

STATEMENT OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

“Sunshine Act; Notice of Meeting”

[Notice-PCLOB-2012-01; Docket No. 2012-0013; Sequence No.1]

October 23, 2012

By notice published on October 23, 2012—a week before the Privacy and Civil Liberties Oversight Board (“PCLOB”) meeting to receive public comments, and a mere three days before written statements were due to the agency—PCLOB announced that it will hold its “first public meeting for the purpose of receiving the public’s input on its forthcoming agenda.”¹ Pursuant to this notice, the Electronic Privacy Information Center (“EPIC”) recommends that the PCLOB focus on the following: (1) suspension of the Fusion Center Program; (2) limiting closed-circuit television surveillances; (3) eliminating the use of body scanners; (4) establishing privacy regulations for drones; (5) improving Information Sharing Environment (ISE) and Suspicious Activity Reporting (SARS) Standards; and (6) Privacy Act adherence.

EPIC also requests that EPIC National Security Fellow Jeramie D. Scott be invited to briefly address the PCLOB on these issues on Tuesday, October 30, 2012.

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 constitutional values and the rule of law. EPIC has a particular interest in preserving privacy safeguards

¹ Sunshine Act; Notice of Meeting, 77 Fed. Reg. 64835 (Oct. 23, 2012).

established by Congress and ensuring that new information systems and surveillance programs developed and operated by the federal government comply with all applicable laws.²

EPIC's comments to the PCLOB focus on the need to improve oversight of the Department of Homeland Security ("DHS"). No federal agency has spent more money developing systems of surveillance directed toward the American public than the Department of Homeland Security. It is time for that to change.

EPIC Recommendations to PCLOB

1) Investigation of Fusion Center Program

Fusion Centers bring together information from distributed sources for the purpose of collection, retention, analysis, and dissemination of intelligence. Fusion Centers lack proper oversight and training. The data gathered by Fusion Centers is of questionable quality, potentially violates the Privacy Act, and does not contribute to the counterterrorism efforts of the federal government; furthermore, the funds used for the Fusion Center program are not being properly tracked.³

Pursuant to the Board's statutory authority,⁴ EPIC recommends the review of fusion center's quality of intelligence collected and distributed and whether the Fusion Center program is justified in light of its lack of contribution to counterterrorism efforts.

² See, e.g., EPIC: Information Fusion Centers and Privacy, <http://epic.org/privacy/fusion/>; EPIC: Whole Body Imaging Technology and Body Scanners ("Backscatter" X-Ray and Millimeter Wave Screening), <http://epic.org/privacy/airtravel/backscatter/>; EPIC: Suspicious Activity Reporting, <http://epic.org/privacy/suspicious-activity-reporting/default.html>; EPIC: Video Surveillance, <http://epic.org/privacy/surveillance/>; EPIC: Unmanned Aerial Vehicles (UAVs) and Drones, <http://epic.org/privacy/drones/>; EPIC: The Privacy Act of 1974, <http://epic.org/privacy/drones/>.

³ STAFF OF SENATE COMM. ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS: PERMANENT SUBCOMM. ON INVESTIGATION, 112TH CONG., FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS (Oct. 3, 2012) [hereinafter "Senate Fusion Center Report"].

⁴ Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 801(d)(2), 121 Stat. 266, 353 (2007).

EPIC believes the Fusion Center program should be suspended until adequate training is instituted and specific oversight procedures to prevent future privacy violations are installed. Additionally, any future funding of Fusion Center should be conditioned on meeting the training requirements and oversight procedures.

2) Limiting Closed-Circuit Television (CCTV) Surveillance⁵

DHS has spent hundreds of millions of dollars in grants for the creation and maintenance of camera surveillance systems.⁶ CCTV's ability to prevent crime is overstated and their use impinge upon free speech and free association.⁷ The DHS has supported the deployment of these systems of surveillance even when the communities impacted have not requested them and there is a substantial risk that these cameras already in place will be "upgraded" to incorporate facial recognition technology that will make possible the real time tracking of individuals in public spaces.

Pursuant to the Board's statutory authority,⁸ EPIC recommends the review of any CCTV surveillance used by DHS for any impingement on free speech and free association. EPIC believes any expansion of the CCTV system should cease and the current CCTV system should be subject to strong regulations, oversight, and penalties to prevent abuses and protect the public's privacy and civil rights.⁹

3) Eliminating the Use of Body Scanners

⁵ EPIC, *Comments to the Dept. of Homeland Security*, (Jan. 15, 2008) [hereinafter "EPIC Comments to DHS"], available at http://epic.org/privacy/surveillance/epic_cctv_011508.pdf.

⁶ Email from Toby Levin, Senior Advisor, DHS Privacy Office, to Melissa Ngo, Senior Counsel, EPIC, Nov. 28, 2007 (on file with EPIC).

⁷ See Statement of Lillie Coney, EPIC Associate Director, to the Dept. of Homeland Security Data Privacy and Integrity Advisory Committee (June 7, 2006), <http://epic.org/privacy/surveillance/coneytest060706.pdf>

⁸ Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 801(d)(2), 121 Stat. 266, 353 (2007).

⁹ See EPIC Comments to DHS (providing a privacy and civil liberty protective framework for the use of CCTV).

The DHS has already begun to remove the x-ray body scanners from major US airports. This process should be accelerated and further funding should be suspended. These devices are invasive, ineffective, unconstitutional, and pose a threat to the health of US air travelers.¹⁰ DHS prepared an inadequate Privacy Impact Assessment of the TSA's body scanner test program that failed to identify numerous privacy risks to air travelers.¹¹ The effectiveness of body scanners is questionable and there are less intrusive methods that better protect personal privacy.¹² Nonetheless, the agency seems set on deploying these systems more widely.

Pursuant to the Board's statutory authority,¹³ EPIC recommends that the PLCOB investigate the body scanner program, and other similar systems, including the "Future Attribute Scanning Technology" that are directed toward the public at large..

4) Privacy Regulation for Drones

The use of domestic drones is rising and estimates put the number of drones in use within the next decade at 30,000.¹⁴ Drones are an extremely evasive technology; they can fly at heights that make them unnoticeable and can be equipped with high definition cameras, infra-red sensors, license plate readers, motion detection sensors, etc.¹⁵

¹⁰ See EPIC: Whole Body Imaging Technology and Body Scanners ("Backscatter" X-Ray and Millimeter Wave Screening), <http://epic.org/privacy/airtravel/backscatter/>.

¹¹ Petition to Suspend Body Scanner Program, http://epic.org/privacy/airtravel/backscatter/petition_042110.pdf

¹² *Id.*

¹³ Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 801(d)(2), 121 Stat. 266, 353 (2007).

¹⁴ Lynn Herman, *30,000 Drones in American Skies, Civil Liberties in Jeopardy*, Digital Journal (Feb. 13, 2012), <http://digitaljournal.com/article/319564>.

¹⁵ Customs and Border Protection Today, Unmanned Aerial Vehicles Support Border Security (July/Aug. 2004), available at http://www.cbp.gov/xp/CustomsToday/2004/Aug/other/aerial_vehicles.xml.

Pursuant to the Board's statutory authority,¹⁶ EPIC recommends a review of the ways in which drones operated by the US government violate the privacy of Americans. EPIC believes strong regulation should be implemented for the domestic use of drones.¹⁷

5) Improving Information Sharing Environment (ISE) and Suspicious Activity

Reporting (SARS) Standards

Since 9/11 there has been an emphasis on increased sharing of terrorism information with Federal, State, local, and tribal entities and the Information Sharing Environment was created. There has also been a greater emphasis on reporting suspicious activity that might be terrorism-related and Suspicious Activity Reporting was implemented.

Pursuant to the Board's statutory authority, EPIC recommends the investigation into the ISE and SARS program, particularly the quality of information that is reported and shared and whether the relevant databases associated with the program are in compliance with the Privacy Act and other "governing laws, regulations, and policies regarding privacy and civil liberties."¹⁸ EPIC believes any suspicious reporting should, at minimal, meet the reasonable suspicion standard and all information evaluated for reliability prior to sharing via the ISE.

¹⁶ Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 801(d)(2), 121 Stat. 266, 353 (2007).

¹⁷ See Petition from EPIC, *et al.*, to Michael P. Huerta, Acting Administrator, FAA (Feb. 24, 2012), available at <http://epic.org/privacy/drones/FAA-553e-Petition-v-1.0.pdf>; see also EPIC Testimony, *Hearing on "Using Unmanned Aerial Systems Within the Homeland: Security Game Changer?"*, available at <http://epic.org/privacy/testimony/EPIC-Drone-Testimony-7-12.pdf> [edit footnote].

¹⁸ Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 801(d)(2), 121 Stat. 266, 353 (2007).

6) Promote Privacy Act Adherence

The Privacy Act was passed in 1974 in response to concerns about the creation and use of computerized databases might impact individuals' privacy rights. Many of the DHS programs mentioned above create computerized databases on individual U.S. citizens.

Pursuant to the Board's statutory authority,¹⁹ EPIC recommends the review of all the above programs for its compliance the Privacy Act of 1974. EPIC believes the broad exemptions DHS claims under the Privacy Act go against the intention of the Act and should be eliminated.

Conclusion

For the foregoing reasons, EPIC strongly recommends that PCLOB focus on the agenda items listed above to ensure the domestic surveillance of DHS is inline with the Constitution, Privacy Act, and other applicable laws and statutes. Furthermore, to fully encourage public input on the PCLOB's agenda and activities, the agency should publish future meeting notices no later than thirty days before the meeting takes place.

EPIC reserves the right to submit additional comments.

Respectfully submitted,

Marc Rotenberg
EPIC Executive Director

Jeramie D. Scott
EPIC National Security Fellow

Khaliah Barnes
EPIC Open Government Counsel

¹⁹ *Id.*

Resources

EPIC: Spotlight on Surveillance: “National Network” of Fusion Centers Raises Specter of COINTELPRO, <http://epic.org/privacy/surveillance/spotlight/0607/>

Statement of Lillie Coney, EPIC Associate Director, to the Department of Homeland Security Data Privacy and Integrity Advisory Committee (Sept. 19, 2007), *available at* <http://www.epic.org/privacy/fusion/fusion-dhs.pdf>

Letter from Marc Rotenberg, EPIC Executive Director and John Verdi, EPIC Staff Counsel to Senate Committee on Homeland Security and Governmental Affairs and the Senate Subcommittee on State, Local, and Private Sector Preparedness and Integration (Apr. 17, 2008), *available at* http://www.epic.org/privacy/fusion/EPIC_ltr_Sen_Fusion_Ctrs.pdf

Press Release, EPIC, EPIC Obtains Documents Revealing Federal Role in State Fusion Center Secrecy (Apr. 11, 2008), *available at* <http://epic.org/press/041108.html>

EPIC: Spotlight on Surveillance: D.C.'s Camera System Should Focus on Emergencies, Not Daily Life, <http://epic.org/privacy/surveillance/spotlight/1205/default.html>

Petition from EPIC et al., to Michael P. Huerta, Acting Administrator, Federal Aviation Administration (Feb. 24, 2012), *available at* <http://epic.org/privacy/drones/FAA-553e-Petition-v-1.1.pdf>

Testimony and Statement for the Record Amie Stepanovich, EPIC Associate Litigation Counsel, Hearing on "Using Unmanned Aerial Systems Within the Homeland: Security Game Changer?" (July 19, 2012), *available at* <http://epic.org/privacy/testimony/EPIC-Drone-Testimony-7-12.pdf>

EPIC, Comments on the Automated Targeting System Notice of Privacy Act System of Records and Privacy Act Exemptions (June 21, 2012), *available at* <http://epic.org/apa/comments/EPIC-ATS-Comments-2012.pdf>

Br. *Amicus Curiae* of Electronic Privacy Information Center (EPIC), *Herring v. United States*, 555 U.S. 135 (2009), *available at* http://epic.org/privacy/herring/07-513tsac_epic.pdf

Whole Body Imaging Technology and Body Scanners, **EPIC**, <http://epic.org/privacy/airtravel/backscatter/>

EPIC v. DHS (Suspension of Body Scanner Program), **EPIC**, http://epic.org/privacy/body_scanners/epic_v_dhs_suspension_of_body.html

EPIC v. DHS (Mobile Body Scanners), **EPIC**, http://epic.org/privacy/body_scanners/mobile_body_scanners/default.html