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

July 24, 2017

The Honorable Martha McSally, Chairwoman
The Honorable Filemon Vela, Ranking Member
U.S. House Committee on Homeland Security
Subcommittee on Border and Maritime Security
H2-176 Ford House Office Building
Washington, DC 20515

Dear Chairwoman McSally and Ranking Member Vela:

We write to you regarding the upcoming hearing on "Deter, Detect And Interdict: Technology's Role in Securing the Border."[1] EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues and manages one of the most extensive open government litigation programs in the United States.[2] EPIC is focused on the protection of individual privacy rights, and we are particularly interested in the privacy problems associated with surveillance.[3]

Last week, EPIC filed a FOIA lawsuit against Customs and Border Protection (CBP) for information about the agency's deployment of a massive biometric surveillance program to track travelers as they enter and leave the United States.[4] EPIC had filed three Freedom of Information ("FOIA") requests in the past year regarding the CBP's implementation of the biometric entry-exit tracking system. The CBP had failed to respond to any of EPIC's FOIA requests.

---

[1] *Deter, Detect And Interdict: Technology's Role in Securing the Border*, 115th Cong. (2017), H. Comm. on Homeland Security, Subcomm. on Border and Maritime Security, https://homeland.house.gov/hearing/deter-detect-interdict-technologys-role-securing-border/ (July 25, 2017).

[2] *See About EPIC*, EPIC.org, https://epic.org/epic/about.html; *EPIC FOIA Cases*, EPIC, https://epic.org/foia/; Marc Rotenberg *et al*, *The Open Government Clinic: Teaching the Basics of Lawyering*, 48 IND. L. REV. 149 (2014); EPIC, *Litigation Under the Federal Open Government Laws 2010* (2010).

[3] EPIC, *EPIC Domestic Surveillance Project,* https://epic.org/privacy/surveillance/, Statement of EPIC, "*Unmanned Aircraft Systems: Innovation, Successes, and Challenges,*" Hearing Before S. Comm. on Commerce, Science, and Transportation, United States Senate, Mar. 13, 2017, https://epic.org/testimony/congress/EPIC-SCOM-Drones-Mar2017.pdf; *The Future of Drones in America: Law Enforcement and Privacy Considerations: Hearing Before the S. Judiciary Comm.,* 113th Cong. (2013) (statement of Amie Stepanovich, EPIC Director of the Domestic Surveillance Project), *available at* https://epic.org/privacy/testimony/EPIC-Drone-Testimony-3-13-Stepanovich.pdf; Comments *of EPIC to DHS*, Docket No. DHS-2007-0076 CCTV: Developing Privacy Best Practices (2008), *available at* https://epic.org/privacy/surveillance/epic_cctv_011508.pdf.

[4] EPIC v. CBP, 17-cv-01438, *Complaint*, https://epic.org/foia/cbp/biometric-tracking/1-Complaint.pdf.

EPIC understands that enhanced surveillance techniques may be part of the discussion over border security.[5] EPIC writes to warn that enhanced surveillance at the border will almost certainly sweep up the personal data of U.S. citizens. Before there is any new deployment of surveillance at the U.S. border, an assessment of the privacy implications should be conducted. Additionally, deployment of surveillance technology should be accompanied by new policy and procedures and independent oversight to protect citizens' rights. And any law enforcement agency that uses surveillance tools should be prepared to comply with all current laws, including any open government laws. The privacy assessments, policies and procedures, and oversight mechanisms should all be made public.

Biometric Entry/Exit Tracking System

Customs and Border Protection (CBP) is currently in the process of implementing a Comprehensive Biometric Entry/Exit Plan.[6] The biometric entry/exit plan includes several initiatives to test the use of biometrics at entry/exit points within the U.S., including along the southwestern border.[7]

In March 2015, CBP began testing the use of facial recognition as individuals enter the U.S.[8] A sixty-day field test of U.S. passport holders entering the country was conducted at Washington Dulles International Airport.[9] In January 2016, CBP expanded the program (named the "1-to-1 Facial Comparison Project") to all U.S. airports and expanded the scope to cover first-time travelers from Visa Waiver Programs.[10]

Last year, CBP began testing the use of biometrics as travelers exited the United States. From June 2016 through November 2016, CBP ran a pilot facial recognition program at Hartsfield-Jackson Atlanta International Airport that required passengers on the route from Atlanta to Tokyo to submit themselves to facial recognition in order to board their departing flight.[11]

---

[5] Samantha Schmidt, *Border wall with Mexico won't be built 'from sea to shining sea,' DHS secretary says*, Washington Post, April 6, 2017, https://www.washingtonpost.com/news/morning-mix/wp/2017/04/06/border-wall-with-mexico-wont-be-built-from-sea-to-shining-sea-dhs-secretary-says/.

[6] Dep't of Homeland Security, *Comprehensive Biometric Entry/Exit Plan: Fiscal Year 2016 Report to Congress* (2016), https://www.dhs.gov/sites/default/files/publications/Customs%20and%20Border%20Protection%20-%20Comprehensive%20Biometric%20Entry%20and%20Exit%20Plan.pdf.

[7] *See, e.g.*, U.S. Customs and Border Protection, *Biometric Travel Security Initiatives*, https://www.cbp.gov/travel/biometric-security-initiatives.

[8] U.S. Customs and Border Protection, *1:1 Facial Recognition Air Entry Pilot Impact Assessment*, 1 (Mar. 11, 2015), https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp-1-to-1-facial-recognition-air-entry-pilot-march-11-2015.pdf.

[9] *Id*.

[10] U.S. Customs and Border Protection, *1:1 Facial Comparison Project Privacy Impact Assessment Update*, 3 (Jan. 14, 2016), https://www.dhs.gov/sites/default/files/publications/DHS-CBP-PIA%20%E2%80%93%20025a%201-1%20Facial%20Comparison%20Project.pdf.

[11] Dep't of Homeland Sec., *Privacy Impact Assessment for the Departure Information Systems Test* (June 13, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-dis%20test-june2016.pdf.

President Trump's Executive Order, "Protecting the Nation from Foreign Terrorist Entry into the United States," explicitly calls on the CBP to "expedite the completion and implementation of biometric entry exit tracking system."[12] CBP is set to expand the scope of the agency's pilot programs testing the use of facial recognition at exits points from the U.S.[13]

Facial recognition poses significant threats to privacy and civil liberties. It can be done covertly, remotely, and on a mass scale. Additionally, there are a lack of well-defined federal regulations controlling the collection, use, dissemination, and retention of biometric identifiers. Ubiquitous and near-effortless identification eliminates individual's ability to control their identities and poses a specific risk to the First Amendment rights of free association and free expression.

The use of facial recognition at the border has real consequences for U.S. citizens as well as non-U.S. citizens. All people entering the U.S., including U.S. passport holders, could be subject to this new screening technique. The CBP should be more transparent and more accountable about its biometric tracking system, which is why EPIC has sued the agency for documents about the program to release to the public.

Acting Director Executive Director Michelini and Executive Assistant Commissioner Owens should be asked:

- **Does CBP intend to implement biometric tracking such as facial recognition on all individuals, including U.S. citizens, entering and/or exiting the U.S.?**

Drones at the Border

Customs and Border Protection (CBP) is already deploying aerial drones with facial recognition technology at the border.[14] In 2013, records obtained by EPIC under the Freedom of Information Act showed that the CBP is operating drones in the United States capable of intercepting electronic communications.[15] The records obtained by EPIC also indicate that the ten Predator B drones operated by the agency have the capacity to recognize and identify a

[12] Exec. Order No. 13,780 § 8.
[13] *Visa Overstays: A Gap in the Nation's Border Security: Hearing Before the Subcomm. on Border & Mar. Sec. of the H. Comm. on Homeland Sec.*, 115th Cong. (2017) (statement of John Wagner, Deputy Exec. Assistant Comm'r, Office of Field Operations, Customs & Border Prot.), *available at* https://www.dhs.gov/news/2017/05/23/written-testimony-plcy-cbp-and-ice-house-homeland-security-subcommittee-border-and.
[14] Russel Brandom, *The US Border Patrol is trying to build face-reading drones*, The Verge, Apr. 6, 2017, http://www.theverge.com/2017/4/6/15208820/customs-border-patrol-drone-facial-recognition-silicon-valley-dhs; Dept. of Homeland Security, *Other Transaction Solicitation (OTS) HSHQDC-16-R-00114 Project: Small Unmanned Aircraft Systems (sUAS) Capabilities*, Jul. 15, 2016, https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSHQDC-16-R-00114/listing.html.
[15] EPIC, *EPIC FOIA - US Drones Intercept Electronic Communications and Identify Human Targets*, Feb. 28, 2013, https://epic.org/2013/02/epic-foia---us-drones-intercep.html (record received available at https://epic.org/privacy/drones/EPIC-2010-Performance-Specs-1.pdf.)

person on the ground.[16] The documents were provided in response to a request from EPIC for information about the Bureau's use of drones across the country. The agency has made the Predator drones available to other federal, state, and local agencies. The records obtained by EPIC raise questions about the agency's compliance with federal privacy laws and the scope of domestic surveillance.

Following the revelations about drone surveillance at the border, EPIC, joined by thirty organizations and more than a thousand individuals, petitioned CBP to suspend the domestic drone surveillance program, pending the establishment of concrete privacy regulations.[17] The petition stated that "the use of drones for border surveillance presents substantial privacy and civil liberties concerns for millions of Americans across the country." *Any authorization granted to CBP to conduct surveillance at the border must require compliance with federal privacy laws and regulations for surveillance tools, including drones.*

Much of this surveillance technology could, in theory, be deployed on manned vehicles. However, drones present a unique threat to privacy. Drones are designed to maintain a constant, persistent eye on the public to a degree that former methods of surveillance were unable to achieve. The technical and economic limitations to aerial surveillance change dramatically with the advancement of drone technology. Small, unmanned drones are already inexpensive; the surveillance capabilities of drones are rapidly advancing; and cheap storage is readily available to maintain repositories of surveillance data.[18] Drones "represent an efficient and cost-effective alternative to helicopters and airplanes," but their use implicates significant privacy interests.[19] As the price of drones "continues to drop and their capabilities increase, they will become a very powerful surveillance tool."[20] *The use of drones in border security will place U.S. citizens living on the border under ceaseless surveillance by the government.*

The Supreme Court has not yet considered the limits of drone surveillance under the Fourth Amendment, though the Court held twenty years ago that law enforcement may conduct manned aerial surveillance operations from as low as 400 feet without a warrant.[21] No federal statute currently provides adequate safeguards to protect privacy against increased drone use in the United States. However, some border states do limit warrantless aerial surveillance. In 2015, the Supreme Court of New Mexico held that the Fourth Amendment prohibits the warrantless

---

[16] *Performance Spec for CBP UAV System,* Bureau of Customs and Border Patrol, https://epic.org/privacy/drones/EPIC-2005-Performance-Specs-2.pdf.
[17] EPIC, *Domestic Drones Petition*, https://epic.org/drones_petition/.
[18] *See generally* EPIC, *Drones: Eyes in the Sky*, Spotlight on Surveillance (2014), https://www.epic.org/privacy/surveillance/spotlight/1014/drones.html.
[19] M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 Stan. L. Rev. Online 29, 30 (Dec. 12, 2011); *See also* Jeffrey Rosen, *Symposium Keynote Address*, 65 Rutgers L. Rev. 965, 966 (2013) ("[A]s police departments increasingly begin to use drone technologies to track individual suspects 24/7, or to put areas of the country under permanent surveillance, this possibility of 24/7 tracking will become increasingly real.").
[20] Bruce Schneier, *Surveillance And the Internet of Things*, Schneier on Security (May 21, 2013), https://www.schneier.com/blog/archives/2013/05/the_eyes_and_ea.html.
[21] *See Florida v. Riley*, 488 U.S. 445 (1989) (holding that a police helicopter flying more than 400 feet above private property is not a search).

aerial surveillance of, and interference with, a person's private property.[22] Accordingly, there are substantial legal and constitutional issues involved in the deployment of aerial drones by law enforcement and state and federal agencies that need to be addressed.

A 2015 Presidential Memorandum on drones and privacy required that all federal agencies to establish and publish drone privacy procedures by February 2016.[23] Emphasizing the "privacy, civil rights, and civil liberties concerns" raised by the technology,[24] President Obama ordered agencies to ensure that any use of drones by the federal government in U.S. airspace comply with "the Constitution, Federal law, and other applicable regulations and policies."[25]

However, the DHS has failed to produce reports required by the 2015 Presidential Memorandum. EPIC has submitted a FOIA request for DHS' policies and reports required under the Presidential Memorandum, but the DHS has failed to respond.

Acting Director Executive Director Michelini and Executive Assistant Commissioner Owens should be asked:

- **How will CBP comply with state laws prohibiting warrantless aerial surveillance when deploying drones?**
- **When will CBP produce the drone privacy procedures required by the 2015 Presidential Memorandum?**

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Subcommittee on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

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

/s/ *Jeramie Scott*
Jeramie Scott
EPIC National Security Counsel

[22] *State v. Davis,* 360 P.3d 1161 (N.M. 2015); *see* Brief of *Amicus Curiae* EPIC, *id., available at* https://epic.org/amicus/drones/new-mexico/davis/State-v-Davis-Opinion.pdf.
[23] President Barack Obama, *Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems* (Feb. 15, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.
[24] *Id.* at § 1(e).
[25] *Id.* at § 1.