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 4, 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 upcoming hearing on the nominations of Aditya Bamzai and Travis LeBlanc to be members of the Privacy and Civil Liberties Oversight Board ("PCLOB" or "Board").[1] Although EPIC takes no position for or against the nominees, this hearing provides a critical opportunity to set out priorities for PCLOB in 2019. The PCLOB plays a vital role safeguarding the privacy rights of Americans and ensuring oversight and accountability of the Intelligence community.

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] And EPIC spoke at the first meeting of the PCLOB in 2013.[5] And EPIC has provided extensive comments to the Board on EO 12333, FOIA procedures, and "defining privacy," among other topics.[6]

---

[1] *Nominations*, 116th Cong. (2019), S. Comm. On Judiciary, (Feb. 5, 2019), https://www.judiciary.senate.gov/meetings/02/05/2019/nominations.

[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 United States Institutionalized Privacy Oversight after 9-11* (September 28, 2006). Available at SSRN: https://ssrn.com/abstract=933690 or http://dx.doi.org/10.2139/ssrn.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

[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

The PCLOB was established because the 9-11 Commission found that "there is no office within the government whose job it is to look across the government at the actions we are taking to protect ourselves to ensure that liberty concerns are appropriately considered."[7] The PCLOB has two core responsibilities: oversight and advice.[8] In its oversight role, PCLOB is expected to review executive branch actions and information disclosure policies. In its advisory role, PCLOB is expected to counsel the President and executive branch agencies on the privacy and civil liberties implications of their proposed policies. PCLOB reports twice a year to the President and Congress, and makes these reports available to the public. These responsibilities are vital checks on the intelligence community.

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 Civil Liberties 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.[9] 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.[10] Although the reports were anticipated to be highly classified, the Board planned to release a high-level public version of the report.[11]

The PCLOB announced in the summer of 2016 that the deadline for the public report would be pushed back to the end of 2016.[12] 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.[13] A spokeswoman for PCLOB confirmed that

---

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] *See* About PCLOB, https://www.pclob.gov/about/.
[8] PCLOB, *History and Mission*, https://www.pclob.gov/about/.
[9] 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.
[10] *Id.*
[11] *Id.*
[12] 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.*
[13] 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.[14]

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.[15]

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.[16] DHS also proposed to use social media analytics to predict human behavior to counter violent extremism.[17]

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

---

[14] 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.

[15] *See* Agency Information Collection Activities: Biometric Identity, 83 Fed. Reg. 24326 May 25, 2018.

[16] 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/.

[17] 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.[18]

4) Monitor Proposals for "Smart" Borders and Assess Privacy Impacts on US 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.

We ask that this letter be entered in the hearing record.

EPIC looks forward to working with the Committee 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

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

---

[18] Universal Guidelines for Artificial Intelligence, https://thepublicvoice.org/ai-universal-guidelines/.