epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

October 16, 2019

The Honorable Dan Sullivan, Chairman
The Honorable Edward J. Markey, Ranking Member
U.S. Senate Committee on Commerce, Science, and Transportation
Subcommittee on Security
512 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Sullivan and Ranking Member Markey:

We write to you in advance of the hearing on "Improving Security at America's Airports: Stakeholder Perspectives."[1] EPIC recently filed a lawsuit against the Customs and Border Protection ("CBP") agency for a failure to establish necessary privacy safeguards for the use of facial images at US borders.[2] Because the Transportation Security Administration ("TSA") has failed to establish necessary privacy safeguards, including ensuring the travelers are able to exercise their legal right to opt-out, ***we request you suspend the TSA's use of facial image technology pending the completion of required public rulemaking by CBP.*** A moratorium should also be established for other DHS components that propose to deploy facial recognition and have not conducted a public rulemaking. ***There is currently no legal authority for DHS' or TSA's use of facial recognition technology.***

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.[3] EPIC is focused on protecting individual privacy rights, and we are particularly interested in the privacy problems associated with surveillance.[4] We applaud Senator Markey and Senator Lee for calling for the suspension of DHS's use of facial recognition in airports until a rulemaking to establish privacy and security safeguards is complete.[5]

Recently, new privacy risks have arisen with the deployment of facial recognition technology at U.S. airports following a 2017 Executive Order to "expedite the completion and implementation

---

[1] *Improving Security at America's Airports: Stakeholder Perspectives*, Senate Comm. on Commerce, Science, & Trans., Subcomm. on Security, 116th Cong. (Oct. 17, 2019), https://www.commerce.senate.gov/2019/10/improving-security-at-america-s-airports-stakeholder-perspectives/6e8bba82-9b59-4f09-b0c4-e8511497f5c4.
[2] *EPIC v. U.S. Customs and Border Protection*, No. 19-cv-689 (D.D.C. filed Mar. 12, 2019); *See* https://epic.org/foia/dhs/cbp/alt-screening-procedures/.
[3] *See About EPIC*, EPIC.org, https://epic.org/epic/about.html.
[4] EPIC, *EPIC Domestic Surveillance Project,* https://epic.org/privacy/surveillance/.
[5] Press Release, Sens. Edward Markey and Mike Lee, *Senators Markey and Lee Call for Transparency on DHS Use of Facial Recognition Technology* (Mar. 12, 2019), https://www.markey.senate.gov/news/press-releases/senators-markey-and-lee-call-for-transparency-on-dhs-use-of-facial-recognition-technology.

of biometric entry exit tracking system."[6] Customs and Border Protection ("CBP") has now implemented the Biometric Entry-Exit program for international travelers at 17 airports.[7] TSA is quickly moving to leverage CBP's Biometric Entry-Exit program to expand the use of facial recognition at airports.[8]

TSA has conducted pilots at John F. Kennedy International Airport and Los Angeles International Airport to test facial recognition technology at security checkpoints servicing international travelers.[9] TSA also tested a fully biometric terminal at Hartsfield-Jackson Atlanta International Airport that used facial recognition to check your bag, go through security, and board a flight,[10] and is currently testing facial recognition at Las Vegas McCarran Airport.[11]

The Las Vegas pilot is testing the "operational effectiveness for matching a traveler's image to the photos on the ID they present."[12] This 1:1 matching is a much more privacy protective implementation of facial recognition. 1:1 matching does not require a massive biometric database, there is no need to retain the image, and the machines conducting the 1:1 match do not need to be connected to the cloud. Such an implementation virtually eliminates data breach risks and the chance of mission creep.

But whether TSA is seriously considering a 1:1 implementation is not clear. The agency's Aviation Security Advisory Committee has failed to fill the committee positions allotted for privacy advocates.[13] And TSA's on roadmap for facial recognition do not include the possibility for implementing 1:1 matching.

In September 2018, TSA released the "TSA Biometrics Roadmap."[14] The Roadmap makes clears TSA's intention to leverage CBP's facial recognition capabilities implemented as part of the Biometric Entry-Exit Program. But alternatives to CBP's cloud-based implementation are not considered in the roadmap. And corresponding privacy safeguards have not yet been established despite TSA moving forward with facial recognition technology.

---

[6] Exec. Order No. 13,780 § 8.
[7] Davey Alba, *The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show* (Mar. 11, 2019), https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for.
[8] TSA, *TSA Biometrics Roadmap* (Sept. 2018), https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.
[9] TSA, *Facial Recognition Technology*, https://www.tsa.gov/node/20451.
[10] TSA, *TSA Releases Roadmap For Expanding Biometrics Technology* (Oct. 15, 2018), https://www.tsa.gov/news/releases/2018/10/15/tsa-releases-roadmap-expanding-biometrics-technology.
[11] *Protecting the Nation's Transportation Systems: Oversight of the Transportation Security Administration*, 114th Cong. (2019), S. Comm. on Commerce, Science, and Trans. (testimony of Patricia F. S. Cogswell TSA Acting Deputy Administrator), *available at* https://www.tsa.gov/news/testimony/2019/09/11/protecting-nations-transportation-systems-oversight-transportation.
[12] *Id.*
[13] TSA, *TSA Announces New Members of Aviation Security Advisory Committee*, (Sept. 27, 2019), https://www.tsa.gov/news/releases/2019/09/27/tsa-announces-new-members-aviation-security-advisory-committee.
[14] *TSA Biometrics Roadmap, supra* note 8.

In response to an EPIC Freedom of Information Act request, CBP recently released 346 pages of documents detailing the agency's scramble to implement the flawed Biometric Entry-Exit system, a system that employs facial recognition technology on travelers entering and exiting the country. The documents obtained by EPIC describe the administration's plan to extend the faulty pilot program to major U.S. airports. The documents obtained by EPIC were covered in-depth by Buzzfeed.[15]

Based on the documents obtained, EPIC determined there are few limits on how airlines can use the facial recognition data collected at airports.[16] Only recently has CBP changed course and indicated that the agency will require airlines to delete the photos they take for the Biometric Entry-Exit program.[17] No such commitment has been made by TSA. Indeed, TSA's Roadmap indicates that the agency wants to expand the dissemination of biometric data as much as possible, stating:

> TSA will pursue a system architecture that promotes data sharing to maximize biometric adoption throughout the passenger base and across the aviation security touchpoints of the passenger experience.[18]

TSA seeks to broadly implement facial recognition through "public-private partnerships" to create a "biometrically-enabled curb-to-gate passenger experience."[19] TSA plans to implement an opt-in model of facial recognition use for domestic travelers but there are no guarantees that in the future TSA will not require passengers to participate in facial recognition or make the alternative so cumbersome as to essentially require passengers to opt-in.

Preserving the ability of U.S. citizens to forgo facial recognition for alternative processes is one of the core privacy issues with CBP's Biometric Entry-Exit program.

EPIC recently sued CBP for all records related to the creation and modification of alternative screening procedures for the Biometric Entry-Exit program.[20] The alternative screening procedure for U.S. travelers that opt-out of facial recognition should be a manual check of the traveler's identification documents. CBP, however, has provided vague and inconsistent descriptions of alternative screening procedures in both its "Biometric Exit Frequently Asked Questions (FAQ)" webpage[21] and the agency's privacy impact assessments.[22] The creation and modification of CBP's

---

[15] Alba, *supra* note 7.
[16] *See* CBP Memorandum of Understanding Regarding Biometric Pilot Project, https://epic.org/foia/dhs/cbp/biometric-entry-exit/MOU-Biometric-Pilot-Project.pdf.
[17] Ashley Ortiz, CBP Program and Management Analyst, Presentation before the Data Privacy & Integrity Advisory Committee, slide 23 (Dec. 2018), https://www.dhs.gov/sites/default/files/publications/SLIDES-DPIAC-Public%20Meeting%2012%2010-2018.pdf.
[18] TSA, *TSA Biometrics Roadmap*, 17 (Sept. 2018).
[19] *Id.* at 19.
[20] *EPIC v. CBP*, 19-cv-00689, *Complaint*, https://epic.org/foia/cbp/alternative-screening-procedures/1-Complaint.pdf.
[21] CBP, *Biometric Exit Frequently Asked Questions (FAQs)*, https://www.cbp.gov/travel/biometrics/biometric-exit-faqs.
[22] U.S. Dep't of Homeland Sec., DHS/CBP/PIA-030(b), *Privacy Impact Assessment Update for the Traveler Verification Service (TVS): Partner Process* 8 (2017), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-may2017.pdf; *see also* U.S. Dep't

alternative screening procedures underscores CBP's unchecked ability to modify alternative screening procedures while travelers remain in the dark about how to protect their biometric data.

Given the close relationship between the TSA's implementation of facial recognition and CBP's Biometric Entry-Exit program, ***the Subcommittee should place a moratorium on TSA's implementation of facial recognition until CBP implements proper privacy assessments, policies and procedures, and oversight mechanisms.***

Facial recognition poses threats to privacy and civil liberties. Facial recognition techniques can be deployed covertly, remotely, and on a mass scale. 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.

Before there is any increased deployment of these programs, CBP must conduct a public rulemaking and TSA must conduct a privacy impact assessment. And deployment of surveillance technology should be accompanied by new policies and procedures and independent oversight to protect citizens' rights.

The use of facial recognition at the border has real consequences for U.S. citizens and non-U.S. citizens. All people entering the U.S., including U.S. passport holders, could be subject to this intrusive screening technique. The privacy assessments, policies and procedures, and oversight mechanisms must all be made public. Most critically, if the TSA creates or expand a system of records that contains personal information retrievable by name, it must comply with the requirements of the Privacy Act so that the public can comment on a record system established by a federal agency.[23]

We ask that our statement be entered into the hearing record.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

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

/s/ *Jeramie Scott*
Jeramie Scott
EPIC Senior Counsel

---

of Homeland Sec., DHS/CBP/PIA-030(c), *Privacy Impact Assessment Update for the Traveler Verification Service (TVS): Partner Process* 5–6 (2017), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-appendixb-july2018.pdf; U.S. Dep't of Homeland Sec., DHS/CBP/PIA-056, *Privacy Impact Assessment for the Traveler Verification Service* 2 (2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030- tvs-november2018_2.pdf.

[23] 5 U.S.C.A. § 552a(e)(4).