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

Marc Rotenberg, EPIC President
Ginger McCall, EPIC Open Government Project Director
David Jacobs, EPIC Consumer Protection Fellow
Alan Butler, EPIC Appellate Advocacy Fellow

Hearing on H.R. 2168, the "Geolocational Privacy and Surveillance Act"

Before the
Subcommittee on Crime, Terrorism, and Homeland Security
of the
House Committee on the Judiciary

May 17, 2012
2141 Rayburn House Office Building,
Washington, DC 20515

Thank you, Mr. Chairman, for the invitation to submit this statement for the record for this hearing on H.R. 2168, the "Geolocational Privacy and Surveillance Act" ("GPS Act") to be held on May 17, 2012 before the House Subcommittee on Crime, Terrorism, and Homeland Security. We ask that this statement be included in the hearing record.

EPIC thanks you, Representatives Chaffetz and Goodlatte, and the members of the Subcommittee, for your attention to this important issue. As communications technologies evolve, new forms of personal information are generated that require new legal safeguards. Your decision to hold this hearing will help protect important privacy rights.

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 location information. Mobile devices have become ubiquitous in modern society, and service providers now routinely record and transmit users' locations. In many instances, this can provide significant benefits to users of new communications services. But in some circumstances, this also poses real risks to privacy and security.

In light of these developments, it is important to establish clear standards to protect the privacy of users by ensuring that locational data is not misused. In this statement, we outline several steps that the Subcommittee 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 Location Data

In 1999, Congress amended the Communications Act of 1934 with the Wireless Communication and Public Safety Act of 1999.[2] The Act required wireless carriers to implement 911 emergency calling and added location privacy provisions to the Telecommunications Act. 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.

EPIC filed comments in April 2001 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, technologically neutral privacy protections would serve the public interest."[3] EPIC encouraged the FCC to enact rules that would give consumers "meaningful control over the collection and use of location

[1] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. § 2510 et seq.).
[2] Pub. L. No. 106-81, 113 Stat. 1286 (1999).
[3] 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. *See also*, Marc Rotenberg, *Communication Privacy: Implications for Network Design*, 36 Comm. ACM 61 (Aug, 1993).

data."[4] In later reply comments, EPIC encouraged the FCC to "carefully constrict the circumstances under which implied consent could be utilized, if at all" [5] 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.[6] With all of these steps, EPIC sought to give users greater control over their location information by requiring opt-in consent for location tracking.

EPIC has previously submitted statements before the House Committee on the Judiciary on the importance of providing safeguards for location privacy. In a June 2010 statement, EPIC offered several steps that could be taken to strengthen the privacy protection of US customers.[7] EPIC recommended that users be fully informed of type of location data being collected and the purpose of the collection. [8] EPIC also recommended that location data not be collected or shared without affirmative consent, and that companies provide users with a simple and free means to refuse the processing of location data for a specific connection or transmission.[9]

More recently, EPIC submitted amicus briefs in several federal court cases involving location privacy. In *United States v. Jones,* the Supreme Court considered whether the government's warrantless installation and use of a GPS device to track a private vehicle implicated the Fourth Amendment.[10] EPIC filed an amicus brief in *Jones,* arguing that the warrantless use of GPS tracking devices could enable pervasive, suspicionless surveillance of Americans with no judicial supervision.[11] Ultimately, the Supreme Court unanimously ruled that the warrantless use of a GPS tracking device by the police violated the Fourth Amendment. The Court said that a search occurs where "the Government physically occupie[s] private property," like a car, "for the purpose of obtaining information."[12] Concurring opinions by Justices

---

[4] *Id.*
[5] 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.
[6] *Id.*
[7] *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.
[8] *Id.* at 7.
[9] *Id*.
[10] *United States v. Jones*, 132 S. Ct. 945 (2012).
[11] Brief of Amici Curiae Electronic Privacy Information Center (EPIC) and Legal Scholars in Support of Respondent, *United States v. Jones*, 132 S. Ct. 945 (2012) (No. 10-1259), *available at* https://epic.org/amicus/jones/EPIC_Jones_amicus_final.pdf.
[12] *Jones*, 132 S. Ct. at 949.

Sotomayor and Alito argued that the use of a GPS tracking device would also violate an individual's reasonable expectation of privacy under a traditional *Katz* analysis.[13]

Following *Jones*, EPIC submitted two amicus briefs in cases involving warrantless access to cell phone location records. In *State v. Earls*,[14] EPIC argued that the New Jersey Supreme Court should overturn a lower court decision holding that an individual has no legitimate expectation of privacy in the location of their cell phone.[15] The cell phone tracking techniques in the case, EPIC argued, "[are] more invasive than the GPS tracking in Jones."[16] Similarly, EPIC filed a brief in the Fifth Circuit urging the court to uphold a lower court ruling that the disclosure of historical cell phone location records without a warrant would violate the Fourth Amendment.[17] EPIC argued that this opinion should be upheld, in light of the Supreme Court's recent decision in *Jones*, because cell phone location records are collected without the knowledge or consent of users. [18] The records in the case, EPIC argued, provide a "comprehensive map of an individual's movements, activities, and relationships, . . . precisely the type of information that individuals reasonably and justifiably believe will remain private."[19]

These activities, which EPIC has pursued for more than a decade, indicate the growing importance of locational data for personal privacy.

II. Location Privacy Concerns Are Substantial and Growing More Acute

Location privacy issues are becoming more substantial as the number of mobile devices increases and location methods become more precise. The number of mobile phone users in the United States increases every year. The Pew Research Center found that 77% of all adults had a cell phone or other mobile device in 2008.[20] By 2012, that figure had risen to 88%.[21]

---

[13] *Jones*, 132 S. Ct. at 954-58 (Sotomayor, J., concurring); *Jones*, 132 S. Ct. at 958-64 (Alito, J., concurring in the judgment).
[14] 22 A.3d 114 (Sup. Ct. N.J. 2011), *cert. granted*, 209 N.J. 97 (2011).
[15] Elec. Privacy Info. Ctr., *State v. Earls* https://epic.org/amicus/location/earls/ (last visited May 16, 2012).
[16] Brief of Amicus Curiae Electronic Privacy Information Center, *State v. Earls*, 209 N.J. 97 (2011) (No. 68,765), *available at* https://epic.org/amicus/location/earls/EPIC-Earls-Amicus-NJ-SCt.pdf.
[17] Elec. Privacy Info. Ctr., *In re Historic Cell-Site Location Information* (last visited May 16, 2012) https://epic.org/amicus/location/cell-phone-tracking/.
[18] Brief of Amicus Curiae Electronic Privacy Information Center, *In re United States for Historical Cell Site Data*, 747 F. Supp. 2d 827 (S.D.Tx. 2010), *appeal docketed*, No. 11-20884 (5th Cir. Feb. 22, 2012), *available at* https://epic.org/amicus/location/cell-phone-tracking/EPIC-5th-Cir-Amicus.pdf.
[19] *Id.*
[20] 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.
[21] Aaron Smith, *46% of American Adults are Smartphone Owners*, Pew Research Center at 2 (Mar. 1, 2012), *available at* http://www.pewinternet.org/~/media//Files/Reports/2012/Smartphone%20ownership%202012.pdf.

American consumers carry their mobile devices everywhere, all day, every day. The location records created by these devices reveal aspects of consumers' social, political, professional, and educational lives. Every time an individual uses their mobile phone, a record is created.[22] The average individual sends or receives calls, text messages, or Internet data more than fifty times per day, generating a constant stream of location data. [23] For certain populations, mobile phone are even more ubiquitous. Young adults, for example, send an average 100 text messages per day.[24] All of these uses generate location data. The location records created provide a comprehensive map of people's movements, activities, and relationships over the course of many weeks and months—precisely the type of information that individuals reasonably and justifiably believe will remain private.

As technology improves, this location data will become more precise. Already, cell-site location data can be used to pinpoint an individual's location to the level of a room or floor in a building. Femtocells—low-power base stations used to route calls between consumers and the cellular network— have a range as small as ten meters.[25] Experts estimate that by 2016, femtocells will constitute 88% of all cell sites globally.[26] Some carriers even triangulate user location for emergency and other purposes.[27] Thus, as the technology develops further, cell phone companies will compile increasingly detailed location records of their users.

Mobile smart phones also contain built-in GPS functionality for location-based services. These devices enable consumers' location information to be collected not just by the carrier or platform developer, but by application developers and third-party advertisers. An examination of 101 popular iPhone and Android applications by the Wall Street Journal revealed that 56 applications either collected or transmitted location information to third parties.[28]

Other companies are also increasingly collecting the location information of consumers. Foursquare, with approximately 3 million users, is a service that lets users "check in" to a place, broadcast this fact to other individuals, and track the history of where they've been and with

---

[22] See Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 26 Berkeley Tech. L.J. (forthcoming 2012).

[23] Aaron Smith, *31% of Text Message Users Prefer Texting to Voice Calls, and Young Adults Stand Out In Their Use of Text Messaging*, Pew Research Center at 2 (Sept. 19, 2011), *available at* http://www.pewinternet.org/~/media//Files/Reports/2011/Americans%20and%20Text%20Messaging.pdf.

[24] *Id.*

[25] AT&T 3G Microcell—Wireless Signal Booster, AT&T, http://www.att.com/shop/wireless/devices/3gmicrocell.jsp (last visited May 16, 2012).

[26] Press Release, Informa Telecoms & Media, The Shape of Mobile Networks Starts to Change as Femtocells Outnumber Macrocells in US (Oct. 21, 2010), www.smallcellforum.org/pressreleases.php?id=269.

[27] Paul A Zandbergen, Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning, 13 Transactions GIS 5, 11 (2009).

[28] *What They Know-Mobile*, Wall St. J., http://blogs.wsj.com/wtk-mobile/ (last visited May 16, 2012).

whom.[29] Businesses are taking advantage of the service by offering discounts and coupons to individuals who "check in" to their location. Foursquare also has an API that allows developers to build on its platform. One recent smartphone application that provoked a particularly strong reaction, Girls Around Me, used information from Foursquare and Facebook to provide a map of women around a user's location.[30] As part of another program, Google collected MAC addresses (the unique device ID for Wi-Fi hotspots) and network SSIDs (the user-assigned network ID name) tied to location information for private wireless networks.[31] The "street view" vehicles also intercepted Wi-Fi "payload" data, which included emails, passwords, usernames and website URLs.[32] Advertisers and marketers also use location information in consumer data profiles, enabling them to track consumers through their daily journey and target them with advertisements based on their location.[33]

Perhaps because of the amount of information that can be derived from location data, this data is often considered sensitive or personally identifiable. For example, the Federal Trade Commission's amendments to the Children's Online Privacy Protection Act ("COPPA") Rule update the definition of Personally Identifiable Information in response to changes in technology, the increased use of mobile devices, and new business practices.[34] Under the new Rule, "personal information" includes "geolocation information."[35] The FTC's 2012 report considers location data to be "sensitive" information the collection of which requires the affirmative consent of consumers.[36]

Not surprisingly, consumers have significant concerns about the protection of location privacy. A recent survey found that 77% of cell phone users did not want to disclose their location to smartphone "Apps" or developers.[37] Consumers also strongly object when companies secretly enable location-tracking services. In May 2011, researchers discovered that an

---

[29] Foursquare, https://foursquare.com/ (last visited May 16, 2012).
[30] *See* Nick Bilton, *Girls Around Me: An App Takes Creepy to a New Level*, N.Y. Times – Bits (Mar. 30, 2012), http://bits.blogs.nytimes.com/2012/03/30/girls-around-me-ios-app-takes-creepy-to-a-new-level/
[31] 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.
[32] *See* Elec. Privacy Info. Ctr., *Investigations of Google Street View*, https://epic.org/privacy/streetview/.
[33] *See generally* Ctr. for Digital Democracy, Google, Inc., *Request for Investigation and Imposition of Fines and Other Remedies for Violation of "Google Buzz" Consent Decree* (2012), *available at* http://www.centerfordigitaldemocracy.org/sites/default/files/CDDGoogleComplaint022212.pd (describing advances in Google's advertising ecosystem).
[34] Federal Trade Comm'n, *FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule* (Sept. 15, 2011), http://www.ftc.gov/opa/2011/09/coppa.shtm.
[35] Children's Online Privacy Protection Rule, 76 Fed. Reg. 59804, 59813 (proposed Sept. 27, 2011) (to be codified at 16 C.F.R. pt. 312), http://www.ftc.gov/os/2011/09/110915coppa.pdf.
[36] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change* 58 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[37] Harris Interactive, Mobile Privacy: A User's Perspective (Mar. 4, 2011) *available at* http://www.scribd.com/doc/54220855/TRUSTe-Mobile-Privacy-Report.

unencrypted file on Apple iPhones stored a ten-month record of a user's location data.[38] During the 2011 holiday season, several malls decided to use shoppers' cell phones to track their movement from store to store.[39] In each case, consumers were outraged and members of Congress investigated the business practices. [40]

III. The GPS Act Sets Out the Necessary Elements of an Effective Privacy Law

A. The Act Establishes Appropriate Circumstances for the Collection of Location Data

The Act prohibits "[a]ny person" from intentionally intercepting or disclosing location data.[41] The Act also prohibits the use of location information by any person "knowing or having reason to know that the information was obtained through the interception of such information in violation of this [Act]."[42] Finally, the Act prohibits the disclosure of location information for the purposes of obstructing a criminal investigation.[43] These prohibitions mirror the protections found in ECPA, which also prohibits the interception, disclosure, and use of wire, oral, or electronic communications.

Like ECPA, however, the Act does not impose an absolute prohibition on the collection or use of location data. Information acquired in the normal course of business may be used or disclosed if doing so is "a necessary incident to the rendition of the service or to the protection of the rights or property of the provider of the service."[44] Location information may be intercepted through "any system that is configured so that such information is readily accessible to the general public."[45] The Act also allows individuals to consent to the interception of their location information, and parents are permitted to give consent on behalf of their children.[46] Location information may also be used in emergency situations or in situations involving the theft of the device sending geolocation information.[47] Finally, as discussed below, the Act contains an exception for information obtained pursuant to a warrant.

---

[38] Nick Bilton, *Tracking File Found in iPhones*, N.Y. Times, (Apr. 20, 2011) https://www.nytimes.com/2011/04/21/business/21data.html.
[39] Ken Wagstaff, *Will Your Mall Be Tracking Your Cellphone Today?*, Time, (Nov. 25, 2011), http://techland.time.com/2011/11/25/will-your-mall-be-tracking-your-cellphone-today/.
[40] *See* Letter from Al Franken, Chairman, Subcomm. on Privacy, Tech. and the Law, to Steve Jobs, CEO, Apple Corp. (Apr. 20, 2011), *available at* http://www.franken.senate.gov/files/letter/110420_Apple_Letter.pdf; *see also* Ashley Lutz, *Malls Cell-Phone Devices to Track Shoppers Halted After Complaints*, Bloomberg (Nov. 28, 2011), http://mobile.bloomberg.com/news/2011-11-28/cell-phone-technology-to-track-shoppers-halted-after-complaints.
[41] H.R. 2168, 112 Cong. §2602(a)(1)(A)-(B) (2012).
[42] *Id.* §2602(a)(1)(C).
[43] *Id.* §2602(a)(1)(D)(i).
[44] *Id.* §2602(b).
[45] *Id.* §2602(e).
[46] *Id.* §2602(d).
[47] *Id.* §2602(f).

B. The Act Establishes a Warrant Standard for Government Access to Location Data

Under the Act, a government entity may intercept location information "only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure."[48] Warrant requirements provide important checks against government abuse. As Justice Sotomayor stated in *Jones*, "the Fourth Amendment's goal [is] to curb arbitrary exercises of police power [] and prevent 'a too permeating police surveillance.'"[49] As the Supreme Court has long-recognized, a warrant requirement strikes a reasonable balance between the protection of privacy and the needs of law enforcement. "Although some added burden will be imposed upon the Attorney General, this inconvenience is justified in a free society to protect constitutional values."[50] Here, a warrant requirement enables legitimate access to location information by law enforcement while protecting the privacy of individuals.

Although the Act makes clear that Government interception of location information is unlawful absent a warrant, it also provide an exception for emergency situations, similar to the emergency exception in ECPA, 18 U.S.C. § 3125. While this exception includes broad language about "emergency situations" that involve "conspiratorial activities," it also makes clear that, even in an emergency, an officer intercepting location information must apply for a warrant within 48 hours of interception.[51] In the event that the warrant application is denied, the information "shall be treated as having been obtained in violation of this chapter and an inventory shall be served on the person named in the application."[52] This provides a strong deterrent to any officer intercepting location information without sufficient grounds for a warrant.

C. The GPS Act Establishes a Private Right of Action to Ensure Enforcement

Importantly, the Act applies to private parties as well as law enforcement. The Bill prohibits the interception and disclosure of location information by "any person," a term that includes private companies and individuals.[53] The Bill's civil damages provision provides that "any person whose geolocation information is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from a person, other than the United States, which engaged in that violation such relief as may be appropriate."[54] The Bill's damage provision allows plaintiffs to recover the greater of "actual damages suffered by the plaintiff and

[48] *Id.* §2602(h)(2).
[49] *United States v. Jones*, 132 S. Ct. 945, 956, (2012) (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).
[50] *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 299 (1972).
[51] H.R. 2168, 112 Cong. § 2604(a) (2012).
[52] *Id.* § 2605(b) (2012).
[53] *Id.* §2602(a)(1).
[54] *Id.* §2605(a).

any profits made by the violator as a result of the violation" or "statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000."[55]

Private rights of action strengthen enforcement and allow individuals to seek remedies. They empower consumers to enforce the law themselves, create a strong disincentive for the irresponsible handling of consumer data, and provide a necessary backstop to the current enforcement scheme.

Statutory damage provisions ensure that individuals can seek compensation for and deter privacy violations. Harms suffered as a result of privacy violations are often difficult to quantify, and include intrusions upon individuals' autonomy, mental and emotional distress, loss of reputation and trust, and an increased risk of identity theft, financial loss, erroneous credit information, and even bodily harm. Thus, privacy laws frequently feature statutory damage provisions to ensure adequate enforcement of privacy interests.[56]

IV. The European Commission Has Provided an Effective Model for the Protection of Location Privacy

Concerns regarding locational privacy are arising in other countries, as well. The approach of the European Commission, 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,[57] the European Commission has created an effective framework for the regulation of locational data.

The Directive requires that location data other than traffic data be processed anonymously or with the consent of the individual, and provides protections to ensure that this consent is meaningful.[58] 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. Finally, the processing of data is restricted to what is necessary for providing the value-added service.

The Article 29 working party, an E.U. advisory group of experts on privacy and data

---

[55] *Id.* §2605(c).

[56] *See* Fair and Accurate Credit Transactions Act, 15 U.S.C. §§ 1681 *et seq.*; Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510 *et seq.*;Video Privacy Protection Act, 18 U.S.C. § 2710; Driver's Privacy Protection Act, 18 U.S.C. § 2724; Telephone Consumer Protection Act, 47 U.S.C. § 227; Cable Communications Privacy Act, 47 U.S.C. § 551.

[57] 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/eurlex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

[58] *Id.* Art. 9.

protection, has also issued an opinion on geolocation information.[59] The opinion states that "*prior informed consent* is also the main applicable ground for making data processing legitimate when it comes to the processing of the locations of a smart mobile device in the context of information society services."[60] Furthermore, if the purpose for which the data is being used changes in a material way, consent must be obtained again.[61] Finally, the opinion provides that individuals must be able to withdraw their consent without suffering negative consequences for the use of their device.[62]

The Transatlantic Consumer Dialogue (TACD) has also passed a resolution on mobile commerce that addresses privacy concerns of consumers.[63] 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."

V. EPIC's Recommendations

A. There Should be Limitations on the Use of Location Data

As currently drafted, the bill regulates the interception of location data, but once consent is obtained, there are no limitations on use of this information. The bill should be modified so that location data is only used consistent with the context in which it was provided. Moreover, consumers should have the opportunity to access the location data that is collected and there should be limitations on the period of storage for location data.

In particular, a purpose-specification or "respect for context" principle is likely to play an important role in the protection of location privacy. In many cases, location information is already collected by companies. The privacy risk, therefore, comes not in the collection (or "interception") of location information, but in its use. For example, Verizon recently started using geolocation information for business, marketing, and advertising purposes after failing to give new customers meaningful notice of these changes.[64] Currently, the Bill only prohibits the "use" of location information if that information was obtained through interception, *i.e.*, illegally.[65] The application of a context- or purpose-specification principle would prohibit data use that violates contextual integrity, instead of only prohibiting data use that follows an illegal interception.

---

[59] Working Party 29 Opinion Geolocation services on smart mobile devices, 881/11/EN, May 2011, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.
[60] *Id.* at 14.
[61] *Id.* at 15.
[62] *Id.* at 16.
[63] Transatlantic Consumer Dialogue, Resolution on Mobile Commerce, August 2005, http://www.tacd.org/cgibin/db.cgi?page=view&config=admin/docs.cfg&id=283.
[64] *See* Elec. Privacy Info. Ctr., *In re Verizon Wireless*, https://epic.org/privacy/ftc/in_re_verizon.html (last visited May 16, 2012).
[65] H.R. 2168, 112 Cong. §2602(a)(1)(C).

B, The Act's Consent and Public Information Exceptions Should Be Clarified

The Act provides an across-the-board prohibition on the interception, disclosure, and use of location information, subject to a few discrete exceptions.[66] This framework makes clear that location information is sensitive, protected, personal information that cannot be misused. However, in order for this prohibition to be effective the exceptions must be narrow and clear. The Act defines an exception allowing interception of location information "pertaining to another person if such other person has given prior consent,"[67] but it does not explain or imply what sort of consent is required. The Act also provides for an exception where location information is accessed "through any system that is configured so that such information is readily accessible to the general public,"[68] without reference to the source or use of such information. If these exceptions are not narrowly defined, they could provide an enormous loophole for third party collection and disclosure of sensitive location information.

The Act's consent exception is crucial. Section 2602(d) creates an exception for interceptions of location information "pertaining to another person if such other person has given prior consent to such interception."[69] Companies have often intercepted location data without the affirmative consent of consumers. When Verizon and OnStar announced the collection of location information, they obtained "consent" by requiring consumers to opt out of such collection. And when several malls announced that they would begin monitoring the paths that consumers traveled from store to store, the "consent" of consumers was obtained through a few lines of text attached to a mall directory. Arguably, announcing a practice and then requiring consumers to opt-out of that practice does not constitute "prior" consent as the statute requires, nor do inconspicuous notices provide a means of "giv[ing]" consent. However, the Bill's language is sufficiently unclear to allow for the interception of location information through hidden notices or on an opt-out basis. The approach recommended by the FTC, the Trans-Atlantic Consumer Dialog, and EPIC, is to ensure that consent is meaningful by requiring consumers to opt in to the use of their location data.

Section (e) of the Act outlines the exception for "public information," which specifies that it is not unlawful to access location information "through any system that is configured so that such information is readily accessible to the general public."[70] Similar language in the Wiretap Act has recently been a source of confusion and controversy in the case of Google's Street View program.[71] Section (e) is also likely to be a source of confusion, since it does not make clear whether configuring a system in such a way that "information is readily accessible" eliminates all protections for users of that system. It is also unclear whether accessing location

[66] *Id.* § 2602(a)(1).
[67] *Id.* § 2602(d)(1).
[68] *Id.* § 2602(e).
[69] *Id.* § 2602(d).
[70] *Id.*§ 2602(e).
[71] *See* Elec. Privacy Info. Ctr., *Ben Joffe v. Google*, http://epic.org/amicus/google-street-view/ (last visited May 16, 2012).

information through such a system would allow downstream misuses that would otherwise be prohibited. More fundamentally, the Act does not provide a definition, or even an example, of "readily accessible" information.

Users may not know, or may not have control over, the configuration of a particular system that they use, like Foursquare or Facebook.[72] Some systems enable location sharing by default, without the users' explicit consent, and would thus broadcast location information in a way that could allow downstream misuse.[73] More importantly, privacy settings on social media sites typically allow different degrees of privateness.[74] Even when a person has control over the configuration of such a system, as in the case of a home Wi-Fi network, it is unclear why a configuration that allows "access" to location information should authorize collection of that data, except to the extent that it indicates consent under Section (d).[75] As currently drafted, Section (e) causes confusion, acts as a potentially large loophole for all online information collection, and provides no clear benefit over the consent-based exception.

C. The GPS Act Should Apply Fair Information Practices to Location Data Stored by Private Actors

Fair Information Practices (FIPs) can provide an effective solution to location privacy concerns. One recent formulation, the Consumer Privacy Bill of Rights contained in the Administration's listed the following principles:

- Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices.
- Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- Security: Consumers have a right to secure and responsible handling of personal data.

---

[72] *See* Julia Angwin & Jeremy Singer-Vine, *Selling You on Facebook*, WALL ST. J. (Apr. 7, 2012), at C1.

[73] This is especially clear in the case of recent apps that combine personal location information with other related information to provide a "mapping" service. *See* Nick Bilton, *Girls Around Me: An App Takes Creepy to a New Level*, N.Y. Times – Bits (Mar. 30, 2012), http://bits.blogs.nytimes.com/2012/03/30/girls-around-me-ios-app-takes-creepy-to-a-new-level/.

[74] *See* Naomi Gleit, *More Privacy Options*, Facebook Blog (Mar. 19, 2008), http://blog.facebook.com/blog.php?post=11519877130.

[75] It is important to note that one of the goals of Google's Street View program was to collect and map the location of private Wi-Fi networks, which it did by logging network data from "open" networks across the world. *See* Elec. Privacy Info. Ctr., *Investigations of Google Street View* , https://epic.org/privacy/streetview/ ((last visited May 16, 2012). Even Google recognized that such sweeping collection of personal information required some degree of consent, and they eventually allowed users to "opt out" of their program. Kevin J. O'Brien, *Google Makes Sweeping Concession on Data Collection*, N.Y. TIMES, Nov. 16, 2011.

- Access and Accuracy: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
- Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- Accountability: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.[76]

FIPs are central to American privacy law, appearing most prominently in the Privacy Act of 1974.[77] Trans-Atlantic consumer groups have recommended similar principles in the context of location privacy, such as transparency, data minimization, purpose limitation, limitation of data retention periods and data security.[78] EPIC recommends that the Act apply FIPs to stored location data.

VI. Conclusion

EPIC respectfully requests that the Subcommittee take the following steps outlined in this statement:

- In general, adopt FIPs to location data stored by private actors;
- Specifically, adopt purpose-specification and data limitation requirements;
- Clarify the consent exception to require that users affirmatively consent to data collection;
- Clarify the public information exception to prevent the creation of a loophole for online information collection.

Thank you for your consideration of our views. We would be pleased to provide any further information the Committee requests.

[76] White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy, Feb. 23, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.
[77] *See* Privacy Act of 1974, 5 USC § 552a.
[78] Transatlantic Consumer Dialogue, Protecting Mobile Privacy in a Hyper-local World, May 2012.