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 8, 2019

The Honorable Jerrold Nadler
Chairman
U.S. House Committee on the Judiciary
2141 Rayburn House Office Building
Washington, DC 20515

The Honorable Doug Collins
Ranking Member
U.S. House Committee on the Judiciary
2141 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Nadler and Ranking Member Collins:

We write to you in advance of your hearing, *Oversight of the U.S. Department of Justice*.[1] The committee should take this opportunity to ensure the Department of Justice operates transparently and protects American consumers. The Committee should also learn the Department's views on domestic surveillance after the Supreme Court's decision in *Carpenter v. United States*.[2]

The Electronic Privacy Information Center (EPIC) was established in 1994 to focus public attention on emerging privacy and civil liberties issues.[3] Over the years, EPIC has worked with administrations of both parties and has frequently submitted statements to this Committee.[4]

Americans are rightly concerned about the scope of government surveillance, the impact of new technologies, and the protection of constitutional freedoms.[5] The Department of Justice must update policies to reflect changing technologies and legal precedent. The Department must safeguard the public consistent with the rule of law and our constitutional heritage. To this end, this Committee should ensure that the DOJ operates transparently and consistently with Supreme Court precedent.

---

[1] *Oversight of the U.S. Department of Justice*, U.S. House Comm. on Judiciary (Feb. 8, 2019), https://judiciary.house.gov/legislation/hearings/oversight-us-department-justice.
[2] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[3] EPIC, *About EPIC* (2016), https://epic.org/epic/about.html.
[4] *See, e.g.*, EPIC v. FBI, 865 F. Supp. 1 (D.D.C. 1994) (concerning FBI director wiretapping surveys); EPIC v. DOD, 241 F. Supp. 2d 5 (D.D.C. 2003) (concerning the Total Information Awareness program); EPIC v. FBI, 72 F. Supp. 3d 338 (D.D.C. 2014) (concerning the agency's "Next Generation Identification" program);
Statement from EPIC to the H. Comm. on Judiciary (Dec. 12, 2018), https://epic.org/testimony/congress/EPIC-HJC-AntitrustOversight-Dec2018.pdf (concerning oversight of the antitrust agencies); Statement from EPIC to H. Comm. on Judiciary (Dec. 10, 2018), https://epic.org/testimony/congress/EPIC-HJC-GoogleOversight-Dec2018.pdf (concerning Google's business practices).
[5] Abigail Geiger, *How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks*, Pew Res. Ctr. (June 4, 2018), http://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/.

Congress Should Work with the Department to Update Federal Wiretap Law After *Carpenter*

Last year, the U.S. Supreme Court overturned the Fourth Amendment exception that permitted warrantless searches of records held by third parties.[6] In *Carpenter v. United States*, the Court held that the Fourth Amendment protects cell phone location data and that the government must generally obtain a warrant before obtaining location data from a private party.[7] Congress has an opportunity to enact broad protecting consumers' personal data, similar to the federal wiretap act of 1968 enacted after major Court decisions in *Katz v. United States* and *Berger v. New York*.[8]

Congress and the Department should work together to codify protections for Americans' personal data held by third parties.[9] An updated law will provide clarity for law enforcement and meaningful protections for Americans. Any updated law should:

- Establish across-the-board warrant requirements for compelled disclosure of all categories of personal data held by third parties, subject only to narrow exceptions defined in the statute;
- Impose particularity requirements and provide for judicial oversight of searches conducted on seized hard drives and other data repositories;
- Limit retention periods for seized personal data and establish deletion obligations;
- Provide for actual notice of warrants to data subjects and limit the use of gag orders on service providers; and
- Expand a "wiretap report"-style transparency regime to all surveillance orders and ensure adequate oversight.

The Department Should Improve Reporting on Surveillance Orders

For over twenty years, EPIC has reviewed the Administrative Office of the U.S. Courts' annual reports on the use of federal wiretap authority. EPIC also analyzes the annual letters provided by the Attorney General to Congress regarding the use of FISA authority.[10] EPIC posts

---

[6] Carpenter, *supra* note 2.
[7] *Id.* at 2217.
[8] Katz v. United States, 389 U.S. 347, 361 (1967); Berger v. New York, 388 U.S. 41 (1967); EPIC, *Electronic Communications Privacy Act (ECPA)*, https://epic.org/privacy/ecpa/.
[9] *See* Marc Rotenberg, *Carpenter Fails to Cabin Katz as Miller Grinds to a Halt: Digital Privacy and the Roberts Court*, Am. Const. Soc. S. Ct. Rev. (Dec. 4, 2018), https://www.acslaw.org/analysis/acs-supreme-court-review/carpenter-fails-to-cabin-katz-as-miller-grinds-toa-halt-digital-privacy-and-the-roberts-court/; Alan Butler, *Supreme Court Puts Us On a Pro-Privacy Path for the Cyber Age*, Hill (June 29, 2018), http://thehill.com/opinion/judiciary/394808-supreme-court-puts-uson-a-pro-privacy-path-for-the-cyber-age.
[10] *See, e.g.*, Admin. Office of the U.S. Courts, *Wiretap Report 2015*, http://www.uscourts.gov/statistics-reports/wiretap-report-2015; Letter from Assistant Attorney General Peter Kadzik to Charles Grassley, Chairman, U.S. Senate Committee on the Judiciary, et al., Apr. 28, 2016, https://fas.org/irp/agency/doj/fisa/2015rept.pdf.

these reports and letters when they are available and notes significant changes and developments.[11]

The annual report prepared by the Administrative Office of the U.S. Courts provides a basis to evaluate the effectiveness of wiretap authority, to measure the cost, and even to determine the percentage of communications captured that were relevant to an investigation. These reporting requirements ensure that law enforcement resources are appropriately and efficiently used while safeguarding important constitutional privacy interests.

By way of contrast, the Attorney General's annual FISA report provides virtually no meaningful information about the use of FISA authority other than the applications made by the government to the Foreign Intelligence Surveillance Court.[12] There is no information regarding cost, purposes, effectiveness, or even the number of non-incriminating communications of U.S. persons collected by the government.

Congress should ensure that the Department only collects location data when it is prepared to be transparent about the practice. As of today, the Department has never publicly released any comprehensive reports concerning the collection and use of cell site location information. In 2017, EPIC submitted two Freedom of Information Act requests to the Department seeking the release of any such reports.[13] EPIC has since sued the DOJ for failing to respond to its FOIA requests.[14] Despite repeated oversight requests and public litigation, there is little to no information available to Congress or the public about how the Department collects the location information of Americans.

The release of federal wiretap reports provides necessary public accountability of federal wiretap practices. These reports allow Congress and others to evaluate the effectiveness of DOJ programs and to ensure that civil rights are protected. The reports protect sensitive information about investigations and provide aggregate data about the government's surveillance activities. Congress should ensure that the Department follows that approach when it collects location information or submits FISA requests, particularly after the Supreme Court's decision in *Carpenter*.

The Department Has an Obligation to Protect Consumers

American consumers have faced a constant barrage of privacy invasions and data breaches over the last five years. Facebook granted unauthorized access to sensitive profile

[11] *See* EPIC, *Title III Wiretap Orders: 1968-2015*, http://epic.org/privacy/wiretap/stats/wiretap_stats.html; EPIC, *Foreign Intelligence Surveillance Act*, http://epic.org/privacy/terrorism/fisa/; EPIC, *Foreign Intelligence Surveillance Court (FISC)*, https://epic.org/privacy/terrorism/fisa/fisc.html.

[12] It is clear from the Attorney General's annual reports that FISC applications are routinely approved with very rare exceptions. *See* Amnesty Int'l USA v. Clapper, 638 F.3d 118, 140 (2d Cir. 2011) ("Empirical evidence supports this expectation: in 2008, the government sought 2,082 surveillance orders, and the FISC approved 2,081 of them."). Of the Government's 1,499 requests to the FISC for surveillance authority in 2015, none were denied in whole or in part. *See* 2011 FISA Annual Report to Congress, https://fas.org/irp/agency/doj/fisa/2011rept.pdf.

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

[14] EPIC v. DOJ, No. 18-1814 (D.D.C. Aug. 1, 2018).

information and photographs, Equifax lost control of social security numbers and put millions of Americans at risk, and other companies are collecting, selling, and disclosing consumers' location data without their knowledge. There is a clear need for greater privacy protection in America.

The Department recently took the unprecedented step of filing a brief in the Supreme Court against the interests of consumers and against enforcement of federal law. The case, *Frank v. Gaos*,[15] alleges that Google disclosed consumers' private search data to third parties in violation of federal law. The United States intervened in the case and argued that consumers do not have standing to sue for violations of their federal privacy rights.[16] In the past, the United States has argued that consumers who allege that their rights under federal law have been violated have standing to sue. In *Gaos*, the Department argued the exact opposite.

This Committee should ask the Department for its views on the proper role of the DOJ in such circumstances. For example, should the Department encourage the protection of consumers and enforcement of federal law, or should it discourage such enforcement and instead promote the interests of companies who have been sued for violating privacy rights?

Implementation of the CLOUD Act

Last year, Congress passed the CLOUD Act,[17] which clarifies procedures for U.S. law enforcement to access data stored overseas by U.S. companies and sets procedures for when foreign powers may obtain data in the United States. Under the CLOUD Act, the U.S. government may enter into executive agreements that allow foreign governments to directly access data held by American service providers.[18] Once enacted, the agreements allow foreign governments to bypass review or approval U.S. government and demand data directly from U.S. companies without oversight.

This Committee and the Department must therefore ensure that any agreements made under the CLOUD Act scrupulously protect Americans' rights. This responsibility is clearly defined by the Act itself: Before approving foreign access to American data, the Departments of Justice and State must certify to the House that the foreign government provides "robust" privacy and civil liberties safeguards and minimizes data collection and retention.[19]

The House is given the opportunity to review any proposed agreements and the findings of the executive departments. If it does not object, the agreement goes into effect after 180 days. The House must take seriously its obligation to review proposed agreements. It should ensure that well-established international protections—such as notice to data subjects—are written into agreements. It should press the next Attorney General to require agreements to provide

[15] In re Google Referrer Header Litig., 869 F.3d 737 (9th Cir. 2017), *cert. granted sub nom*, Frank v. Gaos, (U.S. Apr. 30, 2018) (No. 17-961).
[16] *See* Brief for the United States as Amicus Curiae Supporting Respondents, Spokeo v. Robins, 136 S. Ct. 1540 (2016) (No. 13-1339).
[17] Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, Division V.
[18] *Id.* at § 105.
[19] *Id.* at § 105(a).

safeguards and meaningful recourse for individuals who are wrongly targeted. It should further ensure that criteria used to determine eligibility for executive agreements under the CLOUD Act are subject to public review.

The House should also ensure that data-sharing provisions in the CLOUD Act will not be abused to skirt existing U.S. law. The CLOUD Act permits foreign governments to share information with other countries, including the United States. The House must ensure that U.S. law enforcement and intelligence agencies do not simply end-run U.S. law by requesting information on U.S. persons from foreign governments certified under the CLOUD Act.

Thank you for your consideration. We would welcome the opportunity to provide additional information to the Committee. We ask that this statement be entered in the hearing record.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Alan Butler*
Alan Butler
EPIC Senior Counsel

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Jeff Gary*
Jeff Gary
EPIC Legislative Fellow