Testimony of Gigi B. Sohn
President, Public Knowledge

Before the
U.S. Senate Committee on
Commerce, Science & Transportation

Hearing On:
Broadband Providers and Consumer Privacy

Washington, DC.
September 25, 2008

Testimony of Gigi B. Sohn
President, Public Knowledge

Before the
U.S. Senate
Committee on Commerce, Science, and Transportation

Hearing on:
Broadband Providers and Consumer Privacy

September 25, 2008

Chairman Inouye, Ranking Member Hutchison and Members of the Committee, thank you for giving me the opportunity to testify about broadband providers and consumer privacy. I'd like to focus today on the growing use of the collection of technologies known as "Deep Packet Inspection," or DPI, which has immense implications for the privacy rights of the American public. Over the past several months, Public Knowledge, in partnership with Free Press, has been analyzing these technologies and their impact on privacy and an open Internet. In June, our organizations published a white paper entitled *NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking*, which examined the technical and policy aspects of DPI. I applaud the Committee for its continued scrutiny of the use of these technologies.[1]

I. Introduction

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

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

[1] I would like to thank Public Knowledge's Equal Justice Works Fellow Jef Pearlman, Policy Analyst Mehan Jayasuriya, and Law Clerk Michael Weinberg for assisting me with this testimony.
[2] *See* Associated Press article, " Comcast blocks some Internet traffic", (October 19, 2007), *available at* http://www.msnbc.msn.com/id/21376597.

November 2007, calling for the Commission to open a formal investigation into the ISP's practices.[3]

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

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

In May 2008, Representatives Edward Markey (Chairman, Subcommittee on Telecommunications and the Internet) and Joe Barton (Ranking Member, Senate Committee on Energy and Commerce) sent a letter to NebuAd,[7] asking the company to put its pilot tests on hold, pending an investigation into the company's practices. A coalition of 15 consumer advocacy and privacy groups publicly voiced their support for this letter and urged the Congressmen to continue their investigation of NebuAd and other behavioral advertising companies.[8] In June 2008, Public Knowledge and Free Press released a technical analysis of NebuAd's behavioral advertising system, authored by networking researcher Robb Topolski.[9] The report revealed that NebuAd and its partner ISPs repeatedly violated the privacy of users,

---

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

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

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

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

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

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

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

with little or no notification that DPI equipment was being used. Following the release of the report, the House Committee on Energy and Commerce convened a hearing on the topic of DPI, wherein NebuAd CEO Bob Dykes was asked to testify.

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

II. Deep Packet Inspection

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

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

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

III. The Privacy Implications of DPI

It should be clear that the very nature of DPI technology raises grave privacy concerns. An ISP, by necessity, sees every piece of data a user sends or receives on the Internet. In the past, ISPs had little incentive to look at this information and the related privacy concerns provided a strong

[10] See John D. Dingell (Chairman, Senate Committee on Energy and Commerce), Joe Barton (Ranking Member, Senate Committee on Energy and Commerce), Edward J. Markey (Chairman, Subcommittee on Telecommunications and the Internet), Cliff Stearns (Ranking Member, Subcommittee on Telecommunications and the Internet), *Letter to ISPs* (Aug. 1, 2008), *available at* http://markey.house.gov/docs/telecomm/letter_dpi_33_companies.pdf.

deterrent against doing so. However, now that technology is widely available to make use of and monetize this information, companies are exploring the limits of what they can do permissibly.

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

1. ***Purpose***: What purpose is the collected data being used for?

2. ***Collection***: How is the data collected and utilized?

3. ***Consent***: How was affirmative informed consent obtained?

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

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

A. Purpose

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

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

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

B. Collection

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

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

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

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

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

C. Consent

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

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

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

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

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

IV. ISP Disclosures

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

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

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

---

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

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

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

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

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

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

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

The level of detail in the disclosures also fell far short of the minimum that is necessary for customers to make an informed decision. For example, CenturyTel sent an email informing users only that it had "updated its Privacy Policy concerning Internet Access Services" and provided a web link to the updated policy.[17] The policy in question stated only:

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

A later letter sent out by CenturyTel stated the following:

> CenturyTel continually looks for ways to improve your overall online experience. In that regard, we have enhanced our High-Speed Internet service by working with partners to provide targeted, online advertising for your convenience and benefit. Targeted, online advertising minimizes irrelevant or unwanted ads that clutter your Web pages. If you do not wish to receive targeted, online

[16] *See* Response Letter of Knology 2.
[17] Response Letter of CenturyTel 3.
[18] *Id.* 3 (emphasis added).

> advertisements, or if you would simply like more information about CenturyTel's use of online advertising, third-party ad servers and the measures you can take to protect your privacy, please review our Privacy Policy by visiting http://www.centurytel.com/Pages/PrivacyPolicy/#adv.[19]

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

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

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

V. Current Law

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

---

[19] *Id.* 3-4.

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

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

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

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

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

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

---

[21] *See id.* at 6-9.

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

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

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

society where Internet services are increasingly used to transmit personal and sensitive information, this is clearly problematic.

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

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

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

As with Section 222, Section 631 specifically protects sensitive information that network operators are uniquely positioned to collect. However, unlike Section 222, which applies to

[25] 47 U.S.C. § 222
[26] *See* 47 U.S.C. § 222(c)(1).
[27] *See* 47 U.S.C. § 222(d).
[28] *See* 47 U.S.C. § 222(c)(3), (h)(2).
[29] *See, e.g.*, Verizon, http://www.verizon.com/.
[30] *See National Cable & Telecommunications Assn. v. Brand X Internet Services*, 545 U.S. 967 (2005).
[31] *See* 47 U.S.C. § 551(b).
[32] *See* 47 U.S.C. § 551(c)(1).
[33] *See* 47 U.S.C. § 551(a)(2)(A).
[34] *See* 47 U.S.C. § 551(c)(2).

phone customers but not Internet service customers, Section 631 is written to apply to both cable television subscribers and cable Internet subscribers.[35]

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

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

VI. Fixing the Law

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

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

[35] *See* 47 U.S.C. § 551(a)(2)(C)(ii).
[36] Statement of Congressman Edward Markey, 142 Cong. Rec. H1145-06 (Feb. 1, 1996).
[37] The FCC has already presented us with an example of how Commission action and ISP disclosures can be used to help protect Internet users from privacy invasions and impermissible network management practices. In its order finding that Comcast's interference with customer traffic was not reasonable network management, the Commission ordered Comcast to fully disclose the details of its past and planned practices, including use of DPI. *See* Federal Communications Commission, *Memorandum Opinion and Order* ¶ 54-56 (August 1, 2008), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf. Given the authority, the Commission could make this type of disclosure an industry-wide baseline to ensure that customer's decisions about granting consent are based on good, complete information backed the force of law.

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

VII. Conclusion

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

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