epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

February 14, 2019

The Honorable Lindsey Graham, Chairman
The Honorable Dianne Feinstein, Ranking Member
U.S. Senate Committee on the Judiciary
226 Dirksen Senate Office Building
Washington, DC 20510
Facsimile: (202) 224-9102

Dear Chairman Graham and Ranking Member Feinstein:

We write to urge you to hold a hearing on the need for legal protections for Americans' cell phone location data. A detailed report in *The Wall Street Journal* revealed that federal agencies are accessing cell phone location data without warrants or judicial oversight.[1] These agencies are engaging in warrantless location surveillance despite the Supreme Court's ruling in *Carpenter v. United States*, 138 S. Ct. 2206 (2018) that officers must obtain a warrant in order to collect cell phone location data. The sale of location data by data brokers, which made this warrantless tracking possible, is a threat to the privacy and security of all Americans. The Judiciary Committee should close the loopholes that have allowed warrantless location tracking to take place.

The Committee should act quickly on this matter.[2] Cell phones are an essential part of everyday life; we all use mobile apps for personal, financial, business, education, entertainment, and social activities. *Riley v. California*, 573 U.S. 373, 396 (2014). But many of these apps also collect a significant amount of data about who we are, where we are, and what we are doing.[3] Users might permit the disclosure of data that is necessary for the functions of an app (e.g. to find where they are on a map, hail a ride, or check the nearby weather). But these apps should not disclose location data to data brokers. And that data should not be used for warrantless surveillance.

The Supreme Court established in *Carpenter* and *Riley* that cell phone data is entitled to Fourth Amendment protections but also encourages Congress to address this complex issue through legislation.[4] The Stored Communications Act, 18 U.S.C. §§ 2701 et seq., does not currently protect

---

[1] Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.

[2] *See* Editorial Board, *The Government Uses 'Near Perfect Surveillance' Data on Americans*, N.Y. Times (Feb. 7, 2020), https://www.nytimes.com/2020/02/07/opinion/dhs-cell-phone-tracking.html.

[3] https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf.

[4] *Carpenter*, 138 S. Ct. at 2496 (Alito, J., concurring) ("it would be very unfortunate if privacy protection in the 21st century was left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.") *See also* Marc Rotenberg, *Carpenter Fails to Cabin Katz as Miller Grinds to a Halt: Digital Privacy and the Roberts Court*,

cell phone location data.[5] Congress should now establish location privacy provisions in Chapter 121.[6] The "Location Privacy Protection Act," which was previously introduced several times by a group of Senators on the Judiciary Committee, would add a new § 2713.[7] The new section should prohibit the unauthorized collection or disclosure of geolocation information from a communications device. This general prohibition would be subject to several narrow exceptions, including for law enforcement access pursuant to a warrant. The law should also require companies that collect geolocation information to make public the nature of their collection as well as the purposes, uses, and disclosures that they make. The law should require these companies to provide a simple mechanism for users to access, delete, or revoke authorization to collect their location data. The law should also establish minimum data security standards for companies that store this data, and should limit how long the data can be retained. Finally, the law should be enforceable by federal prosecutors, state attorneys general, and by individual civil action.

As we stated previously, the Committee should act quickly on this request. The Department of Justice recent announcement that the United States has charged four Chinese military officials for breaking into Equifax, and compromising the authenticating details of Americans, underscores the need for legislative action.[8] The more personal data a company collects, the more they become a target for criminal and nation-state hackers. The collection and aggregation of personal data poses both safety and national security risks. And there is no reason to continue along this path. Both law enforcement and the companies that operate in the mobile app industry should be subject to the same privacy laws and regulations that we have applied to other companies including telephone service providers, internet service providers, cable and satellite tv providers, video rental providers, and healthcare providers.[9]

The Committee should convene a hearing to consider legislative proposals and to address the questions raised by the *Wall Street Journal* report about the sale of location data to law enforcement agencies. Specifically, the Committee should address the following questions:

- How many agencies are currently collecting location data?
- How many data points do these agencies collect per year?
- When did this practice begin?
- How do the agencies acquire location data?
- What data is included?

ACS Supreme Court Review (2018), https://www.acslaw.org/analysis/acs-supreme-court-review/carpenter-fails-to-cabin-katz-as-miller-grinds-to-a-halt-digital-privacy-and-the-roberts-court/.

[5] *See, e.g.*, 18 U.S.C. § 2710; 47 U.S.C. § 552.

[6] Amending the SCA provisions, 18 U.S.C. §§ 2701–2704, would not be workable because the "electronic communications service" and "remote computing service" definitions are too narrow to capture all entities that collect, use, and disclose cell phone location data.

[7] S. 2270, 114th Cong. (1st Sess. 2015).

[8] Kevin Johnson, *Four Members of Chinese Army Charged with Stealing 145 Million Americans' Data in 2017 Equifax Hack*, USA Today (Feb. 10, 2020), https://www.usatoday.com/story/news/politics/2020/02/10/doj-chinese-army-hacked-equifax-stole-145-million-americans-data/4711796002/.

[9] *See* 47 U.S.C. § 222; 15 U.S.C. §§ 6501–6506; 47 U.S.C. § 552; 47 U.S.C. § 338(i); 18 U.S.C. § 2710; 47 C.F.R. §§ 160 et seq.

- How is the data accessed, stored, and used?
- How long is the data retained?
- What legal or administrative oversights or procedures are in place for location data access?

There has been insufficient oversight of law enforcement's location surveillance activities. When Congress enacted the Wiretap Act it established a comprehensive reporting regime to monitor the Government's use of surveillance techniques.[10] But there is no similar reporting regime for location surveillance. We currently have no accurate measurement of how often law enforcement or other agencies are collecting location data. Federal prosecutors have even argued that they have no way to locate all of the location data surveillance orders that they have obtained in the last few years.[11] The problem is likely larger than any one story or anecdote could capture.

Thank you for your timely attention to this pressing issue. We ask that you hold a hearing on this important issue and that our statement be entered in the hearing record.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

/s/ Alan Butler
Alan Butler
EPIC Senior Counsel

Cc: Chairman Jerry Nadler, House Judiciary Committee
Ranking Member Doug Collins, House Judiciary Committee

[10] *See* Admin. Office of the U.S. Courts, *FAQs: Wiretap Reports* (2019), https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports/faqs-wiretap-reports. EPIC tracks these reports and provides updated tables and graphs every year. EPIC, *Title III Wiretap Orders – Stats* (2019), https://epic.org/privacy/wiretap/stats/wiretap_stats.html.

[11] *See* EPIC, *EPIC v. DOJ (CSLI Section 2703(d) Orders)* (2020), https://epic.org/foia/doj/location-data/.