Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
A National Broadband Plan	)	GN Docket No. 09-51
for Our Future	)	

To: The Commission

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

June 8, 2009

Pursuant to the Federal Communications Commission's Notice of Inquiry regarding the Request for Comments on A National Broadband Plan for Our Future,[1] the Electronic Privacy Information Center submits the following comments regarding civil liberties and privacy protections in the national broadband plan. Thank you for the opportunity to comment on this important and much-needed initiative.

The Electronic Privacy Information Center (EPIC) is a non-partisan public interest research center in Washington, D.C., established in 1994 to focus on emerging privacy and civil liberties issues. We have a particular interest in communications networks and consumer privacy. EPIC began with a national campaign -- the first online petition -- to protect the freedom to use encryption, a critical technique for network privacy and security. For the past 15 years, EPIC has pursued many of the critical network privacy issues on behalf of Internet users. EPIC has supported and continues to support the FCC's authority to promulgate rules protecting consumer privacy,[2] and has filed amicus briefs in the courts on many occasions both to safeguard communications privacy and to protect the rulemaking authority of the FCC.[3] EPIC worked closely with the Commission in 2006 to establish stronger safeguards for call record information.

[1] In the Matter of A National Broadband Plan for Our Future, GN Docket No. 09-51.

[2] *See Communications Networks and Consumer Privacy: Recent Developments: Hearing Before the Subcomm. on Communications, Technology and the Internet of the H. Comm. on Energy and Commerce*, 111th Cong. 1-2 (2009) (Statement of Marc Rotenberg, Executive Director, EPIC), *available at* http://energycommerce.house.gov/Press_111/20090423/testimony_rotenberg.pdf; accessed May 28, 2009; *see also* Brief for EPIC, Privacy and Consumer Organizations, Technical Experts, and Legal Scholars as Amicus Curiae Supporting Respondents, *Nat'l Cable & Telecomms. Ass'n v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) (No. 07-1312); *available at* http://epic.org/privacy/nctafcc/epic-ncta-050608.pdf (last accessed May 28, 2009) (supporting the FCC's 2007 Order requiring an opt-in system for disclosure of customer proprietary network information).

[3] Brief of the Electronic Privacy Information Center, *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1999) (No. 98-9518) (FCC opt-in privacy rule), *available at* http://epic.org/privacy/litigation/uswest/amicus_brief_SRPR.html; Supplemental Brief, *U.S. v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383) ("intercept" of stored communications), *available at* http://epic.org/privacy/councilman/kerr_amicus.pdf.

We brought the problem of call records sales to the attention of the FCC,[4] and we support the Commission's rulemaking establishing stronger security standards for customer information maintained by the telephone companies.[5]

I. THE COMMISSION SHOULD PURSUE A WIDE RANGE OF APPROACHES, INCLUDING EXERCISE OF ITS ANCILLARY JURISDICTION, TO ADDRESS BROADBAND PRIVACY ISSUES

The Commission seeks comments on whether "the Commission [should] consider as part of its plan whether to exercise its ancillary jurisdiction to address broadband privacy issues, or [whether] other approaches [are] available.[6]

The Commission has recognized that privacy is a critical concern in the development of the national broadband plan: "Americans are using broadband to perform everyday tasks in which they pass personal and confidential information over broadband connections, raising important consumer privacy concerns. As a result, it is important to consider the privacy implications of such use in connection with our development of a national broadband plan."[7] As Acting Chairman Copps has stated, "[a] customer's private information should never be shared by a carrier with any entity for marketing purposes without a customer opting-in to the use of his or her personal information."[8] Consumers want the assurance that when they use new broadband technology, their personal information will be protected and they will not be profiled and tracked by secretive companies, hiding in the shadows of the Internet. A central requirement of a functional and trustworthy communications network is the assurance of privacy protections for users. If the Commission fails to establish strong and effective privacy safeguards for those who transmit private data such as personal messages, confidential business information, and financial and medical records, it will reduce the utility and usage of the nation's broadband infrastructure, directly undermining the goals of widespread adoption and subsequent innovation.

Therefore, EPIC urges the Commission to "exercise its ancillary jurisdiction to address broadband privacy issues"[9] in the development of this plan. As recognized in the Notice, the "Commission has long been committed to safeguarding customer privacy and repeatedly has taken steps to ensure that private customer information is adequately protected," and it is critical to the success of this plan that the Commission act in this regard. Such steps would be consistent with the history of privacy law in the United States, which is largely marked by efforts of Congress to erect safeguards for technologies as they emerge. Privacy safeguards ensure that

---

[4] Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005).
[5] *See, e.g.*, Comments of the Electronic Privacy Information Center *et al.* on the petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network information, CC Docket No. 96-115 (filed Apr. 14, 2006).
[6] In the Matter of A National Broadband Plan for Our Future, GN Docket No. 09-51, ¶ 60.
[7] *Id*. at ¶ 52; *see also id.* at ¶¶ 58-60, 66, 105.
[8] Michael J. Copps, Acting Chairman (then Commissioner), Fed. Commc'ns Comm'n, Statement on the Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115 and WC Docket No. 04-36 (Apr. 2, 2007).
[9] *Id.* at ¶ 60.

data collection is fair, transparent, and subject to law. This approach builds consumer confidence, establishes a stable business environment, and allows for the benefits of new technology while safeguarding key consumer interests.

The protection of privacy has been an essential part of US communications policy since the days when Benjamin Franklin helped enact the country's first privacy law to protect the confidentiality of messages that traveled across the nation's first postal service.[10]

Section 605 of the original Communications Act of 1934 established a clear prohibition on the use of information obtained by wiretapping in a criminal proceeding.[11] Section 222 of the amended Act makes clear that telecommunications companies have an ongoing obligation to protect the confidentiality of customer proprietary network information.[12]

In the mid-1980s, the Internet and new communications services were growing. Individuals used desktop computers to send messages to one another by means of electronic mail. New industries were emerging and new services were being offered. But questions about privacy protection of the new communications environment arose. Congress amended the federal wiretap law and enacted the Electronic Communications Privacy Act, which extended privacy protection to electronic communications and stored messages and enhanced public adoption of new network services.[13]

Similarly, in 1984, Congress passed the Cable Communications Policy Act long before widespread adoption of cable television or two-way interactive communications.[14] That law established strong privacy safeguards, including opt-in protections for subscriber privacy, thereby encouraging adoption of the technology by consumers without the risk that every second of viewing behavior would be collected, sold, or delivered to law enforcement.[15]

In 1991, well before cellular phones were widely distributed, Congress acted to shield the devices from unwanted telemarketing. [16] Subsequent FCC regulations set a high standard for protection of cellular phones, thus allowing wide adoption of the technology while avoiding interruption and privacy invasion caused by unwanted telemarketing.[17] In 1994, those regulations were supplemented by the Telemarketing Act, which resulted in greater consumer protections for telephone privacy.[18]

In keeping with this history, the Commission should exercise its ancillary jurisdiction to ensure that the national broadband plan includes robust privacy safeguards, lest consumers' critical broadband privacy interests go unaddressed. The rollout of national broadband will

---

[10] *See* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET (2002).
[11] Ch. 652, § 605, 48 Stat. 1064 (1934) (codified as amended at 47 U.S.C. §§ 151 *et seq.* (2008)).
[12] 47 U.S.C. § 605 (2008).
[13] Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522.
[14] 47 U.S.C. § 551 (2008).
[15] *Id.*
[16] Telephone Consumer Protection Act of 1991 (TCPA), 47 U.S.C. § 227.
[17] 47 C.F.R. § 64.1200 (2009).
[18] Telemarketing Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 1601-1608 (2008).

dramatically increase the incentives for and potential value of collecting and selling personal consumer information;[19] reliance on industry self-regulation, therefore, is unlikely to be sufficient. Indeed, even now, industry self-regulation has not prevented ISPs and major Internet companies from collecting and using consumer data in extremely troubling ways.[20] Furthermore, although lawmakers have indicated plans to propose legislation protecting Internet privacy,[21] such legislation is not guaranteed to become law. Even if an Internet privacy law were passed, it may not provide adequate privacy protections.[22] Therefore, the Commission can and should lead the way by explicitly enshrining consumer privacy protections in the national broadband plan.

II. SPECIFIC COMMENTS

A. The Commission Should Not Collect Personally Identifiable Information in Furtherance of the National Broadband Plan

The Commission seeks comments on "how the Commission should balance legitimate confidentiality interests in the data it collects against goals of accountability and openness,"[23] *"whether the Commission should, as a part of its national broadband plan, seek to collect additional data from broadband providers, consumers, health care providers, schools, libraries or other governmental organizations,"*[24] *and "how the Commission can use [broadband subscribership data at the Census Tract level] to report on the status of broadband deployment, including any benefits and limitations inherent in these data."*[25]

Collection of accurate and current data regarding broadband penetration is a critical component of setting benchmarks and measuring progress. This important goal, as well as the Commission's responsibilities under the Broadband Data Improvement Act,[26] can be achieved while also maintaining meaningful privacy safeguards by excluding any personally identifiable

---

[19] *See* discussion of deep packet inspection *infra* Part II.C.

[20] Concern about these practices led Representatives Markey, Dingell, Barton, and Stearns to request information about the collection and use of consumer information from thirty-three leading Internet and broadband companies. *See* Representative 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=content&task=view&id=3425&Itemid=125. Similarly, Charter Communications only backed off its plan to partner with NebuAd to track users' online activity when confronted with opposition from privacy groups and Representatives Markey and Barton. *See* Keith Regan, *Charter Scraps User-Tracking Plan After Privacy Flap*, E-COMMERCE TIMES (May 25, 2008), http://www.ecommercetimes.com/story/63563.html?wlc=1243531488. Even if self-regulation had resulted in sufficient privacy safeguards at present, the dramatically higher incentives to collect and market personal user information that will accompany both new technologies and the expanded adoption of existing ones will make it highly unlikely that self-regulation alone will adequately protect consumers.

[21] *See, e.g.* Adrianne Kroepsch, *Tailored Web Ads? Not on My Computer*, CQ POLITICS (May 12, 2009), http://www.cqpolitics.com/wmspage.cfm?parm1=5&docID=news-000003114877 (noting that both Representative Boucher and Senator Dorgan either plan to or are considering introducing such legislation).

[22] While some Senators wish to regulate in this arena, others would prefer to rely on industry self-regulation; on either side, however, many Senators may lack the technical expertise needed to craft legislation that adequately protects consumer privacy. *See* Peter Whoriskey, *Senate Grapples With Web Privacy Issues*, WASH. POST, July 10, 2008, at D3.

[23] In the Matter of A National Broadband Plan for Our Future, GN Docket No. 09-51, ¶ 32.

[24] *Id.* at ¶ 33.

[25] *Id.* at ¶ 61.

[26] Broadband Data Improvement Act of 2008, 47 U.S.C. §§ 1301-1304 (2009) (BDIA).

information from the collected data. Data collected on the census tract level, for example, would allow the Commission to accurately assess broadband penetration and such information as data transmission speed and broadband service pricing without raising the legitimate confidentiality and privacy concerns referred to in paragraph 32 of the Notice. The Commission should ensure that any data collection is premised on legitimate need, and that those data are collected at the greatest level of generality that will still meet the requirements of the BDIA and the plan's benchmarking and reporting requirements.

B. Consumer Adoption of Broadband Depends on Robust Privacy Safeguards

The Commission seeks comments on whether "issues of privacy [are] inhibiting consumer use and adoption of broadband technology"[27] *and on "consumer expectations of privacy when using broadband services or technology and what impact [ ] privacy concerns have on broadband adoption and use."*[28]

Consumers expect that their personal information is private when using broadband services and are reluctant to adopt technologies that inadequately safeguard their privacy. Polling results demonstrate that the vast majority of consumers believe that their Internet activity is private,[29] and that consumers are strongly opposed to companies selling their personal information or using it in ways other than they intended.[30] Once consumers became aware of the uses to which their personal information may be put, they will be less likely to adopt broadband technology, thus directly undermining one of the central goals of the national broadband plan. Lack of robust privacy protections, therefore, is inimical to both the goals of the national broadband plan and consumers' expectations regarding broadband use.[31] Communications technologies like broadband should be designed for precisely what they are intended for: to enable communication between people, not to allow surveillance on private citizens and monetization of their personal information.

It is likely not a coincidence that many of the countries with the highest broadband penetration rates are among those with the most robust online privacy protections. The United

---

[27] In the Matter of A National Broadband Plan for Our Future, GN Docket No. 09-51, ¶ 52.
[28] *Id.* at ¶ 59.
[29] *E.g.*, Consumers Union, *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy* (2008), *available at* http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html ("61% are confident that what they do online is private and not shared without their permission; 57% incorrectly believe that companies must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations; 48% incorrectly believe their consent is required for companies to use the personal information they collect from online activities; 43% incorrectly believe a court order is required to monitor activities online.).
[30] *See, e.g.*, Consumers Union, *supra* note 29 ("The poll revealed that 93 percent of Americans think internet companies should always ask for permission before using personal information and 72 percent want the right to opt out when companies track their online behavior."); John B. Horrigan, *Cloud Computing Gains in Currency: Online Americans Increasingly Access Data and Applications Stored in Cyberspace*, PEW INTERNET AND AMERICAN LIFE PROJECT, Sept. 12, 2008, http://pewresearch.org/pubs/948/cloud%E2%80%90computing%E2%80%90gains%E2%80%90in%E2%80%90currency (noting that, among cloud application users, 90% "would be very concerned if the company at which their data were stored sold it to another party," 80% "would be very concerned if companies used their photos or other data in marketing campaigns," and 68% "would be very concerned if companies who provided these services analyzed their information and then displayed ads to them based on their actions").
[31] *See supra* notes 7-8 and accompanying text.

States currently ranks fifteenth among the Organization for Economic Cooperation and Development (OECD) member countries with broadband penetration at 26.7 broadband subscribers per 100 inhabitants, outpaced by countries such as Norway (ranked third, at 34.5), Korea (ranked sixth, at 32.0), and Sweden (ranked seventh, at 32.0),[32] all of which, unlike the United States, have enacted omnibus privacy legislation.[33]

Consumers' expectations of privacy will be met, and their reluctance to adopt broadband technology allayed, if the Commission incorporates the privacy standards promulgated by the OECD's Privacy Guidelines[34] into the national broadband plan. These guidelines apply to "personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties."[35] The OECD Privacy Guidelines require, among other things, that there should be limitations on the collection of information; collection should be relevant to the purpose for which it is collected; personal data should only be disclosed with the subject's consent or by authority of law; there should be a policy of openness about the information's existence, nature, collection, maintenance and use; individuals should have rights to access, amend, complete, or erase information as appropriate; and that the data controller should be held accountable for compliance with these principles.[36] The national broadband plan should include a requirement that broadband service providers participating in this plan meet these standards, but, recognizing that standards must change as technology changes, we note that these should not be taken as exhaustive and fixed, but rather as minimum standards.

C. The National Broadband Rollout Risks Enabling the Expansion of Deep Packet Inspection; the FCC Should Establish Strong Rules to Safeguard Privacy

The Commission seeks comment "on how the Commission should treat issues such as deep packet inspection and behavioral advertising in developing a national broadband plan and whether there are issues related to other types of information connected with the provision of broadband services that the Commission should consider."[37]

While the National Broadband Plan will stimulate innovation and the economy, at the same time, it will greatly expand opportunities to use DPI and other data collection technology. Traditionally, packet headers are inspected by ISPs for a variety of reasons, including optimization of packet routing, detection of network abuse, and statistical analysis. Such inspection, sometimes referred to as "shallow packet inspection," gives ISPs access to basic

---

[32] OECD Directorate for Science, Technology, and Industry, OECD Broadband Portal, Table 1d. Broadband subscribers per 100 inhabitants (Dec. 2008), *available at* http://www.oecd.org/sti/ict/broadband.

[33] CHRIS KUNER, OECD WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, REPORT ON COMPLIANCE WITH, AND ENFORCEMENT OF, PRIVACY PROTECTION ONLINE 5 (2003), *available at* http://www.olis.oecd.org/olis/2002doc.nsf/LinkTo/dsti-iccp-reg(2002)5-final.

[34] OECD, GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANS-BORDER FLOW OF PERSONAL DATA, OECD Doc. 58 final (1980).

[35] *Id.* at Art. 2.

[36] *Id.* at Arts. 7-14. *See* Marc Rotenberg, THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS 395 (EPIC 2004); *see also* EFF, *Best Practices for Online Service Providers* (2008), http://www.eff.org/wp/osp.

[37] In the Matter of A National Broadband Plan for Our Future, GN Docket No. 09-51, ¶ 59.

information about Internet traffic, but does not disclose the contents of users' email or web surfing to ISPs. In contrast, Deep Packet Inspection provides ISPs with access to the content of all unencrypted Internet traffic that ISP customers send or receive. DPI can generate detailed records of users' Internet activities.

In the early days of the Internet, DPI was effectively impossible to perform on a large scale as a result of limited computing speed and resources. Recent technological advances have made is possible for ISPs and service providers to implement DPI on a large scale. In 2008, Charter Communications' Deep Packet Inspection program is the first large-scale DPI implementation by a major US ISP. Previously, several other smaller American ISPs, including Knology, Wide Open West, and Embarq, have instituted DPI programs.[38]Widespread national broadband access will further increase ISPs' ability to intercept, scan, and store consumers' Internet activities. The new technology regime raises the specter of retrospective government access to logs detailing users' Internet activities. Such logs are often retained by ISPs pursuant to DPI programs, and are subject to government surveillance and civil subpoena. DPI is extremely controversial, and has been roundly criticized by privacy and network neutrality advocates.[39] In addition, DPI raises serious questions concerning the technique's compliance with federal law.

i. DPI by Internet Service Providers Violates the Federal Wiretap Act

DPI technology can be broken into two levels of users: the network providers and other servers.[40] Internet service providers' use of Deep Packet Inspection (DPI) for online-targeted advertising violates the Federal Wiretap Act.[41] In mid-May 2008, some Charter Communications customers received notices stating that Charter would soon begin working with NebuAd to perform DPI of their Internet traffic to profile users based on their Internet activity and to place targeted advertisement. Rep. Markey (D-MA) Rep. Barton (R-TX) played a leading role stopping them.[42]

The ECPA is applicable to activities such as those originally proposed by Charter and NebuAd. The EPCA bars, in most cases, interception of electronic communications (Title I) and unauthorized access to stored communications (Title II). Courts most often define "interception" under ECPA as "acquisitions contemporaneous with transmission."[43] Charter and NebuAd's proposed DPI activities were governed by Title I of the ECPA because a user's information would be captured as it travels between a customer's computer and the requested web site's server – "contemporaneous with transmission." NebuAd's patent application for its DPI device

[38] http://www.dslreports.com/shownews/Embarq-WOW-Bury-Snooping-In-Terms-Of-Service-93375.
[39] *See* U.S. Senate Committee on Commerce, Science, and Transportation Hearing on "Network Neutrality" (February 7, 2006) (Prepared Statement of Vinton G. Cerf, Vice President and Chief Internet Evangelist Google Inc.), *available at* commerce.senate.gov/pdf/cerf-020706.pdf.
[40] John Palfrey, *The Public and the Private at the United States Border with Cyberspace*, 78 MISS. L.J. 241, 248-49 (2008). Palfrey argues there are three types of digital surveillances in the cyberspace: networks, servers, and clients. And he mentioned using DPI technology in the network and server levels. See also EPIC website on Deep Packet Inspection *at* http://epic.org/privacy/dpi/.
[41] Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522 (2008).
[42] Statement of Rotenberg, *supra* note 2.
[43] *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002); *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994).

confirms that information would be collected contemporaneously, and not recreated from ISP server logs or backups.[44] Therefore, Charter and NebuAd's scheme violated the Federal Wiretap Act.

There are similar cases internationally. Last year in the United Kingdom, Phorm publicly announced a deal with British Telecom (BT) and other major British Internet service providers to conduct DPI of users' Internet traffic.[45] BT later admitted it had tested the technology in 2006 and 2007 without informing customers involved in the trial.[46] The technology was subsequently cleared by the UK Information Commissioner's Office (ICO), provided consumers were required to opt in to it.[47]

Earlier this year, the European Commission began a legal infringement proceeding against the UK government.[48] The EU Directive on privacy and electronic communications requires EU Member States to ensure confidentiality of the communications and related traffic data by prohibiting unlawful interception and surveillance unless the users concerned have consented.[49] The EU Data Protection Directive also specifies that user consent must be "freely given specific and informed."[50] It also requires Member States to establish appropriate sanctions in case of infringement[51] and independent authorities must be charged with supervising implementation.[52] EU Telecomms Commissioner Viviane Reding noted that the UK's response to Phorm's activities failed to comply with the EU rules regarding confidentiality and privacy, and "call[ed] on the UK authorities to change their national laws and ensure that national authorities are duly empowered and have proper sanctions at their disposal to enforce EU

---

[44] *See* Network Device for Monitoring and Modifying Network Traffic Between an End User and a Content Provider U.S. Patent Application No. 20,070,233,857 (filed Oct. 4, 2007), *available at* http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220070233857%22.PGNR.&OS=DN/20070233857&RS=DN/20070233857 ("The network device is disposed in line between the computer and the network so that all data traffics are examined. The data packets exchanged between a computer and a website being visited are altered or modified in such a way that . . . the payloads of the packets are changed to suit the need of delivering transparently the targeted commercial information.").

[45] Phorm, Inc., *BT PLC, TalkTalk and Virgin Media Inc confirm exclusive agreements with Phorm ,* Phorm, Inc. (Feb. 14, 2008), *available at* http://www.phorm.com/about/launch_agreement.php (last visited June 1, 2009).

[46] *See* Chris Williams, *BT admits misleading customers over Phorm experiments,* THE REGISTER, Mar. 17, 2008, *available at* http://www.theregister.co.uk/2008/03/17/bt_phorm_lies/ (last visited June 1, 2009).

[47] Richard Wray, *Phorm: UK faces court for failing to enforce EU privacy laws,* THE GUARDIAN, May 24, 2009, *available at* http://www.guardian.co.uk/business/2009/apr/14/phorm-privacy-data-protection-eu. (last visited June 1, 2009).

[48] Europa, *Telecoms: Commission Launches Case Against UK Over Privacy And Personal Data Protection*, Brussels, Apr.il 14, 2009, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570. (last visited June 1, 2009)

[49] Article 5(1), Directive 2002/58/EC, The European Parliament And Of The Council Of 12 July 2002 Concerning The Processing Of Personal Data And The Protection Of Privacy In The Electronic Communications Sector, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

[50] Article 2(h), Directive 95/46/EC, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[51] *Id.,* Art. 24.

[52] *Id.,* Art. 28.

legislation on the confidentiality of communication."[53]

This situation demonstrates that even opt-in schemes, such as the one permitted by the UK, may lack adequate safeguards and may leave users uncertain whether their network traffic is being monitored. It is critical that a clear legal prohibition of DPI must be maintained in order to safeguard users' privacy.[54]

ii. The Commission Should Regulate Behavioral Advertising Activities to Protect Consumer Privacy

Many companies track and compile consumers' online activities to conduct online behavioral marketing and advertising. For example, Google, Yahoo, and Microsoft use their search engines to collect user log data to analyze their behavior and provide tailor-made advertisements.[55] Online social networks, such as Facebook and MySpace, also have the power to collect user data.[56] When consumers make online purchases, their personally identifiable information (PII) might not be private. Online retailers could use cookies[57] and work with a data partner to pull off the purchase history of consumers.[58]

In 2007, the Federal Trade Commission first proposed "Online Behavioral Advertising Privacy Principles," which focused entirely on self-regulation by the Internet companies.[59] They include suggestions for making privacy policies transparent and clear to consumers, allowing consumers to control over whether their information is collected, obtaining express, affirmative consent prior to using consumer information in a manner materially different from what was originally promised, and only collecting sensitive data for the purposes of behavioral advertising with express, affirmative consent.[60]

After reviewing comments from stakeholders, the FTC revised and released "Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology" in February, 2009.[61] This report adds guidance to the principles set forth in the

---

[53] Europa, *supra* note 26.
[54] Statement of Rotenberg, *supra* note 2.
[55] Louise Story, *To Aim Ads, Web Is Keeping Closer Eye on You*, N.Y. TIMES, 10 Mar. 2008, http://www.nytimes.com/2008/03/10/technology/10privacy.html?_r=1.
[56] *See* EPIC, *Facebook Privacy*, http://epic.org/privacy/facebook/default.html (last accessed June 8, 2009).
[57] "Cookies are text files that have unique identifiers associated with them and are used to store and retrieve information that allow Web sites to recognize returning users, track on-line purchases, or maintain and serve customized Web pages. Cookies may be classified as either 'session' or 'persistent.' Session cookies expire when the user exits the browser, while persistent cookies can remain on the user's computer for a specified length of time." U.S. GEN. ACCOUNTING OFFICE, INTERNET PRIVACY: IMPLEMENTATION OF FEDERAL GUIDANCE FOR AGENCY USE OF "COOKIES" 1 (2001), *available at* www.gao.gov/cgi-bin/getrpt?GAO-01-424.
[58] The Center for Digital Democracy has been working on a project on "Digital Marketing, Privacy & the Public Interest." http://www.democraticmedia.org/current_projects/privacy. *See also* Jeff Chester Reports on Digital Media and the Public Interest, *available at* http://www.democraticmedia.org/jcblog/.
[59] FTC, *FTC Staff Proposes Online Behavioral Advertising Privacy Principles* (Dec. 20, 2007), http://www.ftc.gov/opa/2007/12/principles.shtm.
[60] *Id.*
[61] FEDERAL TRADE COMMISSION STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING: TRACKING, TARGETING, AND TECHNOLOGY (February 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf

previous report, and in addition, urges companies to provide reasonable security for data collected. The report recognizes that prospective changes require a more flexible approach and states that some form of prominent notice and opt-out choice may be sufficient. Finally, the FTC considers financial information, information about children, health information, and Social Security numbers to be sensitive information.[62]

In conclusion, the FTC basically maintains a "self-regulatory approach"[63] on the issue of online behavior advertisement. While these are good policies and provide useful guidance, relying on the Internet companies to enact and follow them is both shortsighted and unlikely to be successful, particularly given the monetary incentives to target advertising as precisely as possible.[64] The protection of this sensitive information is far too important to leave to voluntary adherence with these guidelines, particularly when these incentives will only increase with the expansion of broadband adoption. Additionally, not all consumers are sufficiently aware of their privacy options to respond to opt-in protections. For example, when Google unveiled its most recent behavioral advertising plans, it gave users the right to see and edit their Google-generated profiles and gave them a way to avoid being tracked entirely. But many people are not paying close enough attention to notice. According to polling by the Consumer Reports National Research Center, "61% [of Internet users] are confident that what they do online is private and not shared without their permission,"[65] demonstrating that self-regulation and opt-in protection has not been enough. The Commission should exercise greater oversight of practices in the online advertising company and demonstrate more willingness to distinguish between sensible business practices and those that should not be permitted.

---

[62] *Id.*

[63] FTC, BEHAVIORAL ADVERTISING, MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES, *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf

[64] Microsoft's associate general counsel noted that targeted ads can bring in as much as ten times more revenue than non-targeted ads. Grant Gross, *Opting out of Targeted Ads Too Hard, Privacy Advocates Say*, CIO, June 4, 2009, http://www.cio.com.au/article/306083/opting_targeted_ads_too_hard_privacy_advocates_say; *see also* Brian Morrissey, *Aim High: Ad Targeting Moves to the Next Level*, ADWEEK, Jan. 1, 2008, *available at* http://www.adweek.com/aw/magazine/article_display.jsp?vnu_content_id=1003695822 (noting that, while the average cost per thousand page impressions (CPM) is only $2.50, the CPM of the average tailored ad is $10).

[65] Consumers Union, *supra* note 29.

D. The National Broadband Plan Improves Access to Electronic Medical Records, But Also Increases Risks to Medical Privacy

The Commission seeks comment "generally on the interaction between broadband development and improved access to medical records and healthcare."[66]

The promotion of the national broadband plan will improve access to electronic medical records, but must be accompanied by robust privacy protections.[67] Since 1995, EPIC has identified the importance and established principles for Federal privacy protection for medical records.[68] In 2005, EPIC and Patient Privacy Rights[69] launched an online petition[70] calling for strong medical privacy safeguards to establish stronger protections in the United States for patients' medical information.[71] There is also widespread public support for medical privacy measures.[72]

EPIC has addressed the danger of re-identification of patient information. In order to comply with federal and state privacy laws, patient-identifying information in pharmacies' prescription records is encrypted and de-identified, often with software installed by the data mining companies themselves. The rest of the prescription record remains intact. Thus, a patient's entire drug history is correlated, and each provider can be identified along with their prescribing habits. This practice raises privacy concerns for both patients and health care providers.

There are several instances where supposedly de-identified information has been re-identified and associated with a particular person. In Massachusetts, for example, the Group Insurance Commission (GIC) released patient specific data of state-employee health records.[73] This data did not contain the names, addresses, or Social Security numbers of any of the state employees.[74] As a result, the state agency had believed this data to be anonymous.[75] However, Latanya Sweeney[76] was able to use this data and cross-reference it to publicly available voter-registration data to track down the health records of then-Governor William Weld.[77]

---

[66] In the Matter of A National Broadband Plan for Our Future, GN Docket No. 09-51, ¶ 82.
[67] EPIC has long advocated the importance of these protections. *See* EPIC, *Medical Record Privacy*, http://epic.org/privacy/medical/default.html (last accessed June 8, 2009).
[68] "Epic Alert: Principles for Federal Privacy Protections of Medical Records." Volume 2.13 http://epic.org/privacy/medical/EPIC_Principles.txt (Oct. 30, 1995).
[69] http://www.patientprivacyrights.org/.
[70] http://www.patientprivacyrights.org/site/PageServer?pagename=Petition_for_Prescription_Privacy.
[71] http://epic.org/press/102605.html.
[72] For a compilation of statistics showing the salience of privacy concerns regarding electronic medical records and the vast public support for privacy safeguards for medical records, see EPIC, *Medical Privacy: Public Opinion Polls*, http://epic.org/privacy/medical/polls.html (last accessed June 1, 2009).
[73] *See* Latanya Sweeney, Testimony Before the Pennsylvania House Select Committee on Information Security, *Recommendations To Identify and Combat Privacy Problems in the Commonwealth*, October 5, 2005.
[74] *Id.*
[75] *Id.*
[76] Latanya Sweeney is a member of the EPIC Advisory Board, *see* http://epic.org/epic/advisory_board.html#sweeney.
[77] *Id.*

EPIC submitted an amicus brief recommending that prescription information instead be identifiable by zip code or medical specialty and used only for non-commercial purposes.[78] Such an approach would still provide useful information to researchers, pharmaceutical companies, and other entities while affording additional privacy protections to both providers and patients.

In the same fashion, EPIC urges the Commission to require similar protections for all electronic medical records to prevent sensitive patient information from being re-identified or otherwise compromised. Given the degree of legitimate public concern with the privacy of medical records, patients may forego certain treatments and medications if they cannot be confident that their privacy will not be compromised. Therefore, the national broadband plan must attend to the serious privacy implications of increased access to electronic medical records.

Respectfully submitted,

Marc Rotenberg, Esq.
EPIC Executive Director

John Verdi, Esq.
EPIC Senior Counsel

Richard Chang
EPIC 2009 IPIOP Clerk

Lia Ernst
EPIC 2009 IPIOP Clerk

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C., 20009

[78] *See* Brief of EPIC et al. as Amicus Curiae Supporting Appellant, *IMS Health, Inc. v. Ayotte*, 550 F.3d 42 (1st Cir. 2008) (No. 07-1945).