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 2, 2019

The Honorable Lucille Roybal-Allard, Chairwoman
The Honorable Chuck Fleischmann, Ranking Member
U.S. House Committee on Appropriations, Subcommittee on Homeland Security
H-307 The Capitol
Washington, D.C. 20515

Dear Chairwoman Roybal-Allard and Ranking Member Fleischmann:

We write to you in advance of the FY2020 Budget Hearing for the Transportation Security Administration ("TSA").[1] EPIC has recently filed a lawsuit against the Customs and Border Protection ("CBP") agency for failure to establish necessary privacy safeguards for the collection of facial images at US borders.[2] Because these same images are made available to the TSA, both components of the Department of Homeland Security ("DHS"), we respectfully that you suspend funding for the TSA's use of facial image technology pending the completion of required privacy impact assessments by CBP, and other DHS components.

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 the protection of individual privacy rights, and we are particularly interested in the privacy problems associated with surveillance.[4]

Recently, new privacy risks have arisen with the deployment of facial recognition technology at U.S. airports as a consequence of a 2017 Executive Order to "expedite the completion and implementation of biometric entry exit tracking system."[5] Customs and Border Protection ("CBP")

[1] *FY 2020 Budget Hearing – Transportation Security Administration*, House Comm. on Appropriations, Subcomm. on Homeland Security, 116th Cong. (April 2, 2019), https://appropriations.house.gov/legislation/hearings/fy-2020-budget-hearing-transportation-security-administration.
[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/; *The Future of Drones in America: Law Enforcement and Privacy Considerations: Hearing Before the S. Comm. on the Judiciary* (2013) (statement of Amie Stepanovich, Director of the EPIC Domestic Surveillance Project), 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.
[5] Exec. Order No. 13,780 § 8.

has now implemented the Biometric Entry-Exit program for international travelers at 17 airports.[6] TSA is quickly moving to leverage CBP's Biometric Entry-Exit program to expand the use of facial recognition at airports.[7]

TSA has already deployed facial recognition technology at one TSA Checkpoint servicing international travelers.[8] In September 2018, TSA released a "TSA Biometrics Roadmap," detailing its plans to use facial recognition, including on domestic travelers.[9] The Roadmap makes clears TSA's intention to leverage CBP's facial recognition capabilities implemented as part of the Biometric Entry-Exit Program. But corresponding privacy safeguards have not yet been established.

In response to EPIC's 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.[10]

Based on the documents obtained, EPIC determined that there are few limits on how airlines can use the facial recognition data collected at airports.[11] 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.[12] 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.[13]

TSA seeks to broadly implement facial recognition through "public-private partnerships" in an effort to create a "biometrically-enabled curb-to-gate passenger experience."[14] Currently, TSA plans to

---

[6] 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.
[7] TSA, *TSA Biometrics Roadmap* (Sept. 2018), https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.
[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] TSA, *TSA Biometrics Roadmap* (Sept. 2018), https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.
[10] 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.
[11] *See* CBP Memorandum of Understanding Regarding Biometric Pilot Project, https://epic.org/foia/dhs/cbp/biometric-entry-exit/MOU-Biometric-Pilot-Project.pdf.
[12] 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.
[13] TSA, *TSA Biometrics Roadmap*, 17 (Sept. 2018).

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 privacy issues with CBP's Biometric Entry-Exit program. Senator Markey (D-MA) and Senator Lee (R-UT) called for the CBP to suspend facial recognition at the border to ensure that travelers are able to opt-out of facial recognition if they wish.[15]

In fact, EPIC recently sued CBP for all records related to the creation and modification of alternative screening procedures for the Biometric Entry-Exit program.[16] 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[17] and the agency's privacy impact assessments.[18] The creation and modification of CBP's 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 Appropriations Committee should halt funding for TSA's implementation of facial recognition until CBP's Biometric Entry-Exit program implements proper privacy assessments, policies and procedures, and oversight mechanisms.*

EPIC's expertise in this field is extensive. EPIC would like to remind the Committee that in 2009, Verified Identity Pass, Inc., a corporate participant in the TSA Registered Traveler program ceased operations after declaring bankruptcy, following a massive data breach concerning personal data, including biometric identifiers.[19] 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.

---

[14] *Id.* at 19.
[15] 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.
[16] EPIC v. CBP, 19-cv-00689, *Complaint*, https://epic.org/foia/cbp/alternative-screening-procedures/1-Complaint.pdf.
[17] CBP, *Biometric Exit Frequently Asked Questions (FAQs)*, https://www.cbp.gov/travel/biometrics/biometric-exit-faqs.
[18] 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 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.
[19] EPIC, *Bankruptcy of Verified Identity Pass and the Privacy of Clear Registered Traveler Data*, https://www.epic.org/privacy/airtravel/clear/.

EPIC had warned Congress back in 2005 of the risks of the Registered Traveler program.[20] 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-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.[21]

Facial recognition continues to pose 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.

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. Before there is any increased deployment of these programs, 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 the privacy assessments, policies and procedures, and oversight mechanisms should all be made public. Most critically, if the TSA 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.[22]

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

---

[20] *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.
[21] *Id.*
[22] 5 U.S.C.A. § 552a(e)(4).