CENTER FOR DEMOCRACY & TECHNOLOGY

Statement of Leslie Harris
President and Chief Executive Officer
Center for Democracy & Technology

Before the House Committee on Energy and Commerce,
Subcommittee on Communications, Technology and the Internet

# "The Privacy Implications of Deep Packet Inspection"

## April 23, 2009

Chairman Boucher 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 privacy implications of the technique known as "deep packet inspection" (DPI).

In CDT's view, DPI poses serious challenges both to privacy and to the openness and innovation that are the hallmarks of the Internet. The success of the Internet can be traced in part to its defining "end-to-end" principle: the simple idea 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 gatekeepers.

The end-to-end principle is supported by a policy framework that generally protects Internet service providers from intermediary liability (i.e., liability for content that originates with users) unless the network operator is directly involved in the creation of the content.[2] For decades, adherence to the end-to-

---

[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).

[2] As part of the Telecommunication Act of 1996, Congress enacted broad immunity for ISPs and online service providers from liability for content posted by customers or third parties. See 47 U.S.C. § 230. Section 230 has been a critical foundation for the huge explosion of "Web 2.0" content and services on the Internet. For information on the origin and

CENTER FOR
DEMOCRACY
&
TECHNOLOGY Keeping the Internet Open, Innovative, and Free
1634 I St., NW, Suite 1100, Washington, DC 20006 • v. +1.202.637.9800. • f. +1.202.637.0968 • http://www.cdt.org

end principle has preserved the Internet as a trusted platform and has supported unparalleled levels of innovation, economic activity, and individual expression.

In recent years, however, massive growth in data processing power has spurred the development of new "deep packet inspection" (DPI) technologies that potentially allow Internet service providers (ISPs) and other intermediaries to analyze all of the Internet traffic of millions of users simultaneously. The use of DPI technology, though still in somewhat limited deployment, raises profound questions about the future of privacy, openness, and innovation online.[3]

It is important to stress at the outset that *all* applications of DPI raise serious privacy concerns because all applications of DPI begin with the interception and analysis of Internet traffic. Policymakers must carefully consider each use of DPI and balance the perceived benefit of its use against the risks to privacy and civil liberties, as well as to the Internet's character as an open platform. CDT believes that only rare uses of DPI will be acceptable after such a balancing. Today, DPI applications include management of network congestion, detection of network threats, content blocking for intellectual property protection and child safety, behavioral advertising, and government surveillance.

CDT has been outspoken in opposition to government-mandated content filtering by ISPs[4] and in support of the call for Internet neutrality legislation to prohibit discrimination between Internet data streams.[5] While we will briefly discuss those issues below, our testimony today will principally focus on the privacy implications of DPI. This statement builds on testimony we gave to this Subcommittee last July,[6] taking into account developments since then.

Unlike other media, the Internet is decentralized. Control is vested at the ends of the network with its individual uses, and its end-to-end communications are largely unfettered. Consumers expect that their Internet transmissions will not

---

scope of Section 230, see an amicus brief that CDT filed with the 9th Circuit in 2008, available at www.cdt.org/privacy/spyware/20080505amicus.pdf.

[3] 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 usage or service plans. This testimony focuses exclusively on packet inspection and analysis by intermediaries at the middle of the network rather than at the endpoints.

[4] 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. 15, 2004), http://www.cdt.org/speech/pennwebwebblock/20040915highlights.pdf.

[5] 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.

[6] Alissa Cooper, Testimony of Alissa Cooper 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), http://cdt.org/testimony/20080717cooper.pdf.

be intercepted or analyzed en route by an intermediary.  DPI systems defy this expectation, threatening the basis for consumer trust online.  The use of DPI is also at odds with well accepted "Fair Information Practices,"[7] can be disruptive to Internet and Web functionality,[8] and may – in some instances – run afoul of existing communications privacy laws.[9]

Companies that use DPI to track consumers' online activities to serve targeted advertisements or to manage network congestion often stress the anonymous and limited nature of the information they compile.  However, the privacy concerns that arise from the use of DPI begin with the interception, diversion or copying of substantially all of the Internet traffic of all subscribers.  Just because ISPs or advertising networks may use only a small portion of what is captured and do not retain other information does not diminish the breadth and intrusiveness of the initial data capture.

DPI technologies are being deployed within a technological environment where consumers are sending more personal data through their ISPs than ever before, and more data is being collected, retained for longer periods, and shared among more parties.  However, even while existing sectoral privacy protections have been far outpaced by technological innovation, our nation still has no baseline consumer privacy law.  Self-regulation, while important, has proven to be insufficient to protect privacy in the online context.  For all of these reasons, Congress needs to take a comprehensive look at the current and emerging practices associated with DPI, and should approach the technology with great skepticism. Congress should also take a comprehensive look at online privacy issues at large.  We recommend that Congress take the following steps:

- Building on the inquiries posed last year by Chairman Markey,[10] the Subcommittee should seek additional information directly from ISPs and their partners about how they are using DPI.  Specifically, for what purposes are ISPs currently using DPI?  Are additional uses anticipated? What information are ISPs collecting or examining, and how long is that information retained?  Are ISPs using DPI on a continuous basis or only intermittently, such as in response to security incidents or to sample

---

[7] The FIPs are a set of generally accepted principles for protecting the privacy of personal data in a variety of contexts. The FIPs have become a standard model for privacy protection frameworks.  *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.

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

[9] *See 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,* Appendix A to the Statement of Alissa Cooper Before the Subcommittee on Telecommunications and the Internet of the House Committee on Energy and Commerce, 110th Cong. (2008), http://cdt.org/testimony/20080717cooper.pdf.

[10] *See* Congressman Ed Markey, *Lawmakers Ask Top Broadband and Internet Co.s to Detail Use of User-Tracking Tech,* Aug. 1, 2008, http://markey.house.gov/index.php?option=com_content&task=view&id=3425&Itemid=141.

traffic for aggregate usage analysis?  Are third parties paying ISPs to use DPI to identify or manipulate or divert certain content?  If so, for what purposes?  In what circumstance – if any – have ISPs obtained the consent of their customers to conduct DPI?  How has consent been obtained?   In what circumstances do ISPs believe consent is not required?

- Based on its ongoing research into DPI and other critical privacy concerns, the Subcommittee should take the lead in developing baseline, technology-neutral consumer privacy legislation, based on Fair Information Practices, that will address not only DPI but also the range of privacy issues facing companies and consumers.  Such legislation could limit the use of DPI and provide safeguards for its deployment in those cases where it is acceptable.

- Congress should work to enact Internet neutrality legislation that specifically addresses content discrimination by Internet service providers.  This legislation should avoid overly detailed rulemakings or specific technical mandates and should respect ISPs' needs to secure their networks and manage congestion, while ensuring that discriminatory practices are not allowed to create new Internet gatekeepers and erode the medium's openness to innovation.

- Congress should examine and strengthen the communications privacy laws regarding government surveillance to cover new services, technologies and business models with consistent rules.  In particular, the Electronic Communications Privacy Act (ECPA) needs to be revised to better reflect modern uses of digital communications technology.  While that effort must be broader than DPI, and will probably fall under the jurisdiction of another Committee, the effort may benefit from the record created here.

## ◪ Understanding Deep Packet Inspection

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 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. However, 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,[11] CDT disagrees. Application headers have

---

[11] *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.

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.

## ◤ The Privacy Risks of Deep Packet Inspection

CDT believes that DPI in nearly every context raises substantial privacy concerns. 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 along 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 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 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, DPI runs the risk of damaging consumer confidence in the medium.

Certain characteristics of DPI also seriously challenge traditional Fair Information Practices. Consider the FIPs principle of limiting data collection to what is necessary to complete the task at hand. How can this idea be squared with DPI equipment that has the capability to collect and analyze every single Internet packet for millions of Internet users?[12] Although DPI can be implemented with limits on the types of data collected, the legal framework

---

[12] *See* Procera, PacketLogic PL10000 Series, http://www.proceranetworks.com/images/datasheets-2008-11-03/DS-PL10000-11-3-08.pdf (last visited Apr. 19, 2009).

provides almost no useful guidance for where such limits should be set, given the lack of a comprehensive privacy law in the U.S.

Transparency is another core FIPs principle that DPI challenges. DPI equipment vendors compete on how invisible an impact their technology will 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 almost entirely undetectable. This means ISPs and others may be able to deploy DPI systems that are invisible even to sophisticated consumers. With DPI hidden from view, consumers will be largely unaware that their data streams are being intercepted and thus 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 intercepts and 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 used to re-identify individuals when combined with other information. In this way, DPI tends to sweep in personal information even when the party doing the packet inspection does not seek such information.

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.

Finally, as DPI technology matures and becomes more widely deployed, it will also pose serious threats in terms of government surveillance. As a general

---

[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").

matter, the rules for government surveillance have failed to provide adequate privacy protection in the face of technological change. The implications of DPI remain largely unexplored, although the government has clearly displayed a seemingly unlimited appetite for electronic surveillance. For criminal investigations, government monitoring of the content of communications is still limited by the principles of probable cause and particularity, but the rules for monitoring of transactional data are very weak.

In the context of national security, the 2008 changes to the Foreign Intelligence Surveillance Act may have permitted bulk collection of both transactional data and the content of international communications. Last week's revelation in the New York Times of significant "over collection" illustrates the risks of permitting government surveillance without adequate judicial checks and balances.[14] The problem is that the government can use any capability deployed for commercial purposes. Widespread deployment of DPI, whether or not it is initially used for legitimate commercial purposes, would offer to the government a staggering ability to closely and constantly monitor Internet communications. It is probably fair to say that there are not in place today adequate rules of judicial approval and oversight to control the use of that capability.

In sum, DPI poses unique risks to individual privacy. Moreover, once the technology is acquired for a legitimate purpose such as responding to network threats, it will be hard to draw the line at ever more intrusive uses as third parties approach the network operators with proposals to monetize Internet traffic and the government makes greater demands. Given DPI's intrusive nature, this Subcommittee is right to closely examine its current and projected uses and consider its risks.

## ◩ Concerns in Addition to Privacy

In addition to the foregoing privacy concerns, which CDT believes are implicated by all uses of DPI, the practice can raise a number of other concerns which will vary by specific application. While the focus of this testimony is on the broad privacy consequences of DPI, this section will briefly address some additional concerns which merit serious consideration as Congress continues its investigation of DPI.

---

[14] Eric Lichtblau and James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, New York Times April 15, 2009, http://www.nytimes.com/2009/04/16/us/16nsa.html.

Using DPI to identify specific types of communications for the purposes of prioritization – for example, in response to network congestion or pursuant to ISP partnerships with content providers – can undermine the openness of the Internet and threaten its status as a platform for innovation. Historically, open and standardized technical protocols have enabled innovators to develop and deploy new content and services on the Internet without needing to seek permission from any gatekeeper. DPI could place the power to discriminate among content and services in the hands of network-level intermediaries, threatening this openness and hindering future innovation. CDT believes that network providers should not be in the business of picking winners and losers from among Internet content and services,[15] and some uses of DPI could increase the risk that this could happen.

Using DPI to identify and filter or block certain illegal or undesirable content, for such diverse purposes as child protection or copyright enforcement, would raise additional concerns. Content filters can suffer from overbreadth problems, blocking material beyond that for which they are intended, including constitutionally protected material.[16] Filters designed for copyright enforcement may fail to account for fair use and the possibility that a particular Internet user might be authorized to make a particular intercepted transfer. Perhaps most importantly from a policy perspective, broad use of DPI to detect and block illegal or undesirable content on the network could undermine U.S. advocacy for Internet freedom in repressive regimes around the world. As one example, the Chinese government has already deployed DPI filtering to censor material it finds objectionable from the Internet.[17] U.S. efforts to press foreign regimes to abandon Internet surveillance and censorship may be undercut if we are seen to engage in similar behavior with respect to our own designated classes of forbidden content.

## ⬊ Assessing Potential Uses of Deep Packet Inspection

In assessing specific uses of DPI, the first thing to note is that some may already be regulated or prohibited under the federal Wiretap Act and the Cable Act. In a memo issued last July, CDT explored in some depth the application of the

---

[15] CDT has proposed a framework for Internet neutrality legislation that specifically addresses the issue of content discrimination by ISPs. *See* CDT, Transition Memo for President Barack Obama: Internet Neutrality, November 2008, available at http://cdt.org/transition/InternetNeutrality.pdf.

[16] *See supra* note 4.

[17] Richard Clayton, Stephen J. Murdoch, and Robert N. M. Watson, *Ignoring the Great Firewall of China*, presented at 6th Workshop on Privacy Enhancing Technologies, Robinson College, Cambridge, United Kingdom (June –- June 30, 2006), http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf.

Wiretap Act and related laws to DPI.[18] We concluded that certain uses of DPI to compile behavioral advertising profiles would probably run afoul of the Wiretap Act absent unavoidable notice and "opt-in" consent. Last September, without expressly embracing our legal analysis, AT&T, Verizon, and Time Warner Cable committed to providing notice and obtaining affirmative consent from consumers before tracking their Web activity for targeted online advertising.[19] However, the boundaries of the Wiretap Act are not clear in all contexts. Moreover, the Act was last modified more than 20 years ago and has not kept pace with technology. It simply does not provide sufficient protection to consumers against DPI's risks.

Also, consent has its limitations. For example, it is still difficult to see whether and how unavoidable notice and true consent can be provided in settings where there is little regular communications between the ISP and the customer. Consent is further complicated in the residential context or any other situation where more than one person uses a single Internet connection.[20] As a general matter, online providers have not yet provided an opt-out mechanism in the advertising context that the majority of consumers can effectively utilize, and applications of DPI for behavioral advertising would seem to suffer from the same limitations. 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 successfully negotiate such opt-out processes. Moreover, while a robust notice and opt-in regime might mitigate some privacy concerns of DPI for behavioral advertising, consumers may lack an incentive and are therefore highly unlikely to opt-in to the use of DPI for content filtering or congestion management.

Looking beyond the limitations of consent and the current legal framework, ISPs and policymakers should approach DPI with great skepticism. They should carefully weigh any expected benefits of a proposed use of DPI against the substantial privacy and other risks outlined above. They also should consider whether there may be alternative methods for achieving their goals, with a strong preference for means that do not require sweeping inspection of Internet communications at the ISP level.

---

[18] *See 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*, Appendix A to the Statement of Alissa Cooper Before the Subcommittee on Telecommunications and the Internet of the House Committee on Energy and Commerce, 110th Cong. (2008) http://cdt.org/testimony/20080717cooper.pdf.

[19] See Broadband Providers and Consumer Privacy, Hearing before the Senate Committee on Commerce, Science and Transportation, September 25, 2008
http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=778594fe-a171-4906-a585-15f19e2d602a.

[20] Paul Ohm, The Rise and Fall of invasive ISP Surveillance, University of Illinois L. Rev (2009), Pgs. 62-65, http://ssrn.com/abstract=1261344.

In terms of alternatives to DPI that do not raise the same concerns, network management offers a good example. It has been proposed that an ISP could use DPI to help manage network congestion, by peering into the content of subscribers' traffic to try to identify which traffic appears to need delivery priority and which does not. But alternative congestion management techniques could serve the same goals without inspecting any packet payloads.[21] A congestion management tool that focuses on addressing high volume users responsible for the majority of network traffic does not require DPI because it is content-agnostic. It needs to know the overall volume of bandwidth each user is consuming, but does not care what the content is.

Another proposed tool for DPI is to identify network threats such as spam, malware, and denial-of-service attacks. There may be instances where this would be the most effective and efficient technique. There are also, however, a variety of other security tools available, including tools that operate at the endpoints of the network. Spam filters and anti-malware software, for example, can be deployed at the application level by individual computer users (on email servers, for example), on Web servers, and so forth. There is also a big difference between using DPI sporadically, in response to a current threat or attack, and employing it on an ongoing basis. Security techniques based on DPI should be employed only in targeted fashion when they are truly superior to available alternatives.

DPI aimed at reducing online copyright infringement is likewise just one of a number of possible anti-infringement tools. Other means include lawsuits against infringers and the DMCA's notice-and-takedown regime. Just as important, there are steps that can and are being employed at the edges of the network. Individual websites and content hosting services, such as YouTube and MySpace, actively employ filters to identify copyright-infringing material.[22] Such filtering raises a variety of policy questions, but it does not involve ISP-level DPI and hence does not raise the same level of privacy concerns.

In short, ISPs and policymakers assessing a proposed use of DPI need to consider whether the practice is legal, whether the benefits would really outweigh the substantial costs and whether there are preferable alternatives. CDT believes strongly that this analysis will rarely favor the use of DPI on a broad scale.

---

[21] *See, e.g.,* Filing of Comcast, Inc., *In the Matter of Broadband Industry Practices*, WC Docket No. 07-52 (September 19, 2008), http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6520169715.

[22] *See, e.g.,*YouTube.com, "Audio ID and Video ID," http://www.youtube.com/t/contentid.

## The Privacy of Location Information

The Subcommittee has also expressed interest in privacy issues relating to location information.  Although disclosure of location information can sometimes involve deep packet inspection, such disclosure more commonly happens through a location-based service or application without DPI.  However, CDT strongly shares the Committee's concern about the privacy of location information.

The ubiquity of increasingly high-powered mobile devices has already spawned the Internet's first generation of location-based services and applications.  As the accuracy of location data improves and the expense of calculating and obtaining it declines, location may well come to pervade the online experience.  While the increasing availability of location information paves the way for exciting new applications and services, the increasingly easy availability of location information raises several different kinds of privacy concerns.  Ensuring that location information is transmitted and accessed in a privacy-protective way is essential to the future success of location-based applications and services.

Because individuals often carry their mobile devices with them, location data may be collected everywhere and at any time, often without user interaction, and it may potentially describe both what a person is doing and where he or she is doing it.  For example, triangulation of an individual's mobile phone can reveal the fact that he was at a particular medical clinic at a particular time.  The ubiquity of location information may also increase the risks of stalking and domestic violence if perpetrators are able to use (or abuse) location-based services to gain access to location information about their victims.

Furthermore, location information is and will continue to be of particular interest to governments and law enforcers around the world.  Standards for government access to location information held by companies are unclear at best and far too low at worst.[23]  The existence of detailed records of individuals' movements should not automatically facilitate the ability for governments to track their citizens, but in many cases, laws dictating what government agents must do to obtain location data have not kept pace with technological evolution.

---

[23] *See* Center for Democracy & Technology, "Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology" (2006), available at http://www.cdt.org/publications/digital-search-and-seizure.pdf.  Over the past few years courts have split on the standards protecting location information, with a majority of courts rejecting governmental arguments for a low standard.  *See, e.g., In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communications Service to Disclose Records to the Government*, No. 07-524M (W.D. Pa. Sept. 10, 2008), (available at http://www.eff.org/files/filenode/celltracking/lenihanorder.pdf).  CDT joined an amicus brief that details the key legal argument for a strong standards, available at http://www.cdt.org/security/20080731_lenihan_amicus.pdf.

CENTER FOR DEMOCRACY & TECHNOLOGY

Location-based services can be built to protect against privacy risks by, for example, obtaining affirmative user consent, strictly limiting how long location data is retained, and allowing users to set the precision of their location information. But the comprehensive and sensitive nature of location information collection demands that location-based services be deployed with such heightened protections in place.

CDT believes that there are at least three specific measures needed to protect the privacy of location information, the first two of which would benefit from Congressional action:

- First, the disclosure of precise location information in a commercial context must only be made with specific, informed, opt-in consent in which a user has the ability to selectively disclose location only to trusted parties. [24] As Congress contemplates enacting baseline consumer privacy legislation, such a requirement could easily be part of a broader framework governing sensitive consumer data.

- Second, the standards for government and law enforcement access to location information must be amended to make clear that a probable cause warrant is required for the government to obtain location information.

- Third, location-based services and applications should follow technical standards that give users clear control over the use of their location information and that require the transmittal of privacy rules with the location information itself.[25]

As the Committee is aware, location information is particularly sensitive, and location-aware applications are increasingly pervasive. We look forward to working with the Committee to address the privacy concerns raised by the increasing availability of location information.

---

[24] Some of the location-based social networks and services have been very cautious about privacy, while unfortunately, some companies are seeking to distribution location with little or no privacy protections.

[25] CDT has worked since 2001 within the Internet Engineering Task Force (IETF) on the development of a location privacy standard named Geopriv. *See* Geopriv Working Group Charter, http://www.ietf.org/html.charters/geopriv-charter.html. For more information about this standard, *see* John Morris and Jon Peterson, *Who's Watching You Now?*, IEEE Security and Privacy Magazine, Vol. 5, Issue 1 (January/February 2007) (available at http://www.cdt.org/publications/20070100ieee.pdf). *See also* Alissa Cooper and John Morris, Binding Privacy Rules to Location on the Web, Proceedings of the 2nd International Workshop on Location and the Web, LOCWEB '09 (Boston, Mass., Apr. 04, 2009) (available at http://www.cdt.org/privacy/LocWebFinal.pdf).

## 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, following up on the inquiries made last year, we urge the Subcommittee to seek and compile for the public record additional information directly from ISPs and their partners about how they are using DPI. Specifically, for what purposes are ISPs currently using DPI? Are additional uses anticipated? What information are ISPs collecting or examining, and how long is that information retained? Are ISPs using DPI on a continuous basis or only intermittently, such as in response to security incidents or to sample traffic for aggregate usage analysis? Are third parties paying ISPs to use DPI to identify or manipulate or divert certain content? If so, for what purposes? In what circumstance – if any – have ISPs obtained the consent of their customers to conduct DPI? How has consent been obtained? In what circumstances do ISPs believe consent is not required?

- This Subcommittee should set a goal of enacting within 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, including requiring transparency and notice of data collection practices, minimizing data collection and retention, 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.

- Congress should work to enact Internet neutrality legislation that specifically addresses content discrimination by Internet service providers. This legislation should avoid overly detailed rulemakings or specific technical mandates and should respect ISPs' needs to secure their networks and manage congestion, while ensuring that

discriminatory practices are not allowed create new Internet gatekeepers and erode the medium's openness to innovation.

- 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.

## ◤ 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.

CENTER FOR
**DEMOCRACY**
**TECHNOLOGY**

**FOR MORE INFORMATION**

Please contact: Leslie Harris, (202) 637-9800, leslie@cdt.org