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

January 14, 2019

The Honorable Lindsey Graham, Chairman
The Honorable Dianne Feinstein, Ranking Member
U.S. Senate Committee on the Judiciary
Dirksen Senate Office Building 224
Washington, DC 20510

Dear Chairman Graham and Ranking Member Feinstein:

We write to you regarding the nomination of William Barr to become the next Attorney General of the United States.[1] Although EPIC takes no position for or against the nominee, this hearing provides a critical opportunity to explore the nominee's views on privacy and to set out priorities for the Department of Justice in 2019.

The Electronic Privacy Information Center (EPIC) was established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] Over the years, EPIC has pursued a wide range of matters with Attorneys General of both Democratic and Republican administrations and we have frequently submitted statements to this Committee.[3]

Americans are rightly concerned about the scope of government surveillance, the impact of new technologies, and the protection of Constitutional freedoms.[4] The Department of Justice has an important role to play in updating policies to reflect changing technologies and legal precedent. And the Attorney General of the United States must safeguard the public in a manner consistent with the rule of law and our Constitutional heritage. Mr. Barr's previous Congressional testimony raises substantial concerns that this nominee is out of step with the views of the American people and the Court.

---

[1] *Nomination of the Honorable William Pelham Barr to be Attorney General of the U.S.*, U.S. Senate Comm. on the Judiciary (Jan. 15, 2019), https://www.judiciary.senate.gov/meetings/nomination-of-the-honorable-william-pelham-barr-to-be-attorney-general-of-the-united-states.

[2] EPIC, *About EPIC*, https://epic.org/epic/about.html.

[3] *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); The Future of Drones in America: Law Enforcement and Privacy Considerations: Hearing Before the S. Comm. on the Judiciary, 113th Cong. 7–8 (2013) (statement of Amie Stepanovich, EPIC); Letter from EPIC to the S. Comm. on Judiciary (Sept. 9, 2005), https://www.epic.org/privacy/justices/roberts/0905letter.pdf (concerning the nomination of Roberts, J., to the Supreme Court).

[4] Abigail Geiger, *How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks*, Pew Research Center (June 4, 2018), http://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/.

The Senate Judiciary Committee should pursue questions with the nominee about these issues, particularly whether Mr. Barr still believes that Americans have no Fourth Amendment rights in records held by third-parties.

Barry has Supported the Warrantless Surveillance of the American People

Mr. Barr has consistently supported warrantless surveillance of the American people, which is contrary to our Constitutional heritage and the plain text of the Fourth Amendment. In 1996 testimony, Barr said:

> [T]his country would be well-served if there was more coordination of technology in the law enforcement area under the Attorney General, and the application of intelligence kinds of technology into law enforcement applications. We have a lot of technology that's emerging. It would be tremendous for law enforcement -- ways of identifying people, ways of following people.[5]

And in 2003, Barr told the House Intelligence Committee that FISA was "too restrictive," specifically:

> Another area under FISA that remains too restrictive relates to the government's ability to obtain third-party business records. […] The law is clear that a person has no Fourth Amendment rights in these records left in the hands of third parties. Having willingly entered into transactions with other people, one loses any legitimate expectation of privacy in the records that reflect those transactions. Thus, the government is free to obtain such records from third parties without any showing of probable cause; it is enough that the records are relevant to an investigation.[6]

The Supreme Court made clear in *Carpenter* that there are limits to the third-party doctrine.[7] ***The Committee should ask Mr. Barr whether he still believes that individuals have no Fourth Amendment right in records held by third parties.***

Furthermore, after 9-11 the National Security Agency (NSA) began the mass collection of phone, email, and Internet records of Americans.[8] This program, code-named "Stellar Wind," operated in secret, authorized broad scale warrantless surveillance of Americans and was overturned by the passage of the Freedom Act.[9] Hearings by this Committee made clear that the program failed to achieve its stated goals.[10] Stellar Wind had its roots in the first-ever bulk-collection program,

---

[5] Hearing Before the Comm'n on the Roles and Capabilities of the U.S. Intelligence Community (1996) (statement of William Barr), https://fas.org/irp/commission/testbarr.htm.
[6] Hearing Before the House Select Comm. on Intelligence, 108th Cong. 10 (2003) (statement of William Barr), https://fas.org/irp/congress/2003_hr/103003barr.pdf.
[7] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
[8] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.
[9] Pub. L. 114-23, 129 Stat. 268 (June 2, 2015).
[10] *Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs*, 113th Cong. (2013), S. Comm. Judiciary, https://www.judiciary.senate.gov/meetings/time-change-and-location-change-strengthening-privacy-rights-and-national-security-oversight-of-fisa-surveillance-programs; *Continued Oversight of the Foreign Intelligence Surveillance Act*, 113th Cong. (2013), S. Comm. Judiciary,

approved by the nominee during his previous tenure as the Attorney General.[11] The program, carried out by the Drug Enforcement Agency, tracked billions of Americans' phone calls without ever obtaining a warrant or informing the public.

Through Stellar Wind, the NSA used secret court orders to collect Americans' private information from telephone service providers. During the formative years of the program, the nominee served as the general counsel and executive vice president of Verizon, one of the largest mobile providers at the time. Reports indicate that Verizon participated in the program, exposing millions of Americans to warrantless surveillance by the U.S. government.[12]

After information surveillance programs came to light, it was Barr who led the telecommunications industry's lobbying charge for immunity from lawsuits related to their assistance in the programs.[13] This raises troubling concerns about his willingness to comply with the requirements of the Fourth Amendment and ensure adequate oversight for the extraordinary surveillance powers of the federal government.

DOJ Should Work With Congress to Update Federal Wiretap Law After Carpenter

In *Carpenter v. United States*, the Supreme Court overturned the Fourth Amendment exception that permitted warrantless searches of records held by third parties.[14] The Court held that the Fourth Amendment protects cell phone location data and found that the government must generally obtain a warrant before seeking to obtain such data from a private party.[15] There is an opportunity for a broad statute setting concerning access to personal data, similar to the federal wiretap act of 1968 that followed after the decisions in *Katz v. United States*[16] and *Berger v. New York*.[17]

DOJ and Congress should work together to update the statutory framework for protection of personal data held by third parties following the Supreme Court's decision in *Carpenter v. United States*.[18] The framework should:

---

https://www.judiciary.senate.gov/meetings/continued-oversight-of-the-foreign-intelligence-surveillance-act; *The Surveillance Transparency Act of 2013*, 113th Cong. (2013), S. Comm. Judiciary, Subcomm. Privacy, Tech, and the Law, https://www.judiciary.senate.gov/meetings/the-surveillance-transparency-act-of-2013.

[11] Brad Heath, *U.S. Secretly Tracked Billions of Calls for Decades*, USA TODAY (Apr. 7, 2015), https://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616.

[12] James Bamford, *The NSA Is Building the Country's Biggest Spy Center*, WIRED (Mar. 15, 2012), https://www.wired.com/2012/03/ff-nsadatacenter/.

[13] Mark Hosenball, *Terror Watch: A Secret Lobbying Campaign*, Newsweek (Sept. 19, 2007), https://www.newsweek.com/terror-watch-secret-lobbying-campaign-99841.

[14] *Carpenter, supra* note 7.

[15] *Id.* at 2217.

[16] *Katz v. United States*, 389 U.S. 347, 361 (1967).

[17] *Berger v. New York*, 388 U.S. 41 (1967).

[18] *See* Marc Rotenberg, *Carpenter Fails to Cabin Katz as Miller Grinds to a Halt: Digital Privacy and the Roberts Court*, American Constitution Society Supreme Court Review (December 4, 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/; Alan Butler, *Supreme Court puts us on a pro-privacy path for the cyber age*, The Hill (June 29, 2018), http://thehill.com/opinion/judiciary/394808-supreme-court-puts-us-on-a-pro-privacy-path-for-the-cyber-age.

- Establish an across-the-board warrant requirement 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;
- Expanded "wiretap report"-style transparency regime to all surveillance orders and ensure adequate oversight.

DOJ Should Improve Reporting on Surveillance Orders

For over twenty years, EPIC has reviewed the annual reports produced by the Administrative Office of the US Courts on the use of federal wiretap authority as well as the letter provided each year by the Attorney General to the Congress regarding the use of the FISA authority.[19] EPIC routinely posts these reports when they are made available and notes any significant changes or developments.[20]

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.[21] There is no information about cost, purposes, effectiveness, or even the number of non-incriminating communications of US persons that are collected by the government. Similarly, The Department of Justice has never released to the public any comprehensive reports concerning the collection and use of cell site location information. In 2017, EPIC submitted two Freedom of Information Act requests to DOJ seeking the release of reports on the collect and use of cell site location information.[22] EPIC has since sued DOJ for failure

[19] *See, e.g.,* Administrative Office of the US 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.
[20] *See Title III Wiretap Orders: 1968-2015*, EPIC, http://epic.org/privacy/wiretap/stats/wiretap_stats.html; *Foreign Intelligence Surveillance Act*, EPIC, http://epic.org/privacy/terrorism/fisa/; *Foreign Intelligence Surveillance Court (FISC)*, EPIC, https://epic.org/privacy/terrorism/fisa/fisc.html.
[21] 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, *supra*, note 3.
[22] EPIC, *EPIC v. DOJ (CSLI Section 2703(d) Orders)*, https://epic.org/foia/doj/location-data/.

to respond to our FOIA requests.[23] There is little to no information available to Congress or the public about how these authorities are used and what impact that has on the privacy of individuals.

The use of aggregate statistical reports has provided much needed public accountability of federal wiretap practices. These reports allow Congress and interested groups to evaluate the effectiveness of Government programs and to ensure that important civil rights are protected. Such reports do not reveal sensitive information about particular investigations, but rather provide aggregate data about the Government's surveillance activities. That is the approach that should be followed now for FISA and CSLI, particularly after the Supreme Court's decision in *Carpenter*.

The nominee should be asked whether he believes DOJ should publicly report statistics on FISA and CSLI orders.

DOJ's Obligation to Protect Consumers

Does DOJ have a duty to advocate for the enforcement of federal law and the protection of American 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 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.

DOJ recently took the unprecedented step of filing a brief in the Supreme Court against the interests of consumers and against the enforcement of federal law. The case, *Frank v. Gaos*,[24] arises out of a complaint filed on behalf of Google users who allege that the company disclosed their private search data to third parties in violation of federal law. The parties agreed to settle the case without any substantial change in Google's business practices, and the Court originally granted Certiorari to resolve whether that settlement was "fair, reasonable, and adequate."[25] The United States filed a motion to intervene in the case, which the Court granted. But the Court subsequently requested additional briefing from the parties and the United States concerning "whether any named plaintiff has standing such that the federal courts have Article III jurisdiction over this dispute." In the past, the Government has intervened to argue that consumers who allege that their rights under federal law have been violated have standing to sue.[26] But DOJ broke that trend in *Gaos*, and filed two separate briefs arguing that consumers do not have standing to sue for violations of their federal privacy rights.

Mr. Barr should be asked what the proper role of the DOJ is in such circumstances: is it to encourage the protection of consumers and enforcement of federal law, or to discourage such enforcement and instead promote the interests of companies who have been sued for violating privacy rights?

Implementation of the CLOUD Act

[23] *EPIC v. DOJ*, No. 18-1814 (D.D.C. Aug. 1, 2018).
[24] In re Google Referrer Header Litig., 869 F.3d 737 (9th Cir. 2017), *cert. granted sub nom*, *Frank v. Gaos*, 138 S. Ct. 1697 (2018).
[25] *See* EPIC, *Frank v. Gaos* (2018), https://epic.org/amicus/class-action/gaos/.
[26] *See* Brief for the United States as Amicus Curiae, *Spokeo v. Robins*, 136 S. Ct. 1540 (2016) (13-1339).

Last year, Congress passed the CLOUD Act,[27] which clarifies when U.S. law enforcement may demand data stored overseas by American companies, and sets procedures for when foreign powers may request data stored 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.[28] 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.

The Senate and the next Attorney General 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 Senate that the foreign government provides "robust" privacy and civil liberties safeguards and minimizes data collection and retention.[29]

The Senate 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 Senate 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 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 Senate 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 Senate 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.

We appreciate your consideration of EPIC's views, and 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

[27] Consolidated Appropriations Act, 2018, PL 115-141, Division V.
[28] *Id.* at § 105.
[29] *Id.* at § 105(a).