epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

November 11, 2014

Chairman David Medine
Rachel L. Brand, Board Member
Elisebeth Collins Cook, Board Member
James X. Dempsey, Board Member
Judge Patricia M. Wald, Board Member
Privacy and Civil Liberties Oversight Board
2100 K Street, NW, Suite 500
Washington, DC 20427

Re: Notice PCLOB 2014-05; "Defining Privacy"

Dear Chairman Medine and Members of the Privacy and Civil Liberties Oversight Board:

As the Privacy and Civil Liberties Oversight Board prepares for its public meeting on "Defining Privacy," EPIC urges the Board to prioritize Privacy Act enforcement. The Privacy Act provides a sound framework for privacy protection in the United States. Government agencies within the PCLOB's purview contravene the Privacy Act's intent and pose substantial privacy risks by claiming broad exemptions from coverage under the Act. The Board must improve agency accountability by auditing programs for Privacy Act compliance and recommending expanded authorities under the Privacy Act.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving privacy safeguards established in the Privacy Act of 1974.[1] EPIC has made numerous recommendations to Congress and federal agencies on the need to strengthen Privacy Act protections.[2] EPIC has also twice filed amicus briefs

[1] *See, e.g., The Privacy Act of 1974*, EPIC, https://epic.org/privacy/1974act/; *FAA v. Cooper*, EPIC, https://epic.org/amicus/cooper/; *Doe v. Chao*, EPIC, https://www.epic.org/privacy/chao/.

[2] *See, e.g.*, EPIC et al., *Comments Urging the Department of Homeland Security To (A) Suspend the "Automated Targeting System" As Applied To Individuals, Or In the Alternative, (B) Fully Apply All Privacy Act Safeguards To Any Person Subject To the Automated Targeting System* (Dec. 4, 2006), *available at* http://epic.org/privacy/pdf/ats_comments.pdf; EPIC, *Comments on Automated Targeting System Notice of Privacy Act System of Records and Notice of Proposed Rulemaking, Docket Nos. DHS-2007-0042 AND DHS-2007-0043* (Sept. 5, 2007), *available at* http://epic.org/privacy/travel/ats/epic_090507.pdf. *See also*, EPIC et al., *Comments on the Terrorist Screening Database System of Records, Notice of Privacy Act System of Records and Notice of Proposed rulemaking, Docket Nos. DHS 2011-0060 and DHS 2011-0061* (Aug. 5, 2011), *available at* http://epic.org/privacy/airtravel/Comments_on_DHS-2011-0060_and_0061FINAL.pdf; EPIC, *Comments on Secure Flight, Docket Nos. TSA-2007-28972, 2007-28572* (Sept. 24, 2007), *available at*

in the Supreme Court concerning the Privacy Act.[3] EPIC recently provided expert commentary at a Georgetown Law Center conference celebrating the Privacy Act.[4]

In 2012, following the PCLOB's request for public comments, EPIC recommended that the Board determine whether certain DHS programs, including fusion centers, the Information Sharing Environment, and the Suspicious Activity Reporting Initiative, comply with the Privacy Act.[5]

The Privacy Act is one of the earliest U.S. laws to define privacy. The Act is based on the U.S. Department of Health, Education & Welfare's 1973 report on "Records, Computers, and the Rights of Citizens" (the "HEW" Report) findings and recommendations. The Report was issued by the HEW Secretary's Advisory Committee on Automated Personal Data Systems, which was established "in response to growing concern about the harmful consequences that may result from uncontrolled application of computer and telecommunications technology to the collection, storage, and use of data about individual citizens."[6] The Committee found that because of the "widespread belief that personal privacy is essential to our well-being—physically, psychologically, socially, and morally," it was necessary to safeguard personal privacy.[7] Further, to effectively safeguard personal privacy in an automated world, those keeping records must adhere to "certain fundamental principles of fair information practice[s]":

- There must be no personal-data record-keeping systems whose very existences is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.

---

http://epic.org/privacy/airtravel/sf_092407.pdf. *See also* Letter from Marc Rotenberg and Khaliah Barnes, EPIC, to Senator Daniel Akaka, Chairman, Subcomm. on Oversight of Gov't Mgmt., the Fed. Workforce, and the District of Columbia (Mar. 27, 2012), *available at* https://epic.org/privacy/1974act/EPIC-on-S-1732-Privacy-Act-Modernization.pdf; Letter from Marc Rotenberg and Khaliah Barnes, EPIC, to Senator Daniel Akaka, Chairman, Subcomm. on Oversight of Gov't Mgmt., the Fed. Workforce, and the District of Columbia (May 14, 2012), *available at* https://epic.org/privacy/1974act/EPIC-Supp-S1732-Priv-Act-Modernization.pdf.

[3] Brief for Electronic Privacy Information Center et al. as Amicus Curiae Supporting Petitioner, Buck Doe v. Elaine L. Chao, Secretary of Labor, 540 U.S. 614 (2004) (No. 02-1377), *available at* https://epic.org/privacy/chao/Doe_amicus.pdf; Brief for Electronic Privacy Information Center as Amicus Curiae Supporting Respondent, Federal Aviation Administration v. Stanmore Cawthon Cooper, 132 S. Ct. 1441 (2012) (No. 10-1024), *available at* https://epic.org/amicus/cooper/Cooper-EPIC-Brief.pdf.

[4] GEORGETOWN UNIV. LAW CTR. CTR. ON PRIVACY AND TECH., *The Privacy Act @40* (Oct. 30, 2014), http://www.law.georgetown.edu/academics/centers-institutes/privacy-technology/events/index.cfm.

[5] Comments of EPIC to the Privacy and Civil Liberties Oversight Bd. on Sunshine Act; Notice of Meeting (Oct. 23, 2012) (PCLOB-2012-01; Docket No. 2012-0013; Sequence No.1), *available at* http://epic.org/privacy/1974act/EPIC-PCLOB-Statement-10-12.pdf.

[6] U.S. DEP'T. OF HEALTH, EDUC. AND WELFARE, SEC'Y'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS ix (1973).

[7] *Id*. at 33.

- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[8]

Congress codified the Committee's Fair Information Practices recommendations with the Privacy Act. With the Privacy Act, Congress sought to

> "(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;
> "(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;
> "(3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;
> "(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;
> "(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and
> "(6) be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act."[9]

In this way, the Privacy Act has provided a baseline framework for other privacy laws that incorporate fair information practices.[10]

Congress enacted the Privacy Act with the understanding that secret databases threatened individual liberties and freedom.[11] Through the wholesale collection of sensitive information, government agencies could covertly make decisions about individuals, while denying due process rights such as information access and correction.[12]

---

[8] *Id*. at 41.
[9] The Privacy Act of 1974, Pub. L. 93–579, § 2, 88 Stat. 1896 (Dec. 31, 1974).
[10] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*.; Health Insurance Portability and Accountability Act Privacy Rule, 45 C.F.R. Pts. 160 and 164; Consumer Privacy Bill of Rights.
[11] *Supra* note 9, at § 2 (a) (Congressional findings that "the increasing use of computers and sophisticated information technology . . . has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information" and "the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems . . .").
[12] TECH. AND PRIVACY ADVISORY COMM., DEP'T OF DEF., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 36 (Mar. 2004) ("Data aggregation creates the risk that the resulting profile provides the government with substitutes for information it is otherwise not allowed to access or act upon. Similarly, the ability to aggregate records held by third parties may provide the government with precisely the same

Much has happened since 9-11 that is clearly contrary to the purposes of Privacy Act and the expectation of many Americans who rightly believe that the US government would not develop massive databases to secretly profile Americans.

Government agencies within the Board's purview, like the DHS and NSA, routinely collect personal records without granting individuals basic Privacy Act protections, like access, amendment, and notification rights.[13] The Board's first public solicitation of comments in 2006 prioritized the privacy and civil liberties implications arising from one of the largest government national security databases—the Terrorist Screening Database.[14]

As the Board crafts its privacy agenda, we urge you to prioritize Privacy Act compliance and enforcement of the Terrorist Screening Database and other government databases within the Board's jurisdiction. In the United States, the Privacy Act defines the right to privacy with regard to the collection and use of personal information by federal agencies. It is your responsibility to see that the Act is enforced.

Respectfully Submitted,

Marc Rotenberg
EPIC Executive Director

Khaliah Barnes
EPIC Administrative Law Counsel

Electronic Privacy Information Center
1718 Connecticut Avenue, NW
Suite 200
Washington, D.C. 20009
(202) 483 – 1140

information it previously would have been required to obtain a warrant to access.").

[13]*See, e.g.*, EPIC et al., *Comments on the Terrorist Screening Database System of Records, Notice of Privacy Act System of Records and Notice of Proposed rulemaking, Docket Nos. DHS 2011-0060 and DHS 2011-0061* (Aug. 5, 2011), *available at* http://epic.org/privacy/airtravel/Comments_on_DHS-2011-0060_and_0061FINAL.pdf; EPIC et al., *Comments on the DoD Privacy Program, 32 C.F.R. Part 310, Docket ID: DOD-2013-OS-0023, RIN 0790-AJ03* (Oct. 21, 2013), *available at* https://epic.org/privacy/nsa/Coal-DoD-Priv-Program-Cmts.pdf.

[14]Privacy and Civil Liberties Oversight Bd. Watch List Redress Request for Public Comment, 71 Fed. Reg. 75,752 (Dec. 18, 2006).