- via Google Earth & StreetView.
  - *Your personal information* -- through Orkut (social networking) Gmail, Google Checkout, etc.

- *Where you go/hang out* -- through Google wireless ventures and Android.
- *Where you'll be or where you were* -- through Google Calendar.

- The scale and scope of Google's unauthorized-web-surveillance is truly Orwellian "Big Brother." While Google is not the Government, all this private information that Google collects and stores is certainly available to the Government via subpoena.
- It is also important that this capability of Google's is very different from Microsoft reach because as a software provider, your private information mostly resides on your PC where you control it.
  - In stark contrast, all of the private information listed above that Google collects *resides on Google's servers.*

6. Google's track record does not inspire trust.

- Google does not fairly represent its business to users.
  - Google's rhetoric and public relations intimate that Google works for users – they don't. Google is not paid by users – Google is paid by advertisers and websites.
    - Like investment banks hurt investors during the bubble for not disclosing that their research had a financial conflict of interest, Google puts users at serious risk by not disclosing to them that Google has a financial conflict of interest in looking out for advertiser/website/Google interest before the users' interest.
    - How this conflict could hurt consumers today is that when websites are infected with dangerous malware like phishing for ID theft, Google has not been flagging certain search results as dangerous, when doing so would protect users from sites Google knows not be safe. They are being silent and not protecting users from potential harm because that would discourage traffic, clicks and revenue from Google's real clients: advertisers and websites.
- If the Ponemon survey of Google's users is even remotely accurate, most consumers do not understand that they have forfeited their privacy to Google in return for Google's

free applications. In other words, few people understand that Google thinks they have users' full permission/assent to sell their privacy to the highest bidder.

- Another trust undermining aspect of Google's business is the rampancy of fraud in Google's model.
    - Most people are not aware that click-search is one of the most fraud-prone industries in America. Click Forensics, which is the leading industry tracker of web fraud, estimates that 28% of all Internet clicks are fraudulent.
    - The dirty little secret here is that the gross-revenue business model for search, which was pioneered by Google, makes money off of fraudulent clicks. In other words, Google's gross revenue model does not have a financial incentive to be honest.
    - It is hard to imagine another legal industry in America that would tolerate a 28% gross fraud rate!
- Google also does not inspire trust because **Google's words don't match its deeds**. It is the master of the slippery, self-serving, double-standard:
    - Google's mission is to organize the world's information to make it accessible, when Google is among the most secretive, non-transparent, 'black box' public entities anywhere.
    - Google pushes "open" everything for everyone else, open access, open source, open social, open handset, open spectrum, but the auction process that is at the core of Google's business model is not open but an opaque 'black box' that users cannot see into.
    - Google supports net neutrality regulation for its broadband competitors, but maintains that Google, the world's most dominant access point for the Internet, should not be subject to net neutrality regulation.
    - Google aggressively protects its intellectual property of copyrights and patents, while strongly supporting "information commons" reforms that would decimate the intellectual property rights of their competitors.
    - Google runs its not-for-profit Google.org as a for-profit division of Google, when every other corporation in America abides by the clear separation of for-profit and not-for-profit entities to avoid even the appearance of tax evasion or impropriety.

IV. Conclusion:

The lack of a holistic approach to Internet privacy combined with selective oversight of privacy problems encourages some companies to try and "fall between the cracks" of privacy law, to arbitrage privacy laws and to push the privacy envelope. This is unfortunate because invasion/abuse of privacy is among the most serious problems users face on the Internet. **In short, the lack of a holistic, comprehensive and balanced approach to privacy is a serious threat to American's privacy.**

Vigilant oversight of broadband companies subject to privacy law is appropriate. What is not appropriate is discrimination against broadband providers as the only companies that warrant privacy oversight. The greatest risk comes from application providers like Google and Yahoo, which are not subject to privacy law, and are arbitraging that legal gap, as a competitive advantage to the serious detriment of Americans' privacy. Given Google's exceptional and increasing market power over the business of the Internet, it appears as if **the Subcommittee risks turning a blind eye to the single biggest unaddressed threat to Americans' privacy**.

As others have said, information is power. Power corrupts. Absolute power corrupts absolutely. Google's market power over private information is corrupting Google, just like former FBI Director J. Edgar Hoover was corrupted by his power and mastery of personally-sensitive information. Google's unprecedented arbitrage of privacy law combined with its exceptional lack of accountability is fast-creating this era's privacy-invading, unaccountable equivalent: "J. Edgar Google." Remember the timeless insight, those who don't learn from history -- are doomed to repeat it.

Attachment I:

Precursor Blog posts on Google & Privacy:

J. Edgar Google: Information Is Power + No Accountability

- http://www.precursorblog.com/content/j-edgar-google-information-is-power-no-accountability

Can you trust Google to obey the rules? Is Google accountable to anyone?

- http://www.precursorblog.com/node/769

Why Google storing personal health records is a really bad joke -- the public should be worried...

- http://www.precursorblog.com/node/762

Google's Privacy Lip Service

- http://www.precursorblog.com/content/googles-privacy-lip-service

Google protecting its privacy to invade your privacy; Why Google is the King of Double Standards:

- http://www.precursorblog.com/content/google-protecting-its-privacy-invade-your-privacy-why-google-king-double-standards

J. Edgar Google compiling personal YouTube viewing dossiers

- http://www.precursorblog.com/content/j-edgar-google-compiling-personal-youtube-viewing-dossiers

Attachment II:

Scott Cleland
Founder & President, Precursor® LLC
Chairman, Netcompetition.org

Scott Cleland is one of nation's foremost techcom analysts and experts *at the nexus of*: capital markets, public policy and techcom industry change. He is widely-respected in industry, government, media and capital markets as a forward thinker, free market proponent, and leading authority on the future of communications. Precursor LLC is an industry research and consulting firm, specializing in the techcom sector, whose mission is to help companies anticipate change for competitive advantage. He previously founded The Precursor Group Inc., which *Institutional Investor* magazine ranked as the #1 "Best Independent" research firm in communications for two years in a row. He is also Chairman of Netcompetition.org, a wholly-owned subsidiary of Precursor LLC and an e-forum on Net Neutrality funded by broadband telecom, cable, and wireless companies.

Cleland has a high-profile track record of foreseeing big change before others. He coined the term "techcom" to define how information technology drives the communications future and to best name the new sector that converging communications technologies are creating. *Fortune* profiled Cleland as the first to call "WorldCom: Dead Model Walking" and to predict its bankruptcy. Then WorldCom CEO Bernie Ebbers tried to discredit Cleland's prescient and hard-hitting research on WorldCom by deriding him the "idiot Washington analyst." Cleland has testified before seven different Congressional subcommittees on a variety of forward-looking topics and was the first congressional expert witness asked to testify on what went wrong with Enron.

Mr. MARKEY. Great. Thank you, Mr. Cleland, very much.

Now we are going to turn to questions from the panel, and I want to begin by agreeing with Mr. Cleland, that absolute power corrupts absolutely. So Mr. Dykes, not only do you get access to all of Google, but you get access to all of eBay, Amazon, everyone. If there were 56 companies up here, not just Google but everyone else at a company, you would get access to all of the information, so you are Google times 100 in terms of the information you can with this deep packet inspection coordinating with a broadband carrier get access to. So I would like to get crystal clear, Mr. Dykes, what your privacy position is, and I would like a simple yes or no, please. One, do you support giving consumers clear, conspicuous notice?

Mr. DYKES. Yes, sir.

Mr. MARKEY. Two, do you support a meaningful opt-in standard for authorizing use of a consumer's data?

Mr. DYKES. Well, sir, I would say that to characterize opt-in or opt-out is probably not as important as to say there has to be a very robust notice——

Mr. MARKEY. No, no, no. The difference is that you have got to get the consumer to say yes, OK. Do you support a policy that says the consumer must say yes before you are allowed to roam through all of their personal data and turn it into an information product which is then sold to other companies? Yes or no on that question.

Mr. DYKES. Mr. Chairman, I think you are forcing me into one of those, "Have you stopped beating your wife recently."

Mr. MARKEY. No, no, no, no, no, have you stopped beating the consumer is the question, OK, and I want to know, Mr. Dykes, do you support getting permission affirmatively from the consumer before you start beating them up by sending them other information that they have not asked for? Mr. Dykes, yes or no.

Mr. DYKES. I really must protest and say that it is much more important to ensure that the consumer is well informed on the decision being made than to use the——

Mr. MARKEY. Oh, I already asked you that first question. You already answered that one. That is yes. Now I want to know what you mean by that, and by that, should you get permission from the consumer first, Mr. Dykes? You have absolute power, as Mr. Cleland just pointed out. You are going to have access to all the information. Do you want to give them—will you give them opt-in?

Mr. DYKES. Mr. Chairman, I really have to say that how what we do is characterized is going to be characterized by——

Mr. MARKEY. All right. Let me ask you the third question. Do you agree that consumers who do not grant consent should not have their Web use tracked, intercepted, or profiled?

Mr. DYKES. Yes, Mr. Chairman, we in fact have explained that recently we have created innovation that will enable that.

Mr. MARKEY. So that is a yes, they should not get information if they have not granted consent?

Mr. DYKES. That is right. If they have opted out, for example, they should not be tracked.

Mr. MARKEY. No, I am not saying that. I am saying, if they have not granted consent, that they should not have their Web use tracked.

Mr. DYKES. As we go through this process of informing them, if we are not convinced that somebody has not opted either way——

Mr. MARKEY. Are you going to then consider that to be consent if they have not——

Mr. DYKES. If they have not opted either way, then they are not tracked. For example, if somebody has deleted all their——

Mr. MARKEY. Well, I don't think that is a high enough standard, Mr. Dykes. I think that that is basically saying that silence is consent and that as a result you can do whatever you want with their information. I don't think unless you have gotten their affirmative permission that you should be allowed to be able to take this incredible leap into the breaching of the privacy of Americans. It is like saying that the mailman can open up any letter, can open up any package, find out what is in it, and then start to partner with other companies, letting them know what individual Americans are receiving in the mail, what kind of packages are coming to their house, but it is OK because the consumer doesn't know that you are doing it and hasn't given you the opportunity to say to the mailman, stop opening my packages, stop opening my mail, I don't want anyone to know about it, and so we have a real problem here.

Dr. Reed, can you tell me, sir, how this concept is consistent with the history of the Internet or inconsistent with the history of the Internet?

Mr. REED. Sure. I should clarify that the definition of deep packet inspection used by Mr. Sabet is not quite right. It doesn't involve only looking at label information. It does indeed involve looking at everything in the packet, so the Wikipedia is wrong, as sometimes it is.

What is inconsistent about the history of the Internet, the history of the Internet was designed with the shipping of goods and essentially the ideas that lurk behind common carriage as its background, and it relates to the idea that the only people who should be interested in the actual contents of these messages are the endpoints involved that are the addressee or source of the message, and we carefully chose that design in the original design because we didn't want to make the network more complex, and we knew, A, and B, we knew that the Internet, it was the first network that had multiple jurisdictions involved in the transport of packets. AT&T was only one company but the packets in the Internet flow through many autonomous systems, all of which could potentially cause trouble to the endpoints and which are not under control of a central authority. So the reason we built into the design that the contents of the packets was sacrosanct from both examination and action was specifically to deal with the diversity of the network and to deal with the expectations that could be standardized at the endpoints, that when you sent a packet, it would get there with best efforts. That was the fundamental principle and without examination.

Mr. MARKEY. Thank you, Dr. Reed.

My time is expired. The chair recognizes the gentleman from Florida, Mr. Stearns.

Mr. STEARNS. Thank you, Mr. Chairman.

Mr. Dykes, I can give you a little help on your answers from Mr. Markey. You can say "I don't know." We oftentimes have——

Mr. DYKES. No, I think the way Mr. Chairman further explained it, I think the answer would actually be yes, that we do not track people who we are convinced don't want to be tracked.

Mr. STEARNS. Obviously if the chairman wants to say every time this occurs there has to be an opt-in, then a dialog box would come up all the time, and I am saying if Congress mandated that, isn't it possible that when I go on the Internet and whether we are doing deep packets of information exploration or whether we are doing, as Mr. Cleland talked about, unauthorized surveillance, a dialog box would pop up? Isn't that true under what Mr. Markey—there would be a constant dialog box, and every consumer would have to click in, click out? I mean, isn't that what would happen? Give me the practicality if we went along the reasoning that Mr. Markey is saying is, we need to have an opt-in every time something happens, whether it is a surveillance—because Dr. Reed made a very good point. He is making the analogy between sending a box from Europe to the United States, and there is an address on this box, and we are supposing we let your company go into the box, and there is an implication, Dr. Reed is saying, that you are messing up the box. So you have to make the case here strongly this morning that this is not the same analogy and that the personally identifiable information has nothing to do with health, it has nothing to do with financial records. The compilation that Mr. Cleland is talking about is onerous, and there is lots of stuff coming together, I understand that, but the only way they can get back is through an IP address, and you have to be very clever to do that, but some of the things you are doing are very simple things that you are trying to say, does Stearns enjoy this type of DVD, does he like this movie or does he like such and such, and maybe we will advertise to let him know there is a new war novel coming out that he might like. So I mean, you are on the pivotal point here. Whether opt-in or opt-out, this is the key question. So you have to make the case, and maybe, Mr. Cleland, you can comment too.

Mr. DYKES. So, the laws—Congress over time has balanced a whole series of factors in deciding what laws require opt-in, and opt-in is actually pretty rare, when there is sensitive information, personal information that could harm or embarrass somebody, and so we made a particular point of not having any personally identifiable information, not having any sensitive information, and so by staying at a very high level, broad categories characterized against anonymous profiles, we believe that in the general sense of the law that this country has, we are really in the opt-out mode. But I really don't think the opt-in or opt-out is nearly as important as robust notice to the consumers, so that they truly understand what is going on and then the opportunity to control that. So obviously you don't want to be too intrusive with the notices, but I think there is——

Mr. STEARNS. Tell me how you are giving notices today. How do you give notice to the average consumer?

Mr. DYKES. Today our ISPs generally give notice by either a separate letter in the mail or separate notice in the billing statement or an e-mail in——

Mr. STEARNS. Does that come before or after you have gone through the deep packet information?

Mr. DYKES. Before. We need to have a notice happen at least 30 days before any of the service commences so that we can be sure that people have the opportunity to opt out, and people do opt out.

Mr. STEARNS. So you are saying you already have an opt-out notice in place?

Mr. DYKES. Yes, sir, we do. We have these notices, and these are the notices that in general privacy rules are considered to be very robust notice today. We are going to go beyond that when we introduce or are introducing technology to allow that notice to be online.

Mr. STEARNS. OK.

Mr. DYKES. And we will work with CDT to improve that process and ensure that we find a way to meld the needs of privacy with users' expectations and good user——

Mr. STEARNS. Mr. Cleland?

Mr. CLELAND. Yes. Thank you. The point I want to reiterate is, broadband companies are subject to strict privacy laws. They respect privacy laws. They have cultures that embed policies, practices, and procedures that respect privacy. That is the law. My point here is, we are worried about whether the blinds on the window are perfect when the house doesn't have any walls, and so people are worried about broadband and deep packet inspection that is covered by the law, and there is oversight like this hearing, and there are regulators that can look into it, yet what happens with Google and Yahoo and some of these others is, there is no privacy law, and there is no oversight, and so there is huge arbitrage.

Mr. STEARNS. Dr. Reed?

Mr. REED. Yes, I will just comment that two broadband providers, one noted in this document from Robert Tolpolski, who works with Free Press and Public Knowledge, and another, Charter Communications in the United States, are considering using—or have used, so they have already violated the privacy laws if the privacy laws apply, or are considering using this technology with American citizens with whatever is going on, and Phorm Technology has been actively operating a very similar service based on similar technology in partnership with British Telecom in the UK. So it is a little bit unreasonable to claim that the providers feel they are constrained from using this technology by those laws today. Maybe they haven't consulted their legal department.

Mr. MARKEY. The gentleman's time is expired. The chair recognizes the gentleman from Michigan, Mr. Stupak.

Mr. STUPAK. Thank you, Mr. Chairman.

Mr. Dykes, if you are on one of the ISPs, how do I know, how am I given notice that your company is tracking my information?

Mr. DYKES. Today, sir, we provide notice via a——

Mr. STUPAK. You provide notice or the ISP?

Mr. DYKES. The ISP provides notice. There is a separate note in your billing statement or separate letter, or if they are confident it will be read, an e-mail to you. But as I said previously, we are now introducing newer technology so that notice can be online so you can read it directly there as well.

Mr. STUPAK. And if I opt out and I don't want to be part of this program, you can still track everything I do and every site and where my interests might lie, correct?

Mr. DYKES. Well, the very point of your opting out is that we then don't do that, and if we were already doing it and you opted out, we immediately delete all of the records that we have on such an opted out——

Mr. STUPAK. And you don't track after that?

Mr. DYKES. Correct, sir. We don't collect any data once you have opted out. We delete all the data we might have had. But by providing that notice 30 days before a system begins in your neighborhood, there is a good chance that it never would have been collected.

Mr. STUPAK. What if people don't return, don't respond? Do you just start tracking them?

Mr. DYKES. Sir, that is why we make sure that we are not tracking any personally identifiable information or——

Mr. STUPAK. So the answer is, if I don't respond, I get tracked?

Mr. DYKES. Sir, that is the way the general privacy laws are written today is that where there is no personally identifiable information or sensitive information——

Mr. STUPAK. Well, I think most Americans would state that is not the law. I think most Americans would believe that the information they have about themselves is theirs. Just because I belong to an ISP doesn't give you the right to track me. If I want to be tracked, it should be affirmative. As I said in my opening statement, there really should be an opt-in. Why do I have to opt out? Why should the burden be on the American consumer? Should it not be on the ISP or your company that wants to track my information?

Mr. DYKES. Well, sir, I think that there should be a common set of laws around privacy in this country that generally treats the various technologies in exactly the same manner. What we do with the Internet or offline, et cetera, should have a common set of principles, and I don't think that one set of companies should be penalized versus another set of companies. Given a general law, we are very happy to comply with however that law is set up.

Mr. STUPAK. So if we pass a law that says you can't do any deep packet unless the consumer actually opts in, you would be satisfied with that?

Mr. DYKES. Well, we would be satisfied with any law you pass, sir, so we will work within that.

Mr. STUPAK. OK. Dr. Reed, you spoke about how deep packet technology can be used to assist law enforcement, but you also expressed concerns regarding how it may negatively affect the network's ability to function. How do you reconcile the two?

Mr. REED. In specific law enforcement or——

Mr. STUPAK. Yes.

Mr. REED. Well, first of all, there are two things going on here. Law enforcement use of these technologies, which is in some cases mandated by CALEA, the law you have passed, generally only inspects the packets, generally uses the information derived from those packets in legally sanctioned ways and I presume is using the rules of the government to guard and safeguard that information and how it is used. So while I am——

Mr. STUPAK. So law enforcement more goes for an information packet. From there if there is reason to believe a crime may be committed, that is when they go deeper to identify the individual?

Mr. REED. Well, in fact, a number of these technologies I believe are used currently by law enforcement selectively and by intelligence agencies on foreign traffic——

Mr. STUPAK. Sure, like——

Mr. REED [continuing]. And those technologies are collecting the information but in very safeguarded locations, government-owned or controlled locations. The analysis performed on them is subject to review by various processes ranging from—so they are not just used immediately to react, and the review is a legal review in many cases where, for example, the standards of evidence are required to actually act on that information, so an FBI agent may in fact be using deep packet inspection to derive information, but whether it can be presented in court or used for exploration, those are matters that I, not being a lawyer, am not deeply expert in, but my understanding is that that is quite a different kettle of fish than here. I don't think commercial companies have the ability to carry out such a duty of care.

Mr. STUPAK. Are DPI devices accessible remotely? In other words, what I mean, are they susceptible to hackers who may wish to commit identity theft, in your estimation?

Mr. REED. They could be. I have not examined them. I would be happy to examine, for example, NebuAd's devices and technology, but what I know about them is based on observations by people who detect them in the network and analyze them as black boxes based on what they do and what they seem to do plus their marketing materials, and I have no specific knowledge of how easy it is to break into them. I believe Mr. Dykes is correct that you can make them quite secure if you put that amount of energy into them, but nearly every technology can be broken.

Mr. STUPAK. Thank you.

Mr. MARKEY. The gentleman's time is expired. The chair recognizes the gentleman from Oregon, Mr. Walden.

Mr. WALDEN. Thank you, Mr. Chairman, and I appreciate the hearing on this very important matter, I think, and I concur with the chairman's comments and others that I think the average consumer out there views this more, or wants to, their time on the Internet more like they view the postal system, and I realize that is in disagreement with some on the panel, but I thought the chairman hit it on the head. If I order a package from some site, I don't expect the postal person to go through it on the way, figure out what it is—I thought that was a great analogy, Mr. Chairman—and then decide who they think ought to come and market me, and that is different than walking into a store and realizing I am public and shopping around, I think. And so I think for the Internet to really survive as an engine of commerce, you have to have opt-in, and I think that is what consumers want. That is what I would want. I get enough junk mail. I am not sure I am going to plow through every letter I get or every whatever it is you are—do you have a copy of what you send out, by the way, Mr. Dykes?

Mr. DYKES. Yes, sir, we can provide that to you.

Mr. WALDEN. I would love to see it, but the fact that I have to take affirmative action so that I can stop you from making money on my transactions on the Internet seems sort of backwards. Isn't that really what you are saying I have to do? I have to opt out under your scheme.

Mr. DYKES. Sir, as I said, I think it is most important that we inform you what we are doing. That is——

Mr. WALDEN. That you do what?

Mr. DYKES. That we inform you of what we are doing, robust information, a notice that you can clearly understand what is happening, and then you can make your choice. The——

Mr. WALDEN. But why is the burden on me to make the choice, because the choice you are asking me as a consumer to make is to prevent you from taking an action that enriches you, right?

Mr. DYKES. Sir, the——

Mr. WALDEN. You are in this to make money. That is not a bad thing. But you are building a business model here, and aren't you in part betting that there are going to be consumers who ignore those notices or don't understand them or whatever, so you get to work that angle, plus those who affirmatively say you bet, I like your concept, and there will be some who say yes, update me on the latest from whatever organization.

Mr. DYKES. Sir, the Internet is not like the post office inasmuch as it is actually run by commercial organizations, and the ISPs have noted that more than half of Internet funding is coming from advertising today, and I think it is a legitimate desire on their part to increase the amount of advertising that they receive to help fund the Internet, and so this is a manner to do it with very robust privacy controls.

Mr. WALDEN. Wouldn't the most robust privacy control be that of opt in?

Mr. DYKES. Well, as long as we are not collecting any personally identifiable information or sensitive information, then we believe it is possible to note innocuous commercial categories mapped against anonymous profiles so that there is no consumer harm in that regard and then derive additional value from that.

Mr. WALDEN. But you have the ability to personally track identifiable sensitive information, right? You could get access to that.

Mr. DYKES. Well, we can't access any secure information. If it is an HTTPS transaction, for example, it is just physically not possible for us to track secure transactions such as when you go to your bank. So no, sir, we can't track everything on——

Mr. WALDEN. But if you are an Internet consumer and you are just looking at different sites, you are planning a vacation somewhere and so you go to the site on the Virgin Islands or Crater Lake Lodge in Oregon, you could track that I am looking at that site?

Mr. DYKES. That is an example where we wouldn't then keep track of the fact that you went literally to that site. We would note the fact that you are interested in travel.

Mr. WALDEN. Right, but you would know who I am.

Mr. DYKES. No, we do not know who you are.

Mr. WALDEN. You just know that my IP address?

Mr. DYKES. We don't keep the IP address either, sir.

Mr. WALDEN. But you have access to it?

Mr. DYKES. We don't keep it. We don't——

Mr. WALDEN. That is a different question. Do you ever have access to it?

Mr. DYKES. What we do with the IP address is, we translate them immediately in real time to an anonymous identifier in a one-way cryptology so that we can't find our way back to the IP address. So we don't have access to the IP address.

Mr. WALDEN. Dr. Reed, does that track? I am not questioning what you said. I am just trying to figure out how all this——

Mr. REED. Actually, there is a distinction that I am making that Mr. Dykes may not be making, which is that he is talking about the Internet including all the services that are on the Internet, such as Google and so forth, and I am speaking specifically of the transport part of the Internet. It is the case that banks, for example, while they take your password over a secure link, present things like account information and so forth using HTTP transactions in the clear. That is not true of all banks, but it relates to the point I made earlier about the extra expense. If the banks were to respond properly to this and to their mandate to keep consumer information private, they would have to start using encrypted links for far more than they are currently using them for, and we could have an escalation on encryption. We might have an encryption war, at which point if every piece of traffic were encrypted, there would be no market if you add services. I think there are policy implications to having all the traffic encrypted, and I am not sure I want to go there. But the user at great cost to themselves and the services could avoid this problem, and it just shifts the problem elsewhere.

Mr. WALDEN. My time has run out. I just have a unanimous consent request. I know that the ranking member had sent letters to the chairman of Google in 2007 and 2008, and I wondered if I can just ask for those to be put in the record?

Mr. MARKEY. Without objection, they will be included into the record.

Mr. WALDEN. Thank you, Mr. Chairman. I appreciate it.

[The information was unavailable at the time of printing.]

Mr. MARKEY. And I say to the gentleman from Oregon as well that Mr. Dykes said that the postman is public and he is private, but FedEx and UPS are also private, but they can't open up our packages. They can't open up the mail that we put inside. They are private, too, but we all have an expectation when we put something in FedEx that Mr. FedEx can't open it up before he puts it at our front door.

Mr. WALDEN. Exactly.

Mr. MARKEY. So let us not confuse that issue. It is the same level of privacy expectation.

Let me turn now and recognize the gentleman from Pennsylvania, Mr. Doyle.

Mr. DOYLE. Thank you, Mr. Chairman. I think the post office analogy is important, because it is the way most Americans can relate to what is going on. People would be shocked if they thought the post office or FedEx or anybody else was looking at what is inside their packages, whether they knew who they were or not. Peo-

ple would be shocked to know that. And this all gets down to implied consent. Mr. Stearns talks about a dialog box popping up every time, you would have to say whether you opt in or opt out. It doesn't need to be like that at all. It really should just be with the Internet service provider. When I subscribe to America Online or when America Online changes its privacy policy to accept your service, Mr. Dykes, there should be something that pops up on my AOL site when I go on saying something has changed, or if I am just a new subscriber, and it should ask me clearly whether or not I want to be in on a service that is going to look at my information and possibly share that with other people, and do I want to do that or not, and if I say no, I don't want anybody knowing where I go online or what I am doing or if I travel or if am going and looking up information on prostate cancer, I don't want anybody to know that, that I can just check that "no" box, and I don't have to do anything after that. Any site I visit, I am saying I don't want anybody to be inspecting that packet. It could be a simple one opt in, opt out that is presented to you.

Now, I don't know anybody that reads their privacy statements in their bills. If you ever saw them—I have looked at them a couple of times. Your bill comes. There are a couple pages, they are in that real thin paper that is folded. It is about a 2-point print, and if you are old like I am, you can't even see it, and then you are going through that with a magnifying glass, and somewhere in there I guess it tells you that if you don't want somebody to be able to know where you are going to check some sort of opt-out, but if you want to—the big print says if you want to enhance your experience on the Internet, then just we will just take it from here, and you don't have to do anything, we are going to make sure you have a great experience on the Internet.

People don't know this is happening. People do not know that they are implying their consent by saying nothing or the fact that they don't read the fine print in these boxes, and the idea that anybody can examine where you go, what you say, anywhere without expressly saying it is OK with me, I think goes against everything that the country has been founded on and what most Americans understand as their right to privacy under the Constitution of the United States, and I don't care whether an Internet service provider is doing it or Google is doing it, it shouldn't happen, and there should be a clear policy where Americans say I want this, and it should be right up front, and it doesn't need to be a box on every Web site you visit, just your ISP when you are looking at it. Now I will ask some questions.

Mr. DYKES. May I respond?

Mr. DOYLE. Yes, go ahead.

Mr. DYKES. I would like to say I agree with everything you said there. That is exactly my thinking, that there has to be a robust notice, not some big 20-page document, not something in a little box online. This is why I keep emphasizing robust notice as the most important——

Mr. DOYLE. Well, I don't know how you define robust notice, but I know you should have to check the box that says I want you to be able to do this, OK, and no implied consent. It has to be robust, I want to do this consent, and anything short of that I think is a

violation of what most Americans understand as their right to privacy.

Ms. Cooper, I have a question for you. Some people may not know, one of my constituents has released a new record: Girl Talk. He's a mash-up DJ. He released this new album, Feed the Animals, on the Internet, and he is charging like Radiohead, it is pay whatever you want. Now, if record companies and other companies encourage ISPs to use deep packet inspection for tracking copyrighted content and punishing copyright infringers, is it reasonable to worry that the technology would also scoop up consumers of lawful content and other fair uses of copyrighted material?

Ms. COOPER. Well, I will say that I am a huge fan of Girl Talk, and I did download the most recent album at a very low price, but I think you have hit the nail on the head, which is that using technologies like deep packet inspection for applications like copyright filtering raise the question of how to know when you recognize a copyrighted work, whether it is an authorized use of that work or not, and the technology itself of inspecting the packets, assembling the packets into a piece of data that you could recognize as a copyrighted work cannot tell you whether a use is authorized or not. That is a judgment that needs to be made by a person, perhaps multiple people. It depends on the context. It depends on if it is a fair use or not. And so you cannot rely simply on this technology to be able to say yes, this is an illegal use of someone's work or no, it is not.

Mr. DOYLE. Dr. Reed, first of all, thank you for your years of service to the Internet. Tell me, I think you touched on this briefly, will deep packet inspection—don't you think this is really just going to lead to an encryption arms race, where everybody is just going to start to encrypt their packets to avoid detection, and what do you think the implications of that would be to the Internet if that starts to happen?

Mr. REED. Well, first of all, it would be a great boon for the sellers of encryption technology. But I think it would raise the barrier for many applications, because it is not simple to design actually secure encryption technologies. Although the basic idea of encrypting a packet from end to end is easy, the handing out of specific keys to the right set of people that need to receive that stuff is quite complex, and it depends on a notion of a key distribution network which would then have to exist over the top of the Internet, because everyone would need to get their keys reliably from reliable sources, so it would create a rather elaborate network structure for distribution of keys and security of those keys that is not currently in place to make it actually work. I have been involved in the research on that topic actually since about the same time the Internet started, and industry has not succeeded in doing it, partly because the demand has not been there, the expectation of privacy was good enough, but also for two other reasons. One is the reason that there is public interest in not having too strong encryption for law enforcement reasons. You want to be able to not depend on breaking the keys but hope that the bad guys will do something bad for at least discovering bad things, and then the other reason is that the actual physical security of those keys and physical distribution involves trust relationships that don't exist in

society today. Who would you trust to get your key from? Maybe you trust your ISP, maybe not.

Mr. DOYLE. Thank you.

One last question. Mr. Dykes, your testimony says basically that when I surf the Web and I don't opt out, I give you implied consent to share everything that I do, and that is a one-sided consent. Pennsylvania, where I come from, requires both ends of a conversation to consent to any wiretaps. Your service listens to all Web conversations that you sought or obtained consent from millions of people, if not billions of Web pages and content providers. If you have not specifically obtained consent from all these millions of Web page and content providers, why do you think that your service doesn't violate Pennsylvania's wiretap law, or why it wouldn't apply to you?

Mr. DYKES. Sir, I am not a lawyer, but I have spoken to my lawyers, and they have not identified any legal barriers to our entry in any States, but we would be happy to work with you or your staff to go through that in more detail.

Mr. DOYLE. I see my time is up, Mr. Chairman.

Mr. CLELAND. Mr. Doyle, can I make a comment?

Mr. MARKEY. I am sorry. The gentleman's time has expired. I am sorry.

The gentleman from California, Mr. Radanovich.

Mr. RADANOVICH. Thanks, Mr. Chairman, for this hearing.

I do have a question of Dr. Reed. Mr. Cleland gave what I thought was a very interesting analogy about dealing with ISPs and trying to perfect the window shade on a window in a house with no walls. Would you respond to his comments about the difference between search engines and ISPs? I would be curious to know your comments on that.

Mr. REED. Well, I can respond on different levels. I agree with Mr. Cleland that there are strong concerns about the amount of private information that is captured and used by search engine companies and others and that there needs to be some thought given to that scale of collection. It is a different kind of collection, because it is captured by a site that you go to, but in the case of Google, for example, I know that they are kind of the only game in town for a certain kind of thing, not because of a mandate but because they are really good. So I see this particular focus on the transport part as relevant to this committee, and I am not really prepared to talk about the technology inside Google much further than that.

Mr. RADANOVICH. All right. Thank you.

Mr. Cleland, do you have a solution for this? Is it one type of—is it DPI, is it cookies? What is your answer to all this?

Mr. CLELAND. Well, I think, sir, the question also allows me to respond to Mr. Doyle and what he had said. There is a holistic problem here with privacy, and don't be fooled of thinking that there is only one way to be tracked or there is only way for somebody to violate your privacy. Now, packets going through, the expectation is that these packets should be delivered and not interfered with. OK. That is understood. Now, what you do when you are not an ISP, like when you are Google or Yahoo or these others, and they want to track you, they track clicks. Now, they can do the

same thing. You said you didn't want anybody to know if you went to the prostate cancer page. Well, there is a packet that could transmit that, or a click. So there is more than one way to skin a cat, and the problem here is that you are focusing only on broadband deep packet inspection as one way to invade your privacy and turning a complete blind eye to the way that you can track clicks and a myriad of other ways that you can glean the same information and actually potentially a whole lot more. Does that answer your question?

Mr. RADANOVICH. Yes, it does.

Ms. Cooper, I would like to get a comment from you, as well. Do you recognize the advantage of DPI insofar as the potential protection of piracy and those issues as well, the value of something like DPI?

Ms. COOPER. So I think DPI does have some beneficial uses. The one that comes to mind immediately is for detection of network attacks, viruses, spam, distributed denial of service attacks, and those sorts of things where an ISP might have an indication that an attack is coming from a certain IP address or from a certain location, and being able to look a little bit more deeply into the packet can help to thwart those kinds of attacks. So I certainly think that DPI has some beneficial uses, but I really think it needs to be evaluated on a case-by-case basis where you can weigh the risks against the benefits and evaluate the other protections around how it is deployed with the notice and what the limits are on the data collection, so I really think it is a neutral technology. I don't think it is a good or a bad technology, as most technologies are, but I think it deserves a contextual evaluation.

Mr. RADANOVICH. Consumers have to be able to check the box, basically, and say you consent.

Ms. COOPER. Well, in some cases, yes, I think you can imagine certain applications of DPI that you would only want to have consumers, you know, fully informed and consenting to and other examples like with the spam example. If you had to consent to every time your ISP or your e-mail provider blocked a spam for you, that might be something that you would only want to consent to once, or the model would probably look different. So I really think it deserves a case-by-case evaluation.

Mr. RADANOVICH. Thank you.

Thank you, Mr. Chairman.

Mr. MARKEY. The gentleman's time is expired. The chair recognizes the gentleman from Texas, Mr. Gonzalez.

Mr. GONZALEZ. Thank you very much, Mr. Chairman.

Let me preface this question with a story, and actually the reporter's name is Luis Story. I think it was the New York Times. In January 2008, 14.6 billion searches were conducted. Yahoo, Google, Microsoft, AOL, and MySpace record at least 336 billion transmission events in a month, not counting their networks. Yahoo has the most data collection points in a month on its own sites, about 110 billion collections, or 811 for the average user, plus 1,709 other opportunities to collect data about the average person on partner sites such as eBay, at which Yahoo sells the ads.

So my question, should privacy rights and obligations begin and end at the doors of the ISPs solely? Ms. Cooper, just a yes or no.

Should we only be—and I know that my colleague from California touched on it. Should that be our only concern? Do privacy rights and obligations that we seek to protect and impose on all players really begin and end only at the doors of the ISPs? Just a yes or no.

Ms. COOPER. No, we should have comprehensive privacy protections.

Mr. GONZALEZ. Mr. Dykes?

Mr. DYKES. I agree, we should have comprehensive privacy protection that is technology-neutral.

Mr. GONZALEZ. Dr. Reed?

Mr. REED. Yes.

Mr. GONZALEZ. Mr. Sabet?

Mr. SABET. Yes. One point, by the way, is Dr. Reed agrees with my definition from Wikipedia offline.

Mr. GONZALEZ. Mr. Cleland?

Mr. CLELAND. It should be holistic. It shouldn't just be on ISPs.

Mr. GONZALEZ. All right. And I know that we are concentrating on certain technology utilized by ISPs, but I would hope that no one leaves this room today or a viewer or listener thinks that this committee is not concerned about the overarching responsibility and duty that we wish to impose on everyone out there. Mr. Doyle is saying it is another jurisdiction, but we are actually discussing many things that may go way outside the jurisdiction of this committee and such, but nevertheless, you are going to have a collaboration along the way. It seems to me that everyone is—the holy grail here is some sort of an opt-in as opposed to what we generally follow in other models of opt-out, an affirmative act saying that you will agree after there is full, and as the chairman indicated, clear and conspicuous disclosure, which we all agree on, and then some affirmative act, in this case it would be an opt-in. So there are different ways to opt in, and I am just wondering, and I will be asking a couple of the witnesses if they would agree that this would be adequate and sufficient across the board, whether it is an ISP or an application company. What if they were able to obtain the opt-in in the following manner? One, that would tell the consumer check this box, whether it is on the screen or whatever or an envelope saying after full disclosure, conspicuous clear language, simply using the service will be interpreted as an opt-in. Would you be satisfied, Ms. Cooper, with an arrangement, simply using the service would be an affirmative act of opting in to all conditions and terms of the provider?

Ms. COOPER. I think it depends on the service. I think at times affirmative express consent is absolutely necessary, and at other times it is not. I think it is dependent upon the data being collected, the sensitivity of the data, the laws that we have in place. All of those things are important to the decision——

Mr. GONZALEZ. We would have to have different standards on that type of opt-in language, depending on the type of information that is being gathered. I just think that may be an impossible task. I am not sure.

Dr. Reed, would you be satisfied with that kind of an opt-in arrangement? Simply using the service equates to an affirmative act of opting in.

Mr. REED. No, not in the case of ISP access to the Internet.

Mr. GONZALEZ. No, I am talking about everyone that should have a responsibility and duty to safeguard this particular information when they gather it and making sure there is full disclosure to the consumer that it is being collected and shared. What does it matter whether it is Embarq or whether it is Google? It is still my information. One, full disclosure; two, an adequate opt-in process. Why are we making that distinction is the real curious question. I think for the most part you all have distinctions without differences. It is whether we have—maybe because of the scope of the technology and the ISP status. You are saying, well, that is a mortal sin, we will let everyone get away with venial sins. Well, I hate to tell you, I think the consumer is just going to be concerned with the tremendous information out there that may constitute a lesser sin, but it is still a sin. And by the way, all these centers are all worshipping at the common altar of the advertising dollar, which promotes and supports the entire system, whether you are a network, ISP, or an application company, and that is the reality, and I know, I think the chairman has been very reasonable and generous with me, and he has let me go over my amount of time, and I yield back.

Mr. MARKEY. The gentleman's time has expired. The gentlelady from California, Ms. Eshoo.

Ms. ESHOO. Thank you, Mr. Chairman, for yet another substantive hearing on an all-important issue. It is great having you be chair, because that is what we have done since you have taken over, so thank you. And thank you to all the witnesses.

First of all, I can't help but think of the following with my Intelligence Committee cap on, and that is that the penultimate intelligence is to know how people think, and I think that that applies to a lot of what we are talking about here. I think that users should be notified in the most meaningful way on what information is being collected, how it is being used, how they can opt out of certain forms of data collection, and I think that medical information collected really should be treated as one of the most sensitive or the most sensitive data. So I just want to state that.

I apologize for coming in later than other members, but it gave me an opportunity to read what we didn't have yesterday and that is some of the testimony. Mr. Cleland, I derived from your testimony, from your statement, that you are not for net neutrality. Is that—that is pretty obvious.

Mr. CLELAND. Exactly.

Ms. ESHOO. Yes, not for net neutrality. Let me ask you this. Are you paid any consulting fees by any of the Bells, cable or anyone?

Mr. CLELAND. As I disclosed when I came in here, I am testifying on my own behalf. However, another——

Ms. ESHOO. Are you paid by anyone——

Mr. CLELAND. I am chairman of NetCompetition.org. It is funded by wireless telecom and cable companies. So that is——

Ms. ESHOO. So the answer is yes?

Mr. CLELAND. Yes. I have always disclosed it every place I go.

Ms. ESHOO. Well, I wasn't here when you disclosed that, so I am glad to hear that, and I think it is important for the record, and I think it is important to highlight it for the record.

Now, in your statement, you said that broadband companies are subject to section 222 of the Communications Act. Now, I think for the record, we need to clarify this, because for telephone services, that is so, but not for broadband service. Do you agree with that?

Mr. CLELAND. Well, where we are is an evolution on that in the sense of telecom——

Ms. ESHOO. Well, I mean, just yes or no. We don't have to——

Mr. CLELAND. No, because it is a very complicated question in the sense that law enforcement and other things——

Ms. ESHOO. I mean, it is very important about the obligations under 222. Telephone services come under that obligation, but broadband services do not. So what I am doing is, I am differing with you in terms of what it is in your statement, so we are just going to leave it at that.

Now, let me get to this whole issue of how we achieve the kind of privacy and the implementation of that as all of this continues to be broadened out, because the Internet is going to keep growing. There always are going to be new ways of getting to people, trying to attract them to buy things, to sell things, but we don't want that used against them. So let me ask you, Mr. Dykes, do you think that there should be legislation that provides a statutory framework for what data can be collected, how it can be used, and how consumers can either opt in or opt out of the collection?

Mr. DYKES. Yes, I do.

Ms. ESHOO. You do?

Mr. DYKES. Yes, absolutely. I said in my testimony, we differently support a base privacy law across all industries that is technology neutral.

Ms. ESHOO. Let me ask the whole panel this. I am concerned that greater innovations in network capacity, data speeds, storage, and that more data containing potentially harmful software will be encrypted and then escape the current network of firewalls. Is this a legitimate fear? I mean, should government be addressing this?

Mr. DYKES. Well, in my view, no, it isn't. The Internet today operates with secure sites such as banks that do for the most part display their information in a secure manner, and that is appropriate because there really isn't—people shouldn't be looking at that date, and it doesn't really have commercial value for advertisers anyway. In other areas where it is a travel site, the innocuous categories that we track such as travel or automotive, for example, those are also subject to the search engines wanting—and they want the search engines to know that they have those subjects and so there is a natural process for sites to not want to be secure so that in fact they can be part of the search process and other links, et cetera, and so——

Ms. ESHOO. But I don't know from your answer whether this is a legitimate fear on my part.

Mr. DYKES. Well, my point is that—actually Mr. Reed previously expressed that fear, and what I am saying is, that I don't think that that is a fear, because we keep our characterizations at a sufficiently high level that people are not going to be fearful, and that is why we have to continue to publicize this, that we have very strong privacy controls, no personally identifiable information, and

we are only tracking innocuous categories mapped against those anonymous profiles.

Mr. MARKEY. The gentlelady's time has expired.

Ms. ESHOO. Thank you, Mr. Chairman, and can I just make a very quick observation? It is the first time in telecommunications testimony that J. Edgar Hoover has come into it. I don't know whether Mr. Cleland is referring to some kind of telecom cross-dressing, or what. I just wanted to highlight that.

Mr. MARKEY. I thank the gentlelady. The chair recognizes the gentlelady from California, Ms. Solis.

Ms. SOLIS. Thank you, Mr. Chairman, and I want to applaud you for having this very important hearing. When I read about the background on this, of course I am concerned coming from California where we have, I think, a lot of stricter rules in place that look at two-party wiretapping, and I want to get feedback from Ms. Cooper and Mr. Dykes on that and how you are going to deal with States like mine, but I have a couple of questions, two concerns. One is, you are able to profile who I am because I go on the Internet. You can see my likes, dislikes or whatever. But what about those people that may have language barriers or that may be senior citizens who could be gullible to specific types of unscrupulous advertisers or individuals who at a certain point can determine some vulnerabilities, and people in my community, Latinos and others, at a certain age, what have you, could be vulnerable to folks that take advantage of them, and specifically targeting advertisements at them, which we know happens now even in the print media and television, but mostly print. Many in our community are taken advantage of. I am concerned about predatory types of movement that could happen and how we detect that and how we can really help consumers who are maybe not language literate or because they speak only Spanish. So I want to ask Ms. Cooper if you can talk about what I have raised. But those are some of the concerns that I am thinking about out loud right now.

Ms. COOPER. I think the concern that you raise is legitimate, and the broader context in which we have discussed this concern is how these behavioral profiles that are getting created about consumers are really used. It is one thing to target a car ad to someone who has been interested in buying cars, but it is another thing to abuse the profiles as you are talking about to target vulnerable populations or to use the profiles for decisions about things like credit or employment or insurance, and because it is kind of a black box and we don't really know all of the ways that these profiles are being used and it is really invisible to the consumer. They, as we discussed already, don't even know that this kind of tracking is going on, but even if they do know, it is extremely difficult, if not impossible, for them to find out what the profile says, who it has been sold to, who else is using it, how it is being used, and so I think we still have a lot of work to do to find out what all of those secondary uses are and who is conducting them and if that is even OK. I think if information is collected for one particular purpose, even if consumers are informed and they opted in to that, that doesn't mean that there is a license to use it for all these other purposes.

Ms. SOLIS. Can you address the two-party wiretapping issue?

Ms. COOPER. Sure. So there are some States like California whose wiretapping laws require consent from both parties to the communication, so on the Internet, that would be both the consumer and the Web site that the consumer is visiting. In the context of the wiretapping laws, there is not a lot of case law about how those apply specifically to the Internet. There are telephone cases, and in some cases, if you have a call going from one State to another, the one-party-consent case trumps, so there only needs to be consent from one party. If you have a call coming from a two-party State to a one-party State, in California, there is some case law that shows that you still need consent from both parties, but it has only been applied in the telephone context.

Ms. SOLIS. So would you encourage us as our subcommittee kind of mulls through this to look at potential frameworks or something that could address this issue?

Ms. COOPER. Absolutely. I mean, there is the federal wiretapping laws on the books, which we think are fairly clear on their application to this model, but as we have been discussing today, there are all these other kinds of data collection going on which don't fall under that framework, and we certainly think that is an area of work good for this committee.

Ms. SOLIS. I have 17 seconds. I am sorry. Mr. Dykes.

Mr. DYKES. Well, on your first question, I agree with Ms. Cooper. It really is the responsibility of all advertisers and advertising companies to have responsible behavior, and so the questions that you raise are really not specific to ISP-based advertising because, as the panel has noted, there is lots of this data collected in many ways, and so, for example, as an industry, we don't advertise and the laws require us not to advertise to children, for example, and so—but as responsible advertisers, we observe the types of concerns that you have, and I don't think people in our industry would cross them, responsible companies.

With regard to your second question, as I said previously, I have spoken to my lawyers on that, and they have not identified any legal barrier to operating in any State, but we would be happy to work with your staff to further elaborate on that.

Ms. SOLIS. You said something earlier though that business has a legitimate role because they are paying for this access. So where do you draw the line to say that maybe some of these folks that are paying may not be—how could I say—honest in the way that they are targeting, for example, alcohol and tobacco? There are certain populations that we know industries target. Those are questions that I have concerns about.

Mr. DYKES. So the way that is generally handled is that the industry through industry associations certifies certain companies to say that we act responsibly, we operate within these standards, and the advertisers advertise with companies who meet those standards, and so there is a role for the advertisers themselves to have some policing to only advertise with companies that operate in a responsible——

Mr. MARKEY. The gentle——

Mr. DYKES [continuing]. Manner, and that I think is the effective way short of a law on the subject. Self-policing does occur in this industry and I think has been reasonably effective.

Mr. MARKEY. The gentlelady's time has expired. The gentleman from Florida has an additional question.

Mr. STEARNS. Just two questions, Mr. Chairman.

The first is just to clarify. The gentlelady from California brought up Mr. Cleland, what his invested interest was. He disclosed it, and I think just to set the record straight, Ms. Cooper, since the gentlelady brought up funding, I note that according to CDT records, your organization received almost 10 percent of its funding from e-commerce companies such as Google and Yahoo. I just wanted to confirm that. Are you still receiving funding from these companies?

Ms. COOPER. We are. We actually have a very broad base of funding. It is about 50 percent from foundations and 50 percent from high-tech companies, all kinds of different high-tech companies.

Mr. STEARNS. Including Google and Yahoo?

Ms. COOPER. Yes.

Mr. STEARNS. And Mr. Dykes, I think this discussion we had today—and I commend the chairman for having this hearing. I think it is very enlightening, and I think you can sense from everybody's feelings that people are concerned that these deep pockets of information packets that you are going into without anybody knowing about it is a concern. Maybe you should just summarize and tell us this information you are seeking, what is it that everybody is getting so alarmed about so maybe you would allay their fears by just outlining just very simply what is the stuff that you are looking at?

Mr. DYKES. The end result is simply our noting that an anonymous profile qualifies for certain innocuous categories such as travel, automotive, other subjects like that. So they are very innocuous categories, because we don't want to get into sensitive subjects, pharmaceutical ads, for example. We stay away from the sensitive subjects, so it is innocuous categories mapped against anonymous profiles is the end result, and that is why——

Mr. STEARNS. Mr. Doyle mentioned health information, going to look for prostate cancer.

Mr. DYKES. We avoid that.

Mr. STEARNS. I mean, how do we know that you avoid that? Do we just take your word for it?

Mr. DYKES. Well, that is one of the reasons why we are having our system audited, so a Big Four firm can actually say that yes, they do what they say they do. So that is one important element. The other is industry standards around sensitive subjects that they are still being formed, but to the extent that the FTC or other government bodies create a definition around sensitive subjects, we certainly observe that. Meantime, we stay very, very conservative on——

Mr. STEARNS. Who does this auditing? When you say you are audited, who——

Mr. DYKES. We haven't named the firm, but we have indicated that we would have one of the Big Four audit firms audit our systems to ensure that we do what we say we do.

Mr. STEARNS. An accounting firm is going to audit you?

Mr. DYKES. Well, those firms—correct. Those firms also do auditing of the subject, as well on privacy standards, as well as accounting standards.

Mr. STEARNS. I don't know if that is going to provide a degree of confidence to think that an accounting firm is going to audit you to——

Mr. DYKES. There is such a thing as——

Mr. STEARNS [continuing]. Whether you are going into sensitive boxes of information, deep packets. I don't know, Mr. Dykes, whether that is going to calm the fears.

Mr. DYKES. Sir, there are actually standards on privacy audits.

Mr. STEARNS. And you can't announce how that accounting firm is today? Have you selected that——

Mr. DYKES. It hasn't been finally selected.

Mr. STEARNS. So you don't even have an accounting firm doing it yet?

Mr. DYKES. Well——

Mr. STEARNS. You are speculating that you will.

Mr. DYKES. Sir, we are a startup, so we are just—this is just——

Mr. STEARNS. This is the first stage, the early stage?

Mr. DYKES. Yes.

Mr. MARKEY. Can you try to pick a company, Mr. Dykes, that wasn't the accounting firm for the subprime loan scandal or the dot-com bubble or the Enron? Can you find an accounting company that maybe has a good track record over the last 6 or 7 years, not missing every major accounting scandal, and I don't know what company that might be, but you will be held responsible for anything they miss, by the way. I unfortunately have to say this. In most instances, the accounting firms miss the stuff that the industries want them to miss because they also have consulting contracts. It is not a good situation.

Do any other members have any questions that they might want to ask? Yes, Mr. Gonzalez.

Mr. GONZALEZ. Thank you very much, Mr. Chairman. Just quickly because as you can tell, I think we may have some differences of opinion on application, the exact answer, but make no mistake about it, we all really share the chairman's concern regarding privacy and the duties and obligations that are out there, because we truly believe the American public will be concerned about it. I don't want to overlook the fact that many consumers today are the beneficiaries of, quote, "free services through application companies," and that is very, very valuable, and the reason that they are free is because of advertising dollars, and we have to really understand the role of the advertising dollar out there in the Internet and how it has actually promoted its use and the quality of it and so on, and that can be a scary proposition, depending on what we do. If we do act, I think we have to be careful again of going about business models and then going on what Mr. Sabet said about broadband, and that is, if those pipes are big enough and we keep increasing them, we take excuses away from people who may want to manage them in a way that really deprives the fair use of the Internet the way Dr. Reed envisioned it and has envisioned it for a number of years. So we can't do anything again to impact or restrict the build-

out. Again, I am going to use the word robust in a different context of a broadband network, and that really does concern me.

Lastly, I am going to make this last observation. Whether it is an ISP and how they got to where they are or whether it is Google and how they got who they are, whatever we come up, I think we still have to acknowledge the reality of what Dr. Reed said, but I am going to go and use real quick, Mr. Chairman, a quote, and this was in regards to service by an ISP, and a Mr. Bob Williams said there really should be an onus on the regulators to see this kind of thing is done correctly, meaning the information sharing and collection, and Mr. Williams deals with telecom and media issues at Consumers Union, and this is what he said. He could have read some of the terms earlier when placing the order online, but he just clicked the accept button. Quote: "I am a hard-nosed consumer advocate type. I really should have examined it better than I did," he said. But he added he acted like most consumers because of the lack of alternatives. "You click the accept button because it is not like you are going somewhere else." And that is the backdrop and that is the reality, and I believe that we will be acting responsibly understanding those market forces.

Thank you very much, Mr. Chairman.

Mr. MARKEY. The gentleman's time has expired. Does the gentlelady from California have any additional questions?

So we are going to turn to our panel, and we are going to ask each of you to give us your 1-minute summary of what you want us to remember about this issue of privacy and the American people, and it might help if you told us whether or not you thought opt-in was a good standard. We are talking privacy generally here, not individual companies but just tell us what you think. Should that be the standard? Mr. Cleland?

Mr. CLELAND. Well, I think that we need to have a holistic, comprehensive, balanced approach to privacy law.

Mr. MARKEY. Would that be opt-in?

Mr. CLELAND. Since you have asked, I think what the problem is, when we now go to opt-in or opt-out and it is that binary question, we are a little bit like the problem we have with do-not-call, and because it is complicated, we may end up with a do-not-track where people, just because nobody is minding what is going on in the Internet, people get fed up, and they say well, just let me say somewhere that I don't want to be tracked with anybody, and so when we go with just opt-in or opt-out, what we are doing is, we are basically making something that is not simple real simple when there are a lot of different ways to skin this cat. So I am big on privacy, but one size doesn't fit all. But you do need to look at it comprehensively.

Mr. MARKEY. Mr. Sabet?

Mr. SABET. Yes, a quick summary here is, we really believe that privacy and the open Internet are directly linked, and what you do with the data as a customer of DPI technology is the key. So if you violate people's privacy to manage the Internet, the open Internet, we think that is the real harm here for consumers and the Internet ecosystem.

Mr. MARKEY. Thank you.

Dr. Reed?

Mr. REED. Well, I think opt-in is too glib. It really should be informed consent and understanding of what will happen to the information, that you are being tracked and in the case of the Internet where, for example, you could predict reliably the political affiliation and beliefs of somebody literally by who they are talking to, so if you just monitor who they are talking to, you don't have to know whether they are a Democrat or a Republican. You actually have a much more complex notion of—you have to know what kind of analysis and use will be made of the information and what limits are placed on it, whether it is just for advertising, just for advertising by certain advertisers, just for something, as opposed to selling the unvarnished analytical information for any possible use, and that I think is something that ought to be kept in mind. So start with opt-in, but go beyond it, to opt in to what.

Mr. MARKEY. Mr. Dykes?

Mr. DYKES. I think we need to recognize that the Internet today is more than 50 percent funded by advertising, and to adopt an across-the-board opt-in rule would substantially reduce the value of the advertising across the Internet, so I think that major harm could be incurred that way. So I think a more holistic view of it, but also a more fine-tuned view, such that we are sensitive to the type of data being collected before we decide what the rules should be, I think is the most appropriate way to answer that.

Mr. MARKEY. Ms. Cooper?

Ms. COOPER. I think consumers deserve to have informed, meaningful control over their data. Whether it is opt-in or opt-out, consumers need to be in the driver's seat with respect to what is happening to their data when they go online and when their data is existing offline. They need to be the ones who decide how their data gets to be used.

Mr. MARKEY. Thank you, Ms. Cooper, very much.

When people use the World Wide Web, they don't want it to turn into the wild, wild west when it comes to their personal information, and I think that this analogy which Dr. Reed introduced today is a good one, and it extends to the post office, it extends to FedEx or UPS, that this is just another means of delivering something that a consumer is interested in, and there should be a barrier that exists unless the consumer determines that they do want, in other words, this information to be compromised. What we have learned from Embarq and we have learned from Charter is that in their affiliation with NebuAd that these questions weren't asked from the get-go.

This is a very serious subject. It is one that goes right to the heart of who we are as Americans. Back in 1775 in my congressional district in Lexington, one of the things that was just absolutely agitating the colonists was that the British felt they could come right into your home. There was no search warrant. There was no one that could stop them, and they could just come in. And so the very principles of individual freedom, individual liberty, you are right not to have either the government or a private sector company coming into your life without your permission, is central to who we are as Americans. That is what we fought for. That is what we continue to fight for and try to spread around the rest of the world. We don't believe that either the government or private

sector companies have a right to come in without your permission unless there is a legally obtained warrant, and that is why we are talking about wiretapping laws here today. That is why we are talking about broad privacy laws that have been put on the books over the years. It is because it is a subject of constant debate in our country from our very inception.

So I think that what we are hearing today is strong sentiment from most members that clear notice and meaningful opt-in must be the standard by which cable and phone companies like Verizon or Comcast, to take the names of two companies that are more well known than Charter or Embarq, but if this trend extends, then that is who we will be talking about. We will be talking about these larger carriers who will have the capacity, unless we have some standards, to be able to use this information as a product, and I don't think that Americans really want that to be the standard, notwithstanding the advertising base that the Internet might be based upon. There might be a few companies that suffer if Americans decide that they don't want all of their information to just become something that is put together as an advertising profile of that individual. That is a price just a little bit too high to pay in order to have the Internet the way that a private sector company might want it to be there, and the same way that politicians might want to know all of the private sentiments of voters in their district and be able to get access to it, we can't get access to it. We can hope that they are going to vote for us on Election Day, but there is a certain limit beyond which we can't go in intruding into the privacy of Americans. But it is a natural instinct. Each of us up here would love to know everything that is going on in the homes of all 650,000 people in our district with regard to their political attitudes. That would be very helpful to us. But we can't, and there is a good reason why we can't, because these individuals have a right to their privacy, and the same thing extends over to their right to privacy from advertisers, their right to say no, I don't want you in my front door. When your mother is saying to you as a little kid, when you tell the person knocking on the door they are not home, tell them your mother is not home, but what are they really saying? What your mother is really saying is, we are not home to you, sir, on the front door knocking trying to get inside my home, and that is your right, and it should be your right as an American citizen not to let people inside your mail, inside your packages, inside your packets.

This packet-switched network that Dr. Reed and others invented is something that really goes right to the heart, and the principles that were established really go right to the heart of who we are, and Ranking Member Joe Barton, Chairman John Dingell, and I have already written to a cable and a phone company where either the notice or the opt-in choice was inadequate or missing. So we need to have remedial legal courses for some corporate general counsels, and we need to have the phone and the cable companies step up and clearly say what their policies will be, and as I have proposed previously, we need a comprehensive online privacy bill to close the gaps that exist with search engines and other sites.

So we thank each of you for your testimony. We intend on working very closely. We intend on really raising the profile of this issue

and any companies that are engaging in it so they can become more famous, more well known in terms of what they are doing, and this is going to become an escalating subject of attention for this committee and for the Congress, because any time anyone learns about it, their first thought is, I didn't know that that was happening with all of my information, and that just demonstrates that there has not been notice given to people.

So we thank all of you, and we intend on following up on this issue in the months and years ahead. With that, this hearing is adjourned.

[Whereupon, at 11:47 a.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

STATEMENT OF HON. JOHN D. DINGELL

Thank you, Mr. Chairman, for holding this hearing, and I thank the witnesses for being here.

Deep packet inspection (DPI) is part of the Internet now, and it will be part of the Internet in the future. That much is clear. However, any industry that includes a company whose motto is, "See Everything. Know Everything." is worthy of close scrutiny.

Our job today is to consider how best to balance the deployment of DPI with adequate protection of consumers' privacy. We must also consider the effects of DPI on competition and investment across the Internet.

An immediate concern is the targeted advertising that DPI makes possible. On Monday, Chairman Markey, Ranking Member Barton, and I sent a letter to the phone company Embarq. We expressed concern that Embarq conducted a trial in an unnamed community in its service area of a targeted advertising system that tracked customers' Web use without providing clear notice of the trial to subscribers. Not only did Embarq fail to give its subscribers a chance to opt in to the tracking, but it did not directly notify affected customers that they had a chance to opt out. I find the notion that a broadband provider would implement such tracking with no real notice to the customer to be deeply troubling.

We are in this position, because the Federal Communications Commission (FCC) has yet to establish any clear privacy protections for customers of wireline broadband services. In its rush over the last several years to deregulate broadband services, the Commission has failed to adequately protect consumers. When Chairman Martin testified before this Committee in March of 2007, I asked him when he would remedy this problem. He responded that the Commission would endeavor to act by the end of 2007. Clearly, much work remains to be done at the FCC.

We must also consider what DPI means for the future of the Internet. DPI can be used for legitimate and necessary purposes by broadband providers, such as to reasonably manage network congestion and protect against viruses. To the extent that they utilize DPI for these purposes, I have no quarrel with broadband providers. Unfortunately, DPI can also be used for nefarious purposes, such as unfairly blocking certain applications or slowing one Web site's traffic at the expense of another. We in Congress must be vigilant in the face of these and other abuses. The importance of an open and competitive Internet cannot be understated.

I hope today's witnesses will help the Committee in its examination of DPI by addressing a few questions. How should broadband providers notify subscribers they are planning to track customer Web use? Should providers be required to obtain opt-in consent? What privacy rules should apply to broadband providers? And how do we ensure that DPI does not stifle innovation on, and investment in, the Internet?

I thank the witnesses for being here, and I look forward to the testimony.
