epic.org

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

March 18, 2013

Representative Jim Sensenbrenner, Chairman
Representative Bobby Scott, Ranking Member,
Committee on the Judiciary
Subcommittee on Crime, Terrorism,
Homeland Security, and Investigations
2141 Rayburn House Office Building
Washington, DC 20003

Re: ECPA Part 1: Lawful Access to Stored Content

Dear Chairman Sensenbrenner, Ranking Member Scott, members of the Committee:

Thank you for your attention to the important issue of electronic communications privacy and your invitation to EPIC to submit a statement for the record. Few issues facing Internet users today are of greater concern than online privacy. It is for this reason that we are writing to urge the Committee to undertake a comprehensive review of the Electronic Communication Privacy Act ("ECPA"). In particular, we ask you to consider the need to update the law to protect electronic communications from interception by private parties, and to consider the growing significance of cloud computing in the provision of Internet-based services. The Electronic Communications Privacy Act provides, at best, uncertain protection for important categories of personal information. Several recent developments, discussed briefly below, demonstrate the inadequacy of the current law and underscore the need for comprehensive reform.

The Electronic Privacy Information Center ("EPIC") is a non-partisan public interest research organization established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC fully supports the Committee's examination of the Electronic Communications Privacy Act of 1986 ("ECPA").[1] EPIC has testified and submitted numerous statements and amicus briefs on issues related to ECPA, including protections for residential Wi-Fi communications,[2] private location records,[3] and messages in "electronic storage."[4]

---

[1] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. § 2510 et seq.).
[2] *See* EPIC, *Ben Joffe v. Google*, http://epic.org/amicus/google-street-view/ (last visited Mar. 18, 2013).
[3] *H.R. 2168, the "Geolocational Privacy and Surveillance Act": Hearing Before the H. Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 125 (2012) (statement of the Electronic Privacy Information Center), *available at* https://epic.org/privacy/location_privacy/EPIC-Location-Privacy-Statement-5-17-12.pdf; *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the H. Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 109 (2010) (statement of the Electronic Privacy Information Center), *available at* https://epic.org/privacy/ECPA_Statement_2010-06-24.pdf.

(1) Google's Wi-Fi Interception Underscores the Need for Reform

Last week, thirty-eight state attorneys general reached a $7 million settlement with Google over privacy violations resulting from the interception of personal information from private Wi-Fi networks.[5] And Google conceded that it acted improperly when it captured private wireless communications.

The interception occurred after Google deployed vehicles equipped with digital cameras and other devices used to capture street images and catalog the locations of residential networks. Using hidden Internet receivers Google Street View vehicles also collected an enormous amount of data from nearby home and office wireless networks. Data collected by Google's vehicles included MAC addresses (unique device identifiers for wireless devices), network SSIDs (the user-assigned ID for a wireless network), the location of identified networks, and even so-called "payload" data – which included emails, passwords, usernames, websites, and other sensitive information.[6] The Federal Communications Commission subsequently fined Google $25,000 for obstructing an investigation into the Street View program,[7] and a private class-action lawsuit is still pending before the U.S. Court of Appeals for the Ninth Circuit.[8]

EPIC has argued that ECPA protects the contents of private communications transmitted over wireless networks, but the law's application in this area is still uncertain. Google has suggested that all unencrypted communications, even those sent via private networks, are "readily available to the general public" and thus not protected under ECPA.[9] Congress should make clear that is not the case. Indeed, this is the conclusion that Senator Durbin drew at a hearing last year with the Chairman of the FCC.[10] Chairman Genachowski agreed and said that "the law should protect people even if they have unencrypted wi-fi."

As the *New York Times* editorial board explained this weekend, "Google has also said that it has privacy safeguards to ensure that the locations of individual wireless users are not disclosed without their consent. Those assurances do not go far enough. Congress needs to explicitly protect such information from prying eyes."[11] We agree with the *New York Times* that Google's Wi-Fi interception "shows the need to overhaul a 27-year-old federal law that is not up to the task of addressing new forms of privacy invasion."

---

[4] *Jennings v. Jennings*, __ S.E. 2d ___, 2012 WL 4808545 (S.C. Oct. 10, 2012), *petition for cert. filed* (U.S. Jan. 7, 2013) (No. 12-831).

[5] *See* EPIC, *States Fine Google for Street View Privacy Violations*, https://epic.org/2013/03/states-fine-google-for-street.html.

[6] *See* EPIC, *Investigations of Google Street View*, https://epic.org/privacy/streetview/; *see also WiFi Data Collection: An Update*, Google Blog (May 14, 2010), http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.

[7] Fed Commc'n Comm'n, Google, Inc., File No. EB-10-IH-4055 (2012) (Notice of Apparent Liability for Forfeiture), http://transition.fcc.gov/DA-12-592A1.pdf.

[8] *See Ben Joffe v. Google*, No. 11-17483 (9th Cir. Oct. 17, 2011).

[9] .*See* Brief of Google, Inc., *Joffe v. Google*, No. 11-17483 (9th Cir. Feb. 8, 2012).

[10] *See* EPIC, *On Google Spy-Fi, Senator Durbin Calls for Update to Wiretap Law, FCC Chair Agrees Law Should Protect Unencrypted Communications*, https://epic.org/2012/05/on-google-spy-fi-senator-durbi.html.

[11] Editorial, *Googling You,* N.Y. Times, Mar. 16, 2013, https://www.nytimes.com/2013/03/17/opinion/sunday/google-street-view.html?_r=0.

(2) Key Terms in ECPA Now Lack Coherence

The recent decision of the South Carolina Supreme Court in *Jennings v. Jennings* also underscores the need for a comprehensive overhaul of ECPA.[12] In *Jennings*, five justices were unable to agree on the scope of ECPA protections for opened e-mail messages stored in the cloud. Specifically, the court could not agree on the interpretation of "electronic storage," a key term in the Act.[13] The distinctions drawn by the judges in *Jennings* are also in conflict with an important decision in Ninth Circuit that will lead to considerable confusion in the federal courts if the Supreme Court does not grant review.[14] For this reason, EPIC, along with eighteen other privacy organizations, recently filed an amicus brief with the Supreme Court in support of certiorari.[15] It is our view the key terms in ECPA will continue to present interpretive problems until Congress takes action to update the law.

(3) Current Law Provides Inadequate Protection for Location Records

In the course of previous ECPA reform efforts, EPIC has routinely urged Congress to address the need to protect location information.[16] Current electronic privacy laws have not only failed to keep pace with changing communications technologies, they also lack key protections for a steadily expanding category of private data: subscriber location records. As the Supreme Court recently recognized in *United States v. Jones*, location data "reflects a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations."[17] Yet ECPA does not distinguish between private location records and other, less invasive, data such as call toll records.[18] The current lack of protection for location data is unjustifiable given the state of technology and the Supreme Court's decision in *Jones*.

Courts have struggled to establish clear standards for the collection and use of location data, and without Congressional guidance they will continue to struggle. While there is a growing consensus that location records implicate Fourth Amendment interests,[19] recent cases cannot set clear standards because of the good faith exception and the lack of certainty in the law

---

[12] *Jennings v. Jennings*, __ S.E. 2d ___, 2012 WL 4808545 (S.C. Oct. 10, 2012), *petition for cert. filed* (U.S. Jan. 7, 2013) (No. 12-831).

[13] *See* 18 U.S.C. § 2710(15).

[14] *See Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004).

[15] *See* Brief Amici Curiae of Nineteen Privacy, Civil Liberties, and Consumer Organizatinos in Support of Petition for Certiorari, *Jennings v. Broome*, No. 12-831 (Feb. 7, 2013).

[16] *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. (2010) (statement for the record of Electronic Privacy Information Center), *available at* http://epic.org/privacy/ECPA_Statement_2010-06-24.pdf.

[17] *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

[18] *See generally* 18 U.S.C. § 2703.

[19] *See, e.g.*, *Jones*, 132 S. Ct. 945; *State v. Zahn*, 812 N.W. 2d 490 (S.D. 2012); *In re U.S.*, 620 F.3d 304 (3d Cir. 2010); *Commonwealth v. Connolly*, 454 Mass. 808 (2009); *People v. Weaver*, 12 N.Y.3d 433 (2009); *In re U.S.*, 747 F. Supp. 2d 827 (S.D. Tex. 2010); *Commonwealth v. Wyatt*, 30 Mass. L. Rptr 270 (Mass. Sup. Ct. 2012); *State v. Holden*, 54 A.3d 1123 (Del. Super. Ct. 2010).

pre-*Jones*.[20] Even though many courts agree that Fourth Amendment protections apply to location data, they do not agree on what legal process is necessary to satisfy the standard. Courts are ill equipped to establish clear standards due to the technically and factually complex nature of the problem.[21]

Rather than wait for courts to develop privacy standards on an ad-hoc basis, Congress should undertake a comprehensive rewrite of the ECPA. By pursuing a broad legislative overhaul of current electronic privacy laws, Congress can establish important new privacy safeguards for personal information. This is especially important given the growing dependence of consumers on cloud-based services that routinely store user data on remote servers. Under the current law, investigators can collect private data from individuals without any minimization or use limitation requirements. Such broad surveillance should be limited by appropriate procedural checks and balances. Also, stronger security standards should be established, and limitations on commercial exploitation made clear.

We would welcome an opportunity to discuss these matters in more detail in testimony before the Committee.

Sincerely,

Marc Rotenberg,
EPIC Executive Director

Alan Butler,
EPIC Appellate Advocacy Counsel

David Jacobs,
EPIC Consumer Protection Counsel

Cc: Chairman Bob Goodlatte, House Judiciary Committee
Ranking Member John Conyers, House Judiciary Committee

[20] *See*, *United States v. Barajas*, ___ F.3d ____, 2013 WL 781789 (10th Cir. 2013) (noting that the mere use of a phone for criminal activity is insufficient to establish probable cause, but declining to rule on that issue because of the good faith exception).
[21] *See* Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311 (2012).