Statement for the Record of
the Electronic Privacy Information Center (EPIC)

Marc Rotenberg, Executive Director
Jared Kaprove, Domestic Surveillance Counsel
Ginger McCall, Staff Counsel

Hearing on

"ECPA Reform and the Revolution in Location Based Technologies and Services"

Before the

Committee on the Judiciary
Subcommittee on the Constitution, Civil Rights, and Civil Liberties
United States House of Representatives

June 24, 2010
2237 Rayburn House Office Building
Washington, DC

Mr. Chairman, Members of the Committee, this statement was prepared for the hearing "ECPA Reform and the Revolution in Location Based Technologies and Services" to be held on June 24, 2010 before the House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties. We ask that it be included in the hearing record.

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] and locational information. Mobile devices have become ubiquitous in modern society, and they have become increasingly capable of recording and transmitting users' locations. In light of this, it is important that clear standards are formulated in order to protect the privacy of users by giving the users control over their own data and requiring an opt-in model for the use of this data. This statement outlines several steps that the Subcommittee on the Constitution, Civil Rights, and Civil Liberties can take to strengthen the privacy protection of US customers whose data is collected and used by companies around the world.

I. EPIC has a Longstanding Interest in the Privacy of Locational Data

In 1999, Congress amended the Communications Act of 1934 with the Wireless Communication and Public Safety Act of 1999. The Act required wireless carriers to implement 911 emergency calling and added location privacy provisions to the Telecommunications Act.[2] Section 222 protects location information along with other customer proprietary network information (CPNI), requiring user "approval" for uses or disclosures.[3] CPNI includes "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier."[4]

Express prior authorization of the customer is required for uses and disclosures of "call location" information, with certain exceptions. These exceptions are to providers of emergency services, to family and guardians in emergency situations, and to information or database services solely for assisting in delivering emergency services.[5] Location technologies not based on CPNI, or not run by an entity subject to the § 222 protections, are not covered by these regulations. After the Act was passed, the Federal Communications Commission (FCC) considered a rulemaking to develop guidelines governing the collection and use of location data generated by wireless communications systems.

During this time, in April of 2001, EPIC filed comments encouraging the FCC to follow through on the rulemaking process because "location privacy is one of the most significant issues facing American consumers and the expeditious establishment of comprehensive,

[1] Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. § 2510 et seq.).
[2] Pub. L. No. 106-81, 113 Stat. 1286 (1999).
[3] 47 U.S.C. § 222(c)(1).
[4] 47 U.S.C. § 222(h)(1)(A).
[5] 47 U.S.C. § 222(d)(4).

technologically neutral privacy protections would serve the public interest. "[6] EPIC recognized that locational tracking technologies "enable the creation of detailed daily itineraries for millions of consumers, [and] have the potential to fundamentally alter the nature and use of wireless communications systems. "[7] EPIC encouraged the FCC to enact rules that would give consumers "meaningful control over the collection and use of location data."

In later reply comments, EPIC stated that "rulemaking is needed . . . because some commenters recognize limits on implied consent, while others do not."[8] Because of this, EPIC encouraged the FCC to "carefully constrict the circumstances under which implied consent could be utilized, if at all"[9] and to clarify the meaning of several key terms—including "location information"—that are used in the Act. EPIC recommended a number of other rules, including a rule that would require consent to be specific as to the third party that can receive the information and the purpose for which that information will be used by that party, and a rule that would require carriers to keep a record of consent for as long as the permission is valid. With all of these steps, EPIC sought to give users greater control over their locational information by requiring opt-in consent for locational tracking.

The FCC ultimately declined to embark on rulemaking regarding the Wireless Communications and Public Safety Act. The Commission said that a federal statute enacted in 1999 "imposes clear legal obligations and protections for consumers,"[10] and that "the better course is to vigorously enforce the law as written, without further clarification of the statutory provisions by rule."[11] Commissioner Michael Copps dissented, citing EPIC's comments and arguing, "Commission action is needed because the statute's meaning apparently is subject to varying interpretations within the industry."[12]

II. Locational Privacy Concerns are Substantial and Growing More Severe

The FCC's failure to address locational privacy issues should be remedied as soon as possible. The problem grows more severe as the number of mobile device users increases and location-based advertising technology becomes more advanced. The number of American cell phone users increases every year. The Pew Research Center found that 77% of all adults had a cell phone or other mobile device in 2008.[13] By April 2009, this number had risen to 85%.[14]

Cell phone usage is also increasingly commonplace among younger demographic groups. A Pew Research Center study on Social Media and Mobile Internet Use Among Teens and

---

[6] EPIC, Comments to the F.C.C. on Commission Public Notice, DA 01-696 (Apr. 6, 2001), *available at* http://www.epic.org/privacy/wireless/epic_comments.pdf.
[7] *Id.*
[8] EPIC, Reply Comments to the F.C.C. on Commission Public Notice, DA 01-696 (Apr. 24, 2001), *available at* http://www.epic.org/privacy/wireless/epic_reply.pdf.
[9] *Id.*
[10] F.C.C., Order Declining to Commence Rulemaking to Establish Fair Location Information Practices (July 24, 2002), *available at* http://epic.org/privacy/wireless/FCC_order.pdf.
[11] *Id.*
[12] *Id.*
[13] Pew Research Center, Teens and Internet Over the Past Five Years: Pew Internet Looks Back (Aug. 19, 2009), *available at* http://www.pewinternet.org/Reports/2009/14--Teens-and-Mobile-Phones-Data-Memo.aspx.
[14] *Id.*

Young Adults reported that three-quarters (75%) of teens and 93% of young adults ages 18-29 now have a cell phone. The level of usage in this age group has jumped rapidly from 2004 (45% of teens had a cell phone), to 2006 (63% of teens had a cell phone), and then to 2008 (71% of teens had a cell phone).[15] The Pew Research Center found that "in the past five years, cell phone ownership has become mainstream among even the youngest teens. Fully 58% of 12-year-olds now own a cell phone, up from just 18% of such teens as recently as 2004. "[16]

Mobile devices have also become an increasingly popular way to access the internet. A 2009 Pew Research Center study reported that 55% of American adults connect to the internet wirelessly, either through a WiFi or WiMax connection via their laptops or through their handheld device like a smart phone.[17] Roughly half of 18-29 year-olds have accessed the internet wirelessly on a cell phone (55%).

Advertisers and technology companies are taking advantage of these trends and the lack of federal regulation by developing technology that uses mobile device GPS tracking capabilities in order to gather users' information and serve targeted advertisements. On February 19, 2010, it was reported that Point Inside, a company that makes shopping center mapping and navigation apps for smartphones, had announced the launch of its new indoor mobile advertising platform that provides the indoor location and location-specific advertising for mall-based retailers and brands.[18] Advertisements are served on smartphones based on user location and interest in a particular store or brand.[19]

In late 2009, Google announced the launch of a Google smartphone, called the Nexus One. There was wide speculation that Google, the internet's largest advertising company, would use these mobile devices as another opportunity to place advertisements.[20] Some speculated that the company would offer users the choice to subsidize the phone cost by accepting advertisements—a strategy that has been employed by a company in Germany.[21]

Apple, the creator of a number of mobile devices, including the iPhone and iPad, recently made an announcement that applications which utilize location-based advertising would be spurned from its applications store. This announcement, paired with the company's recent

---

[15] *Id.*
[16] Pew Research Center, Social Media and Mobile Internet Use Among Teens and Young Adults (Feb. 3, 2010), *available at* http://pewresearch.org/pubs/1484/social-media-mobile-internet-use-teens-millennials-fewer-blog.
[17] Pew Research Center, Internet, Broadband, and Cell Phone Statistics (Jan. 5, 2010), *available at* http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx.
[18] Mobile Marketing Watch Blog, *Point Inside Launches Indoor Mobile Advertising Solution Via SmartMap Android/iPhone Apps*, Feb. 19, 2010, http://www.mobilemarketingwatch.com/point-inside-launches-indoor-mobile-advertising-solution-via-smartmap-androidiphone-apps-5414/.
[19] *Id.*
[20] Matt Hamblen, *Google's Nexus One Smartphone: Will Mobile Ads Offset Cost?*, Computer World, Dec. 14, 2009, http://www.computerworld.com/s/article/print/9142245.
[21] Matt Hamblen, *Alcatel Lucent to Serve Mobile Ads to Wireless Customers in Germany Who Opt-in*, Computer World, June 29, 2009, http://www.computerworld.com/s/article/9134904.

acquisition of advertising firm, Quattro Wireless, has caused increasing speculation that Apple, itself, plans to have exclusive control over location-based advertisements on its products.[22]

Indeed, with the release of its newest operating system for the iPhone and iPad devices, iPhone OS 4.0, alongside a new advertising platform called iAd, Apple has altered[23] its Terms of Service for users of those devices to include a provision that "Apple and [its] partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device."[24]

Another recent grab for locational data has come from Google's Street View product. When Google began the Street View project in 2007, many privacy concerns were raised, but the debates focused almost exclusively on the collection and display of images obtained by the Google Street View digital cameras. It has been revealed Google was also obtaining a vast amount of Wi-Fi data from Wi-Fi receivers that were concealed in the Street View vehicles. Following independent investigations, Google now concedes that it gathered MAC addresses (the unique device ID for Wi-Fi hotposts) and network SSIDs (the user-assigned network ID name) tied to location information for private wireless networks.[25] Google also admits that it has intercepted and stored Wi-Fi transmission data, which includes email passwords and email content.[26]

As of June 18, 2010, investigations of Google's Street View Wi-Fi data collection have been initiated in eighteen countries and several U.S. states, as well as by the FTC and the FCC.[27] EPIC has written to the FCC suggesting that the actions may have violated, among other things, the Wiretap Act as amended by ECPA.[28] Congressmen Edward Markey and Joe Barton wrote a letter to the FTC asking for such an investigation, also asking whether that agency believed Google had violated federal law.[29]

These examples show the ubiquitous nature of access to location-based data and the necessity of clarity in the laws regulating this form of technology.

---

[22] Chris Foresman, *Apple Tells Devs that Location-Based Advertising is a No-no*, Ars Technica, Feb. 5, 2010, http://arstechnica.com/apple/news/2010/02/apple-tells-devs-that-location-based-advertising-is-a-no-no.ars ; Kevin Anderson, *Apple Hints at Location-based Advertising and Services Strategy*, The Guardian Technology Blog, Feb. 5, 2010, http://www.guardian.co.uk/technology/blog/2010/feb/05/apple-iphone-advertising-location.

[23] David Sarno, *Apple Collecting*, *Sharing iPhone Users' Precise Locations*, L.A. Times, June 21, 2010, http://latimesblogs.latimes.com/technology/2010/06/apple-location-privacy-iphone-ipad.html.

[24] Apple, *Privacy Policy*, http://www.apple.com/legal/privacy/ (last visited June 22, 2010).

[25] Google, *Data Collected by Google Cars*, European Public Policy Blog, Apr. 27, 2010, http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html.

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

[27] For a full discussion of the status of these ongoing investigations, see EPIC, *Investigations of Google Street View*, http://epic.org/privacy/streetview/.

[28] Letter from EPIC to FCC Chairman Julius Genachowski, May 18, 2010, *available at* http://epic.org/privacy/cloudcomputing/google/EPIC_StreetView_FCC_Letter_05_21_10.pdf.

[29] Letter from Edward Markey & Joe Barton to FTC Chairman Jon Leibowitz, May 19, 2010, *available at* http://epic.org/privacy/ftc/google/5_19_10_Markey_Barton_FTC_re_Google_WiFi.pdf.

III. The European Commission has Provided an Effective Model for Regulating Locational Data

Concerns regarding locational privacy are arising in other countries, as well. The responses in Europe, in particular, provide the United States with a possible model to protect the privacy of locational data. With Directive 2002/58 on Privacy and Electronic Communications, also known as E-Privacy Directive, the European Commission has created effective regulation of locational data. The Directive addresses cellular location information.[30]

The Directive differentiates between location information needed to enable transmission and location information used for value-added services.[31] Location data other than traffic data is treated under Article 9, which requires that location data be processed anonymously or with consent of the individual.

Obtaining this consent requires informing the user of the type of data, the purpose of the collection, the duration of the collection and whether a third party will be doing the processing. Consent may be withdrawn at any time, and there must be a simple and free means for a user to refuse the processing of location data for a specific connection or transmission. The processing of data is restricted to what is necessary for providing the value-added service.[32] Further, Article 26 of the Universal Service Directive requires that Member states ensure that providers of public telephone networks make call location information available to emergency authorities.[33]

The Article 29 working party, an E.U. advisory group of experts on privacy and data protection, has issued an opinion further clarifying the rule regarding location information.[34] Consent means specific consent, not obtained as part of an agreement to more general terms.[35] Location data may not be stored beyond the delivery of the location-based service, unless kept for billing purposes, or anonymized.[36] In locating employees, the working group considers the collection excessive in situations where employees would be free to make their own travel arrangements or where the location monitoring is done for the sole purpose of monitoring employees and other means are available.[37] Location information should not be collected outside of working hours, and the working group recommends that location equipment which is also used for private purposes permit employees to turn off the location tracking.

---

[30] Directive 2002/58/EC of 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 (Directive on privacy and electronic communications), *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.
[31] *Id.* at 35.
[32] *Id.* at Art. 9.
[33] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and user's rights to electronic communications networks and services (Universal Service Directive), *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_108/l_10820020424en00510077.pdf.
[34] Working Party 29 Opinion on the use of location data with a view to providing value-added services, 2130/05/EN, November 2005, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf.
[35] *Id.* at 5.
[36] *Id.* at 7.
[37] *Id.* at 11.

The Transatlantic Consumer Dialogue (TACD) has also passed a resolution on mobile commerce that addresses privacy concerns of consumers.[38] The resolution states that the E.U. and U.S. governments should: "Protect consumer privacy in mobile commerce and prohibit use of any personal data (including purchase and location information) for purposes that consumers have not explicitly agreed to or that unfairly disadvantage them." Industry group CTIA has released a "Best Practices and Guidelines for Location-based Services."[39] The guidelines "rely on two fundamental principles: user notice and consent."[40] Notice can be achieved by a disclosure in a privacy policy and consent may be implicit.[41] However, in situations such as child safety or business settings, the decision on the use of location-based services will be made by the account holder, rather than data subject.[42]

IV. EPIC's Recommendations

We specifically recommend that the Subcommittee consider the following objectives in the development of new safeguards to protect location data:

- Require that location not be collected or shared without affirmative user consent;
- Require that consent be fully informed consent: that users be informed of the type of data and the purpose of the collection;
- Require that consent be specific intent: consent which is not obtained as part of an agreement to more general terms;
- Require that companies provide users with a simple and free means to refuse the processing of location data for a specific connection or transmission;
- Require that location data not be stored beyond the delivery of the location-based service, unless kept for billing purposes, or anonymized.

V. Conclusion

EPIC respectfully requests that the Subcommittee takes the steps outlined in this statement, including investigating the ways in which companies gather locational data from their users; clarifying the Electronic Communications Privacy Act's treatment of how companies may gather and store users' data; adopting guidelines similar to those in the European Commission's Directive 2002/58, which would give users control over their locational data; adopting guidelines that mirror those in the TACD resolution, which require companies to obtain explicit consent from users in order to use location data; and ensuring the locational data privacy of U.S. consumers.

Thank you for your consideration of these views.

---

[38] Transatlantic Consumer Dialogue, Resolution on Mobile Commerce, August 2005, http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=283.
[39] CTIA - The Wireless Association, Best Practices and Guidelens for Location-based Services, April 2, 2008, http://www.ctia.org/business_resources/wic/index.cfm/AID/11300.
[40] *Id.*
[41] *Id.*
[42] *Id*.