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 7, 2019

Privacy and Civil Liberties Oversight Board
800 North Capitol Street NW, Suite 565
Washington, DC 20002

Dear Members of the Privacy and Civil Liberties Oversight Board:

We write to you in advance of your upcoming forum "Countering Terrorism while Protecting Privacy and Civil Liberties: Where do We Stand in 2019?"[1] With a full panel of members hopefully appointed soon, 2019 provides a critical opportunity to set out priorities for PCLOB and release long overdue reports. The PCLOB plays a vital role safeguarding the privacy rights of Americans and ensuring oversight and accountability of the Intelligence community. In this letter, EPIC sets out five crucial priorities for the PCLOB in 2019:

1) *Release the Board's report on Executive Order 12333;*
2) *Review the use of facial recognition technology by federal agencies and propose appropriate safeguards;*
3) *Review the use of artificial intelligence and machine-learning algorithms by federal agencies; and propose appropriate safeguards;*
4) *Monitor proposals for "smart" borders and assess privacy impacts on U.S. residents; and*
5) *Reform of Section 702 authority.*

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC has a particular interest in the status of the PCLOB. EPIC testified before the 9-11 Commission to urge the creation of an independent privacy agency after 9-11 to ensure appropriate oversight of the new surveillance powers that would be established by Congress.[3] EPIC also set out several priorities for PCLOB as the agency was shaping its agenda.[4] EPIC spoke at the first meeting of the PCLOB in 2013.[5] And EPIC has provided

[1] *Countering Terrorism while Protecting Privacy and Civil Liberties: Where do We Stand in 2019*, Privacy and Civil Liberties Oversight Board (Feb. 8, 2019), https://www.pclob.gov/newsroom/20190130.html.
[2] *See* About EPIC, EPIC.org, https://epic.org/epic/about.html.
[3] Marc Rotenberg, *Testimony, Security and Liberty: Protecting Privacy, Preventing Terrorism*, National Commission on Terrorist Attacks Upon the United States (Dec. 8, 2003), https://epic.org/privacy/terrorism/911commtest.pdf; *See also* Rotenberg, Marc, *The Sui Generis Privacy Agency: How the U.S. Institutionalized Privacy Oversight after 9-11* (September 28, 2006), https://ssrn.com/abstract=933690.
[4] EPIC Statement to PCLOB, *Sunshine Act; Notice of Meeting* (Oct. 23, 2012), https://epic.org/privacy/1974act/EPIC-PCLOB-Statement-10-12.pdf.
[5] Marc Rotenberg, *Workshop on Domestic Surveillance Programs Operated Under the USA PATRIOT Act and the Foreign Intelligence Surveillance Act*, Privacy and Civil Liberties Oversight Board (July 9, 2013), https://epic.org/privacy/oversight/EPIC-PCLOB-Statement.pdf

extensive comments to the Board on EO 12333, FOIA procedures, and "defining privacy," among other topics.[6]

EPIC has long argued that a full-strength, independent PCLOB is necessary for effective oversight of government surveillance programs. As the PLCOB will now be fully reconstituted, EPIC recommends that the Board prioritize the following issues:.

1) The PCLOB should release the Board's report on Executive Order 12333.

In November 2013 the PCLOB launched a broad examination of the intelligence activities conducted under E.O. 12333 (EO 12333) and their implications for privacy and civil liberties. The Board received briefings on EO 12333 activities from each agency within the Intelligence Community. The PCLOB also convened several meetings, including with representatives of NGOs, to discuss the review of EO 12333.

According to the PCLOB's initial work plan, submitted in April 2015, the Board planned to do an in-depth review of two counterterrorism-related activities conducted under E.O. 12333 that implicated the direct and incidental collection and use of U.S. person information.[7] The review was to culminate in written reports by the end of 2015 that included recommendations as needed to better protect privacy and civil liberties.[8] Although the reports were anticipated to be highly classified, the Board planned to release a high-level public version of the report.[9]

The PCLOB announced in the summer of 2016 that the deadline for the public report would be pushed back to the end of 2016.[10] To date the report has not been released to the public. Documents released by the PCLOB in December 2016 revealed that the complete report is now in the possession of the agency. According to emails sent from the Board to Congressional staff, the board intended to publish a report by the end of 2016.[11] A spokeswoman for PCLOB confirmed that

---

[6] Comments of the Electronic Privacy Information Center to the Privacy and Civil Liberties Oversight Board, *Request for Public Comment on Activities Under Executive Order 12333* (June 16, 2015), https://epic.org/privacy/surveillance/12333/EPIC-12333-PCLOB-Comments-FINAL.pdf; Jeramie D. Scott, Nat'l Sec. Counsel, EPIC, *Prepared Statement for the Record Before the Privacy and Civil Liberties Oversight Board* (Jul. 23, 2014), https://epic.org/news/privacy/surveillance_1/EPIC-Statement-PCLOB-Review-12333.pdf; Comments of the Electronic Privacy Information Center to the Privacy and Civil Liberties Oversight Board, *Freedom of Information, Privacy Act, and Government in the Sunshine Act Procedures* (July 15, 2013), https://epic.org/open_gov/EPIC-PCLOB-FOIA.pdf; Letter from Marc Rotenberg, EPIC President, Khaliah Barnes, EPIC Administrative Counsel, EPIC to PCLOB on "Defining Privacy," at 4 (Nov. 11, 2014), *available at* https://epic.org/open_gov/EPIC-Ltr- PCLOB-Defining-Privacy-Nov-11.pdf.
[7] Privacy and Civil Liberties Oversight Bd., *PCLOB Examination of E.O. 12333* (Apr. 8, 2015), https://www.pclob.gov/library/20150408-EO12333_Project_Description.pdf.
[8] *Id.*
[9] *Id.*
[10] Privacy and Civil Liberties Oversight Bd., *Semi-Annual Report: October 2015-March 2016* (2016), *https://www.pclob.gov/library/Semi_Annual_Report_August_2016.pdf.*
[11] Jenna McLaughlin, *The U.S. Government's Privacy Watchdog Is Basically Dead, Emails Reveal*, The Intercept, (Mar. 3 2017), https://theintercept.com/2017/03/03/the-governments-privacy-watchdog-is-basically-dead-emails-reveal/.

the agency still plans to release its analysis, despite the stepping down of Chairman Medine, but to date the agency has not released the report.[12]

Now that PCLOB once again has a quorum, it is imperative that the Board release the EO 12333 report immediately.

2) The PCLOB should review the use of facial recognition technology by federal agencies and propose appropriate safeguards

New privacy risks have arisen with the deployment of facial recognition technology by CBP at U.S. airports. Through the implementation of the Biometric Entry/Exit program, CBP is expanding the agency's use of facial recognition at ports of entry. CBP has already implemented facial recognition at numerous airports and is seeking to expand the use of the technology at land and sea ports. Indeed, CBP is testing the capability of conducting facial recognition through windshields as automobiles drive up to the border.[13]

Facial recognition poses significant threats to privacy and civil liberties. Facial recognition techniques can be deployed covertly, remotely, and on a mass scale. Additionally, there is a lack of well-defined federal regulations controlling the collection, use, dissemination, and retention of biometric identifiers. Ubiquitous identification by government agencies eliminates the individual's ability to control the disclosure of their identities, creates new opportunities for tracking and monitoring, and poses a specific risk to the First Amendment rights of free association and free expression.

It is imperative the PCLOB review the use of facial recognition technology and its impact of privacy and civil liberties.

3) The PCLOB should review the use of artificial intelligence and machine-learning algorithms by federal agencies and propose appropriate safeguards

The Department of Homeland Security ("DHS") published a white paper outlining the potential use of AI techniques, including for border enforcement. DHS proposed the development of predictive systems to assess future risk. A similar proposal a few years ago – The Future Attribute Screening Technology ("FAST") – was developed to detect "malintent." The program collapsed after it became clear the system would not work.[14] DHS also proposed to use social media analytics to predict human behavior to counter violent extremism.[15]

Artificial intelligence and machine-learning algorithms present numerous privacy and civil liberties issues. Algorithms require large amounts of data, and DHS ignores the requirements of the

---

[12] Julian Hattem, *Surprise Resignation Threatens to Hobble Privacy Watchdog*, TheHill (Apr. 8, 2016), https://thehill.com/policy/national-security/275545-surprise-vacancy-threatens-privacy-watchdog.
[13] *See* Agency Information Collection Activities: Biometric Identity, 83 Fed. Reg. 24326 May 25, 2018.
[14] DHS, *Future Attribute Screening Technology Fact Sheet*, https://www.dhs.gov/publication/future-attribute-screening-technology; Alexander Furnas, *Homeland Security's 'Pre-Crime' Screening Will Never Work*, The Atlantic (Apr. 17, 2012), https://www.theatlantic.com/technology/archive/2012/04/homeland-securitys-pre-crime-screening-will-never-work/255971/; *See*, EPIC v. DHS - FAST Program, https://epic.org/foia/dhs/fast/.
[15] Immigration and Customs Enforcement, *Extreme Vetting Initiative: Statement of Objectives*, https://www.fbo.gov/utils/view?id=533b20bf028d2289633d786dc45822f1.

Privacy Act in order to use personal data with algorithms. Additionally, algorithms end up being black boxes that not only lack transparency but accountability too.

The PCLOB should review the use of AI and machine-learning algorithms to assess the privacy and civil liberties implications of these new technologies. Efforts should be made to ensure that federal agencies comply with the Universal Guidelines for Artificial Intelligence.[16]

4) The PCLOB should monitor proposals for "smart" borders and assess privacy impacts on U.S. residents

There are several proposals now before Congress to establish so-called "small borders." In fact, these systems entail the deployments of mass surveillance techniques, including aerial drones, biometric identification, and x-ray scanning of vehicles, that impact the privacy rights of American residents and Americans travelling across the border.

The PCLOB should be prepared to assess these programs deployed by federal agencies and to propose necessary safeguards or, if required, to terminate "smart border" programs that fail to protect the privacy of Americans.

5) The PCLOB should carefully review and report on reforms to Section 702 authority

Last year, as the result of a Freedom of Information Act lawsuit,[17] EPIC obtained a report containing important information about the FBI's current use of Section 702 authority. The lawsuit challenged the failure of the Department of Justice National Security Division ("NSD") to disclose non-exempt records, in the agency's possession, for reports regarding the Federal Bureau of Investigation ("FBI") queries of data concerning U.S. persons for routine criminal investigations, under Section 702 of the Foreign Intelligence Surveillance Act. The report in question was mandated by the Foreign Intelligence Surveillance Court ("FISC") due to concerns about the possible misuse of Section 702 authority by the FBI. It gives an account of failure by an FBI analyst to follow internal guidance.

Under the DOJ's existing policy, federal agents can search communications collected under Section 702 for information about Americans, even when this information *could not lawfully be targeted* at the front end. Section 702 was enacted to authorize certain electronic surveillance of foreign communications without probable cause. Section 702 requires that the target of an investigation is a non-U.S. person located outside the U.S. However, the FBI's searches these communications, obtained under Section 702, for private information about Americans.

The report required by the FISC, sought by EPIC, arose because of concerns about the possible misuse of Section 702 authority by the FBI. The FISC required production of a report "concerning each instance after December 4, 2015, in which FBI personnel receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information."[18]

---

[16] Universal Guidelines for Artificial Intelligence, https://thepublicvoice.org/ai-universal-guidelines/.
[17] EPIC v. NSD, https://epic.org/foia/nsd/702-query-report/.
[18] *Memorandum Opinion and Order,* [docket no. redacted], slip op. at 78 (FISC Nov. 6, 2015), https://www.dni.gov/files/documents/20151106- 702Mem_Opinion_Order_for_Public_Release.pdf.

The report pertains to only a small subset of backdoor searches: those conducted by the FBI of raw data for routine criminal investigations. Agencies other than the FBI also conduct Section 702 searches. Searches are conducted for non-foreign intelligence purposes under Section 702 that are not for routine criminal investigations. And many backdoor searches are for metadata and minimized data.

The report shows that the FBI analyst failed to follow internal guidance to notify superiors of the search. Footnote two of the report states:

> As part of this process, FBI sent out guidance to its personnel that if they receive and review the results of queries of raw Section 702-acquired information that is identified as concerning a known or presumed United States person in response to a query that is not designed to find and extract foreign intelligence information, they must notify their Chief Division Counsel and the National Security Law Branch of the query and results to determine if it needs to be reported to NSD and the Court. This process was not followed in this instance.

This failure to follow internal guidance raises questions about whether the FBI is accurately recording backdoor searches. It could be indicative of a systemic reporting problem within the agency. The DNI's annual statistical transparency reports may not be reliable if agencies are failing to report searches.[19]

It is imperative that the American public, the PCLOB, and members of Congress consider this report of the FBI's use of Section 702. We urge the PCLOB to recommend that any reform proposal include a full fix of the backdoor search loophole requiring all agencies to obtain a warrant based on probable cause to search Section 702 data for information about U.S. citizens and residents in all investigations.

Reforms must also be made on the provisions of Section 702 that authorize data collection on non-U.S. persons. In 2017, EPIC made submissions to the Irish High Court in the case *Data Protection Commissioner v. Facebook*, a case concerning privacy protections for transatlantic data transfers.[20] The *DPC v. Facebook* case follows a landmark decision of the European Court of Justice which found that there were insufficient legal protections for the transfer of European consumer data to the United States, largely due to the surveillance authority granted to the U.S. government under Section 702.[21] Mr. Schrems, an Austrian privacy advocate who brought the original case, has again challenged Facebook's business practices.[22] The Irish High Court found that there are "well-founded concerns that there is an absence of an effective legal remedy in U.S. law" and referred the matter to the European Court of Justice.[23] Other similar suits have been brought in the EU challenging the Privacy Shield agreement. Section 702 is the central focus of all of these legal challenges.

---

[19] Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities*, https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016.

[20] Amended Outline Submissions of Behalf of the Amicus Curiae (EPIC), *Data Protection Comm'r v. Facebook,* 2016/4809 P*, available at* https://epic.org/privacy/intl/schrems/02272017-EPIC-Amended-Submissions.pdf.

[21] Judgment of Oct. 6, 2015, *Schrems v. Data Protection Comm'r,* Case C-362/14, EU:C:2015:650, *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN.

[22] *Data Protection Comm'r v. Facebook,* 2016/4809 P (H. Ct.) (Ir.)

[23] *Id.*

Section 702 authorizes bulk surveillance on the communications of non-U.S. persons, including EU citizens, by the U.S. government. Without reforms by Congress, Privacy Shield and other transatlantic data transfer mechanisms could very well be invalidated by the European Court of Justice.

EPIC looks forward to working with the Board on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Jeramie Scott*
Jeramie Scott
EPIC Senior Counsel

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