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

May 18, 2010

Julius Genachowski, Chairman
Federal Communications Commission
Room: 8-B201
445 12th Street SW
Washington, DC 20554

Dear Mr. Chairman,

We are writing to you regarding recent reports that Google intercepted and downloaded wireless access (Wi-Fi) communications as part of its "Street View" activity. We understand that Google also downloaded and recorded a unique device ID, the MAC address, for wireless access devices as well as the SSID assigned by users. As you may know, Representative Markey and Representative Barton, two senior members of the House Commerce Committee, wrote to FTC Chairman John Liebowitz to ask the FTC to undertake an investigation and to reply to certain questions by June 2, 2010.

We are writing now to bring this matter to the attention of the Federal Communications Commission and to urge you to open an investigation. EPIC has worked closely with the FCC in the past to establish privacy safeguards for users of communications services, having brought the issue of call records sales to the attention of the Commission in 2005, and having supported the subsequent rulemaking on the issue.[1] EPIC also urged the Commission to investigate the improper release of Americans' call detail information to the National Security Agency.[2] More recently, EPIC filed an amicus brief in support of the Commission in its successful case to protect the privacy of consumer call record information.[3]

---

[1] 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); 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).
[2] Letter from Electronic Privacy Information Center to FCC Chairman Kevin Martin, May 17, 2006, *available at* http://www.epic.org/privacy/wiretap/epic-fcc-nsa.pdf.
[3] Brief for *amici* Electronic Privacy Information Center et al., Nat'l Cable & Telecomm. Assoc. v. FCC, 567 F. 3d 659 (2009), *available at* http://epic.org/privacy/nctafcc/epic-ncta-050608.pdf.

We believe that the Commission should now turn its attention to the significant communications privacy issues arising from Google Street View.

Google launched the Street View service in May 2007, with "360 degree street level imagery" of five American cities.[4] The service raised significant privacy concerns but those concerns focused exclusively on the images that the company was capturing and putting online by means of digital cameras affixed to its vehicles. Some people objected to the fact that the cameras went through residential neighborhoods and captured images through homes windows. Others were surprised to learn that their own images were posted on the Internet by Google.

Google defended the program from privacy objections by stating that they "have been careful to only collect images that anyone could see walking down a public street" and that they would "be sure to respect local laws."[5] Almost a year after launch, after adding a number of locations, Google began blurring the faces of those who appeared in the pictures, citing privacy concerns but again making no mention of Wi-Fi scanning.[6] Google also faced a federal court case that rose to the Third Circuit Court of Appeals, which ruled that the company could face liability for trespassing on private property.[7] As the program has expanded to cover most of the United States as well as over 30 countries abroad,[8] the company has begun capturing data not only with cars, but also with a large tricycle and a snowmobile.[9]

But the reality of Street View was very different. Google has now admitted that Google Street View vehicles have been capturing communications data for years. Google never disclosed this activity. The fact of Google's Wi-Fi spying was obtained by Peter Schaar, the German Commissioner for Data Protection and Freedom of Information, who discovered that the vehicles were scanning networks to compile a database of networks and their physical locations for use in "location-

---

[4] Google, *Google Announces New Mapping Innovations at Where 2.0 Conference*, May 29, 2007, http://www.google.com/press/annc/maps_where20.html.
[5] Peter Fleischer, *Street View and Privacy*, Sep. 24, 2007, http://google-latlong.blogspot.com/2007/09/street-view-and-privacy.html.
[6] Andrea Frome, *Street View Visits Manhattan*, May 12, 2008, http://google-latlong.blogspot.com/2008/05/street-view-revisits-manhattan.html.
[7] Boring v. Google, No. 09-2350, 2010 U.S. App. LEXIS 1891 (3rd Cir. Jan. 25, 2010).
[8] Google, *Where is Street View?*, http://maps.google.com/help/maps/streetview/where-is-street-view.html (last visited May 21, 2010).
[9] Google, *Street View: We Can Trike Wherever You Like*, Oct. 16, 2009, http://googleblog.blogspot.com/2009/10/street-view-we-can-trike-wherever-you.html; Google, *Street View Hits the Slopes at Whistler*, Feb. 9, 2010, http://google-latlong.blogspot.com/2010/02/street-view-hits-slopes-at-whistler.html.

aware" advertising services. Schaar demanded a full audit of the data Google was collecting and the immediate removal of the scanners from the cars.[10]

As part of the audit, it was revealed that not only was Google mapping the physical locations of the networks, but that the vehicles were capturing payload data, meaning all data flowing on those networks. Whatever Internet traffic that was taking place on a given network as the Street View vehicle drove past was captured and stored by Google.[11]

None of Google's Wi-Fi activity was made known to the public or presumably to the Commission until the recent investigation undertaken by European privacy officials. In fact, Google still makes no mention of the Wi-Fi data collection activity on the web page specifically devoted to privacy concerns related to Street View.[12]

This is extraordinary. The capture of Wi-Fi data in this manner by Google Street View could easily constitute a violation of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also known as the Wiretap Act, as amended by the Electronic Communications Privacy Act (ECPA) of 1986 to include electronic communications.[13] Courts most often define "interception" under ECPA as "acquisitions contemporaneous with transmission."[14] The Wiretap Act provides for civil liability and criminal penalties against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any . . . electronic communication [except as provided in the statute]."[15] The Wiretap Act imposes identical liability on any person who "intentionally discloses . . . to any other person the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the interception of a[n] ... electronic communication in violation of this subsection," or "intentionally uses . . . the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the interception of a[n] . . . electronic communication in violation of this subsection."[16] The Wiretap Act also states, "a person or entity providing an

---

[10] *Google-Street-View Tours also Used for Scanning WLAN-Networks*, Apr. 23, 2010, http://www.bfdi.bund.de/cln_134/sid_74A4D9FE1F85492D36F74BB3443C41EA/EN/PublicRelations/PressReleases/2010/GoogleWLANScan.html.

[11] Google, *WiFi Data Collection: An Update*, May 14, 2010, http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.

[12] Google, *Privacy | Google Maps with Street View*, http://maps.google.com/help/maps/streetview/privacy.html (last visited May 18, 2010)

[13] Codified at 18 U.S.C. §§ 2510–2522.

[14] *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).

[15] 18 U.S.C. § 2511(1)(a).

[16] 18 U.S.C. § 2511(1)(c)-(d).

electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."[17]

The Wiretap Act provides for six exceptions from Section 2511(1)-(3) liability. The first five exceptions are clearly inapplicable, including such behavior as execution of FISA warrants and FCC enforcement actions.[18] The sixth exception provides allowances for "electronic communication[s] made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[19] In interpreting this provision, courts have only found communications systems to be so configured when access is common and easy, such as visiting a web site[20] or accessing a shared iTunes library.[21] In the closest analogue to Google's behavior, one court ruled that using a police scanner to intercept unscrambled cordless telephone calls violated the statute.[22] By intercepting and recording unencrypted Wi-Fi transmissions, it is very likely that Google violated the federal Wiretap Act.

The Commission is charged with protecting the interest of US consumers of communications services in the United States and with safeguarding the security and integrity of network services. Section 222 of the Communications Act, for example, sets out clear obligations for providers of communications services to safeguard the privacy of customer information. Section 705 of the Communications Act adds to the Federal Wiretap Act additional restrictions on the intercept of communication "by wire or radio" without authorization.[23] Specifically, the Act states,

> No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any

---

[17] 18 U.S.C. § 2511(3)(a).
[18] 18 U.S.C. 2511(2)(a).
[19] *Id.*
[20] DirecTV v. Barczewski, Nos. 06-2219 & 06-2221, 2010 U.S. App. LEXIS 9754 (7th Cir. Feb. 21, 2007).
[21] United States v. Ahrndt, No. 08-468-KI, 2010 U.S. Dist. LEXIS 7821 (D. Or. Jan. 28, 2010).
[22] Tapley v. Collins, 41 F. Supp. 2d 1366, 1373 (S.D. Geor. 1999).
[23] 47 U.S.C. § 605(a).

information therein contained) for his own benefit or for the benefit of another not entitled thereto.[24]

Violations of Section 705 carry strict penalties, with willful violations "for purposes of direct or indirect commercial advantage or private financial gain" meriting fines of up to $50,000 and prison for up to two years for a first offense.[25]

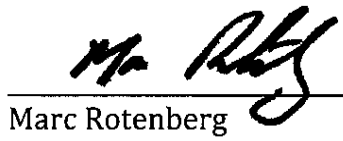
Google CEO Eric Schmidt was recently quoted as saying, "no harm, no foul."[26] Of course, it is not necessary to show "harm" to prove an unlawful intercept. It is the intercept itself that is the violation. This is particularly important when the representation about harm is made by the party that engaged in the illegal activity.

To be sure, many people take advantage of open wireless access points to go online. Absent any criminal intent or conduct, we are not suggesting that that activity is unlawful. But Google's conduct with Street View was very different. The company routinely and secretly downloaded user communications data and the company routinely and secretly mapped private communications hotspots. Moreover, they said not a word about the Wi-Fi data collection during the three-year privacy debate over Street View.

This is why the FCC must undertake an investigation. The FCC has broad authority to execute and enforce the provisions of the Communications Act[27] and the Commission plays a critical role in safeguarding the privacy of American users of communications services.

We look forward to hearing from you as soon as possible regarding the action the FCC intends to take.

Sincerely,



Marc Rotenberg
Executive Director
Electronic Privacy Information Center (EPIC)

---

[24] *Id.*
[25] 47 U.S.C. § 605(e)(2)
[26] Jonathan Fildes, *Google Chief Eric Schmidt Downplays Wi-Fi Privacy Row*, BBC News, May 18, 2010, http://news.bbc.co.uk/2/hi/technology/10122339.stm.
[27] 47 U.S.C. §151.