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.

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

---

[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.

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 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.

---

[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).

[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.

- 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 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 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

[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.

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]

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

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

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.

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

---

[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").

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 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.

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.

[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)).

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 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.

---

[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.").

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 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

---

[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).

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]

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

---

[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.

[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.

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 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.

---

[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.

[24] 18 U.S.C. § 2511.

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 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,

---

[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.

[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).

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.

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

[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.

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.

CENTER FOR DEMOCRACY & TECHNOLOGY

FOR MORE INFORMATION

Please contact:
Alissa Cooper, CDT Chief Computer Scientist
(202) 627-9800
http://www.cdt.org

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 8th, 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

[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.

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 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

---

[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.

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.

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

[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.

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.

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.

---

[8] *Id.* § 2511(3)(b)(ii).

[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

---

[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).

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.

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

---

[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.

"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 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

---

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

[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).

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 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

---

[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).

[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 Bd. 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.

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 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

[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).

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 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

---

[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.

[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).

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 ISP's individual subscribers, as it would be impossible to obtain consent from every single Web site that every subscriber may conceivably visit.

State Laws Requiring Two-Party Consent to 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.

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 . . .

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

[38] Fla. Stat. § 934.03(1).

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

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 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]

---

[40] Cal. Pen. Code § 631(a).

[41] *Id.*

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

[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.

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.

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.

FOR MORE INFORMATION

Please contact: Jim Dempsey, Ari Schwartz, or Alissa Cooper
202-637-9800