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

April 24, 2018

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 hearing on "Border Security, Commerce and Travel: Commissioner McAleenan's Vision for the Future of CBP."[1] EPIC welcomes your continued leadership on CBP oversight and looks forward to opportunities to work with you and your staff.

The Electronic Privacy Information Center ("EPIC") is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC is focused on the protection of individual privacy rights, and we are particularly interested in the privacy problems associated with surveillance.[3] EPIC also manages one of the most extensive open government litigation programs in the United States.[4]

[1] *Border Security, Commerce and Travel: Commissioner McAleenan's Vision for the Future of CBP*, 115th Cong. (2018), H. Comm. on Homeland Security, Subcomm. on Border and Maritime Security, https://homeland.house.gov/hearing/border-security-commerce-and-travel-commissioner-mcaleenans-vision-for-the-future-of-cbp/ (Apr. 25, 2018).
[2] *See About EPIC*, EPIC.org, https://epic.org/epic/about.html.
[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 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).

EPIC understands that enhanced surveillance techniques will 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 increased deployment of surveillance systems 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 all open government obligations. The privacy assessments, policies and procedures, and oversight mechanisms should all be made public. Most critically, if the CBP chooses to create or expand a system of records that contains personal information which is retrievable by name, it must comply with all of the requirements of the Privacy Act, including publishing a System of Records Notice and a Notice of Proposed Rulemaking so that the public is able to comment on a record system established by a federal agency.[6]

Biometric Entry/Exit Tracking System

Recently, new privacy risks have arisen with the deployment of facial recognition technology at U.S. airports. An Executive Order recommends that agencies "expedite the completion and implementation of biometric entry exit tracking system,"[7] and Customs and Border Protection ("CBP") has deployed facial recognition technology at several U.S. airports.[8] But corresponding privacy safeguards have not yet been established.

EPIC would like to remind the Committee that in 2009, Verified Identity Pass, Inc., a corporate participant in the Transportation Security Administration's ("TSA") Registered Traveler program ceased operations after declaring bankruptcy, following a massive data breach concerning personal data, including biometric identifiers.[9] Verified Identity Pass, Inc. operated "Clear," a TSA recognized Registered Traveler program. Clear was the largest Registered Traveler program in the nation operating out of 20 airports with about 200,000 members.

EPIC had warned this Committee back in 2005 of the risks of the Registered Traveler program.[10] We explained that without ensuring compliance with federal Privacy Act obligations, the agency was placing at risk the privacy and security of the American public. We said:

> The Privacy Act creates critical and necessary safeguards not simply to protect privacy, but also to ensure accuracy and accountability. Any government-

[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] 5 U.S.C.A. § 552a(e)(4).
[7] Exec. Order No. 13,780 § 8.
[8] U.S. Customs and Border Protection, *CBP Deploys Facial Recognition Biometric Technology at 1 TSA Checkpoint at JFK Airport* (Oct. 11, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-deploys-facial-recognition-biometric-technology-1-tsa-checkpoint.
[9] EPIC, *Bankruptcy of Verified Identity Pass and the Privacy of Clear Registered Traveler Data*, https://www.epic.org/privacy/airtravel/clear/.
[10] *The Future of Registered Traveler*, 109th Cong. (2005), H. Comm. on Homeland Security, Subcomm. on Economic Security, Infrastructure Protection, and Cybersecurity (testimony of Marc Rotenberg), *available at* http://epic.org/privacy/airtravel/rt_test_110305.pdf.

> approved security system that keeps personal information on individuals should meet the Privacy Act requirements for necessity, relevance, and openness, including individual access and correction. It should be made clear that these requirements apply whether the information originates with the agency or with information provided by the individual.

Facial recognition continues to pose significant threats to privacy and civil liberties. Facial recognitions 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.

Transparency about these biometric surveillance programs is essential, particularly because their accuracy is questionable. In December 2017, a Freedom of Information Act lawsuit pursued by EPIC produced the public release of a CBP report on iris imaging and facial recognition scans for border control. The "Southwest Border Pedestrian Field Test" revealed that the CBP does not perform operational matching at a "satisfactory" level.[11] In a related FOIA lawsuit, EPIC obtained documents from the FBI concerning the Next Generation Identification database which contains facial scans, fingerprints, and other biometrics of millions of Americans.[12] The documents obtained by EPIC revealed that biometric identification is often inaccurate.[13]

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 intrusive screening technique. EPIC has filed a FOIA lawsuit to obtain documents to determine if there are proper privacy safeguards in place for the collection of biometric information at US airports.[14]

There is also a new study from the MIT Media Lab which found that facial recognition is less accurate for persons of color. The MIT study found that the error rate in face recognition software for dark-skinned females was 20.8% − 34.7%, while the error rate for light-skinned males was 0.0% - 0.3%.[15] As the New York Times explained, "[t]hese disparate results, calculated by Joy Buolamwini, a researcher at the M.I.T. Media Lab, show how some of the biases in the real world can seep into artificial intelligence, the computer systems that inform facial recognition."[16] If it is

---

[11] U.S. Customs and Border Protection, *Southern Border Pedestrian Field Test Summary Report,* https://epic.org/foia/dhs/cbp/biometric-entry-exit/Southern-Border-Pedestrian-Field-Test-Report.pdf (December 2016).
[12] *EPIC v. FBI – Next Generation Identification*, EPIC, https://epic.org/foia/fbi/ngi/.
[13] DEPT. OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION, NEXT GENERATION IDENTIFICATION (NGI) SYSTEM REQUIREMENTS DOCUMENT VERSION 4.4 at 244 (Oct. 1, 2010), https://epic.org/foia/fbi/ngi/NGI-System-Requiremets.pdf.
[14] *EPIC v. CBP (Biometric Entry/Exit Program)*, EPIC, https://epic.org/foia/dhs/cbp/biometric-entry-exit/.
[15] Joy Buolamwini and Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research (2018) at 11, *available at* http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
[16] Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, New York Times, Feb. 9, 2018, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

correct that that facial recognition as a form of identification discriminates against persons of color in ways that other forms of identification do not, there is a substantial civil rights concern that the Committee should investigate.

The involvement of private companies raises additional concerns. CBP has enlisted airlines such as JetBlue and Delta to implement face recognition technology in U.S. airports.[17] JetBlue is running a self-boarding program using facial recognition in lieu of checking boarding passes. Delta aims to use facial recognition as part of baggage drop off.[18] It is unclear whether access to biometric identifiers by JetBlue and Delta will lead to non-security uses of biometric identifiers.

These airlines are promoting facial recognition as a convenience, but it's clearly part of a larger effort by the government to implement a biometric surveillance program that will capture the facial images of all air travelers. And travelers do not understand how this system, once in place at airports, could be deployed in other settings,

The CBP and the TSA now plan deploy facial recognition technology at TSA checkpoints—further expanding the use of a privacy-invasive technology without regulations in place to provide proper protections.

Commissioner McAleenan should be asked the following questions:

- **Has the CBP conducted the necessary Privacy Impact Assessments prior to deployments?**
- **Are there plans to increase the use of facial recognition?**
- **Has CBP detected racial bias in the deployment of its facial recognition systems?**
- **What safeguards are currently in place to protect facial scans from hacking or breaches?**
- **What restrictions on the use of biometric identifiers by private companies have been established?**

Drones at the Border

Customs and Border Protection (CBP) is already deploying aerial drones with facial recognition technology at the border.[19] 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

[17] Asma Khalid, *Facial Recognition May Boost Airport Security But Raises Privacy Worries*, NPR, June 26, 2017, https://www.npr.org/sections/alltechconsidered/2017/06/26/534131967/facial-recognition-may-boost-airport-security-but-raises-privacy-worries.
[18] Ben Mutzabaugh, *Delta to test facial-recognition tech on new self-service bag drop*, USA TODAY, May 15, 2017, https://www.usatoday.com/story/travel/flights/todayinthesky/2017/05/15/delta-test-facial-recognition-tech-new-self-service-bag-drops/101703956/.
[19] 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.

intercepting electronic communications.[20] 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 person on the ground.[21] 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.[22] 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.[23] Drones "represent an efficient and cost-effective alternative to helicopters and airplanes," but their use implicates significant privacy interests.[24] As the price of drones "continues to drop and their capabilities increase, they will become a very powerful surveillance tool."[25] *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.[26] 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

---

[20] 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.)

[21] *Performance Spec for CBP UAV System,* Bureau of Customs and Border Patrol, https://epic.org/privacy/drones/EPIC-2005-Performance-Specs-2.pdf.

[22] EPIC, *Domestic Drones Petition*, https://epic.org/drones_petition/.

[23] *See generally* EPIC, *Drones: Eyes in the Sky*, Spotlight on Surveillance (2014), https://www.epic.org/privacy/surveillance/spotlight/1014/drones.html.

[24] 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.").

[25] 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.

[26] *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).

Court of New Mexico held that the Fourth Amendment prohibits the warrantless aerial surveillance of, and interference with, a person's private property.[27] 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.[28] Emphasizing the "privacy, civil rights, and civil liberties concerns" raised by the technology,[29] 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."[30]

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.

Commissioner McAleenan should be asked:

- **How will CBP comply with state laws prohibiting warrantless aerial surveillance when deploying drones?**
- **When will CBP publish the drone privacy procedures report 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

/s/ *Christine Bannan*
Christine Bannan
EPIC Policy Fellow

---

[27] *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.
[28] 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.
[29] *Id.* at § 1(e).
[30] *Id.* at § 1.