July 9, 2019

The Honorable Bennie Thompson
Chairman
Committee on Homeland Security
310 Cannon House Office Building
Washington, DC 20515

The Honorable Mike Rogers
Ranking Member
Committee on Homeland Security
310 Cannon House Office Building
Washington, DC 20515

RE: The Suspension of Face Recognition Technology Use by the Department of Homeland Security

Dear Chairman Thompson and Ranking Member Rogers:

The undersigned organizations, which are dedicated to preserving privacy, civil liberties, and civil rights, write to urge you to immediately suspend the Department of Homeland Security's (DHS) use of face recognition technology on the general public.

The use of face recognition technology by the DHS poses serious risks to privacy and civil liberties, threatens immigrants, broadly impacts American citizens, and has been implemented without proper safeguards in place or explicit Congressional approval. The technology is being deployed today by authoritarian governments as a tool to suppress speech and monitor critics, minorities, and everyday citizens. Congress should not permit the continued use of face recognition in the United States absent safeguards to prevent such abuses.

Moreover, the extraordinary breach of the images of travelers' faces and license plates, surveillance-equipment schematics and sensitive contracting documents by a CBP contractor has made clear that these programs are creating new risks to the privacy and security of Americans.[1] Through carelessly managed programs, DHS itself created new security threats. It would be irresponsible for DHS to move forward with face recognition programs that collect massive amounts of sensitive data until a thorough investigation of this incident is completed and the agency demonstrates that it can fully safeguard its systems.

DHS' Use of Face Recognition Technology

DHS is in the process of integrating and expanding the agency's use of face recognition technology through various programs of its subcomponents. DHS' use of face recognition will affect millions of individuals, who will lack the protections needed against a powerfully invasive surveillance tool.

[1] Drew Harwell, *Hacked documents reveal sensitive details of expanding border surveillance*, Wash. Post (June 21), https://www.washingtonpost.com/technology/2019/06/21/hacked-documents-reveal-sensitive-details-expanding-border-surveillance/.

Customs and Border Protection

The broadest current use of face recognition technology is the Customs and Border Protection's Biometric Entry-Exit program. Without legal authority or the opportunity for public comment, the U.S. Customs and Border Protection (CBP) has broadly deployed facial recognition technology at U.S. airports to all travelers, including U.S. citizens. The agency plans to "incrementally deploy biometric capabilities across all modes of travel — air, sea, and land — by fiscal year 2025."[2]

CBP uses flight manifests and photographs obtained from the State Department to create "galleries" to match with photos captured at international airports.[3] "If CBP does not have access to advance passenger information, such as for pedestrians or privately owned vehicles at land ports of entry, CBP will build galleries using photographs of 'frequent' crossers for that specific port of entry[.]"[4] CBP uses its own equipment as well as that of private firms, other government agencies, and foreign governments to capture face images.[5] Yet, there are no formal rules restricting the use of the photos captured by non-CBP owned equipment.[6]

The steady implementation of CBP's biometric entry-exit program in airports across the country has been widely reported.[7] The program affects a significantly large group of U.S. citizens traveling in and out of the country. At the Atlanta Hartsfield-Jackson International Airport alone, "[a]bout 25,000 passengers move through the terminal each week" and the

---

[2] U.S. Dep't of Homeland Sec., Office of Inspector Gen., OIG-18-80, Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide, 7 (Sept. 21, 2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf [hereinafter OIG Report].

[3] *Id.*

[4] U.S. Dep't of Homeland Sec., U.S. Customs and Border Protection, DHS/CBP/PIA-0056, Privacy Impact Assessment for the Traveler Verification Service, 5 (Nov. 14, 2018) https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf [hereinafter TVS Nov. 2018 PIA].

[5] *Id.* at 7-8.

[6] *See Memorandum of Understanding Between and Among U.S. Customs and Border Protection and [REDACTED] and [REDACTED] Regarding [REDACTED] Biometric Pilot Project at [REDACTED]* (June 2017), https://epic.org/foia/dhs/cbp/biometric-entry-exit/MOU-Biometric-Pilot-Project.pdf.

[7] See e.g., Bart Jansen, *CBP: Orlando is First U.S. Airport to Scan Faces of All International Travelers*, USA Today (June 21, 2018), https://www.usatoday.com/story/travel/flights/todayinthesky/2018/06/21/orlando-international-airport-scan-faces-u-s-citizens/722643002/; Lori Aratani, *Officials Unveil New Facial Recognition System at Dulles International Airport*, Wash. Post (Sept. 7, 2018), https://www.washingtonpost.com/transportation/2018/09/06/officials-unveil-new-facial-recognition-system-dulles-international-airport/; Gregory Wallace, *Instead of the Boarding Pass, Bring Your Smile to the Airport*, CNN (Sept. 10, 2018), https://www.cnn.com/travel/article/cbp-facial-recognition/index.html; Jack Stewart, *Creepy or Not, Face Scans Are Speeding Up Airport Security*, Wired (Nov. 21, 2018), https://www.wired.com/story/airport-security-biometrics-face-scanning/;

majority of those passengers are subject to facial recognition.[8] Further, "CBP hopes to have facial recognition boarding at all US airports serving international flights within 3 or 4 years."[9]

The Biometric Entry-Exit program is flawed. A report on iris and facial recognition technologies at a southern land border found that the technologies did not perform operational matching at a "satisfactory" level.[10] A DHS Office of the Inspector General ("IG") report found that CBP's Biometric Entry-Exit program suffered from technical and operational challenges. The IG report also found that CBP could not "produce biometric matches consistently for individuals in certain passenger groups" with the lowest biometric confirmation rate being for U.S. citizens.[11] Moreover, several reports and studies have noted that face recognition algorithms are often less accurate on certain sub-groups, including women and people with darker skin pigmentation.[12]

Americans returning to the United States have also found it difficult to opt-out of the facial recognition screening, which is their legal right.[13] Travelers routinely report on burdensome procedures intended to compel individuals to undergo facial recognition even if that is not their choice.[14] Additionally, CBP has not undergone formal rulemaking addressing how information collected will be used, disclosed, and retained, and what remedies will exist in cases where individuals are adversely impacted by the use of the technology.

These concerns are further amplified given that CBP uses face recognition technology for purposes that extend far beyond simply verifying whether someone purportedly matches the photograph on their travel document. CBP plans to use the facial recognition to search biometric watch lists – raising questions about how such lists will be compiled and whether they will be the predicate for additional immigration and law enforcement activities[15] The data from the

---

[8] Lori Aratani, *Your Face is Your Boarding Pass at this Airport*, Wash. Post (Dec. 4, 2018), https://www.washingtonpost.com/nation/2018/12/04/your-face-is-your-boarding-pass-this-airport/.
[9] Thom Patterson, *US Airport Opens First Fully Biometric Terminal*, CNN (Dec. 3, 2018), https://www.cnn.com/travel/article/atlanta-airport-first-us-biometric-terminal-facial-recognition/index.html.
[10] U.S. Customs and Border Protection, *Southern Border Pedestrian Field Test Summary Report*, 8 (Dec. 2016), https://epic.org/foia/dhs/cbp/biometric-entry-exit/Southern-Border-Pedestrian-Field-Test-Report.pdf.
[11] OIG Report at 19.
[12] *See, e.g.*, Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
[13] *See* Zack Whittaker, *Yes, Americans can opt-out of airport facial recognition – here's how*, TechCrunch, https://techcrunch.com/2019/05/13/americans-opt-out-facial-recognition-airport/; Allie Funk, *I Opted Out of Facial Recognition at the Airport—It Wasn't Easy,* Wired, July 2, 2019, https://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/.
[14] Allie Funk, *I Opted Out of Facial Recognition at the Airport—It Wasn't Easy,* Wired, July 2, 2019, https://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/.
[15] U.S. Department of Homeland Security U.S. Customs and Border Protection, *Biometric Entry-Exit Program Concept of Operations*, 000039 (June 27, 2017), https://epic.org/foia/dhs/cbp/biometric-entry-exit/CBP-Biometric-Entry-Exit-Concept-of-Operations.pdf.

Biometric Entry-Exit program will also be broadly accessible within DHS with the Coast Guard, Transportation Security Administration (TSA), and Immigration and Customs Enforcement (ICE) all having access to the data.[16]

Transportation Security Administration

The TSA has plans to expand the use of face recognition to all domestic travelers.[17] The TSA Biometric Roadmap envisions the use of face recognition for booking, check-in, bag drop, the security line, access to an airport lounge, and boarding.[18] TSA states it "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."[19]

Similar to CBP, TSA has not undergone rulemaking clarifying how information will be collected, used, or retained. However, TSA's biometric roadmap suggests that its system will be interoperable with CBP, and thus may be utilized for other immigration and law enforcement activities.

Immigration and Customs Enforcement

Recent news reports show that ICE has expanded the agency's deployment and use of face recognition systems. Public records covered by the press this week show that ICE has been sending facial recognition requests to state DMVs for years.[20] As a result, millions of innocent state residents have had their faces scanned by ICE without notice or consent. Internal documents also suggest that ICE plans to leverage CBP's biometric entry-exit system to identify and search for information regarding non-citizens encountered during enforcement activities.[21]

In addition, last year, Amazon marketed the company's facial recognition service "Rekognition" to ICE for border control.[22] A test of Amazon's face recognition software resulted

---

[16] *See* U.S. Department of Homeland Security U.S. Customs and Border Protection, *Biometric Entry-Exit Program Concept of Operations* 000063 (June 27, 2017), https://epic.org/foia/dhs/cbp/biometric-entry-exit/Concept-of-Operations.pdf; *see also* U.S. Department of Homeland Security, *Capability Analysis Study Plan for Biometric Entry-Exit* 000160-000161, https://epic.org/foia/dhs/cbp/biometric-entry-exit/Capability-Analysis-Study-Plan.pdf.

[17] Transportation Security Administration, *TSA Biometrics Roadmap* (Sept. 2018), https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

[18] *Id.* at 18.

[19] *Id.* at 17.

[20] Drew Harwell, *FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches*, Wash. Post (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

[21] *See* U.S Department of Homeland Security U.S. Customs and Border Protection, *Biometric Entry-Exit Program: Concept of Operations*, 000063 (June 2017), https://epic.org/foia/dhs/cbp/biometric-entry-exit/CBP-Biometric-Entry-Exit-Concept-of-Operations.pdf.

[22] Drew Harwell, *Amazon met with ICE officials over facial-recognition system that could identify immigrants*, Wash. Post (Oct. 23, 2018), https://www.washingtonpost.com/technology/2018/10/23/amazon-met-with-ice-officials-over-facial-recognition-system-that-could-identify-immigrants/.

in Amazon's technology falsely matching 28 members of Congress to mugshots and other tests have similarly found the technology to be less accurate on individuals with darker skin pigmentations.[23]

There is a lack of public information on how ICE might use the face recognition capabilities implemented as part of the Biometric Entry-Exit program, ICE's current use of face recognition technology, and whether the agency intends to deploy other face recognition capabilities. There is a serious risk that ICE could deploy face recognition for purposes of indiscriminate immigration enforcement and use the technology, despite its record of error, as a pretext for aggressive questioning and harassment of immigrants—including those lawfully present in the United States.

Secret Service

The U.S. Secret Service is testing the use of face recognition technology to identify people in the public spaces in and around the White House.[24] The spaces around the White House are regularly used for First Amendment-protected protests and demonstrations. The possible use of face recognition to identify individuals near the White House raises serious First Amendment issues and threatens to chill speech.

DHS' Use of Face Recognition Lacks Proper Safeguards and Pose Substantial Risks

Use of face recognition poses a unique threat to Constitutional rights. Participation in society necessarily exposes one's images in public spaces. But ubiquitous and near effortless identification eliminates the individual's ability to control the disclosure of their identities to others and poses a special risk to the First Amendment rights of free association and free expression. The proposed plans by DHS risk creating a world where individuals are forced to submit to face recognition surveillance simply to exercise their right to travel.

The aggregation of biometric data for the use of face recognition and the broad dissemination of this data poses cybersecurity risks and increases the risk of a data breach. Indeed, a CBP vendor who had collected images of travelers along with license plate reader data and other sensitive information was subject to a recent data breach.[25]

Face recognition technology will disproportionately impact already marginalized groups. Studies have shown that facial recognition has significantly higher error rates for darker-

[23] Natasha Singer, *Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says*, N.Y. Times (July 26 ,2018), https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html.
[24] USSS PIA at 1, https://www.dhs.gov/sites/default/files/publications/privacy-pia-usss-frp-november2018.pdf.
[25] Drew Harwell, *Hacked documents reveal sensitive details of expanding border surveillance*, Wash. Post (June 21), https://www.washingtonpost.com/technology/2019/06/21/hacked-documents-reveal-sensitive-details-expanding-border-surveillance/.

skinned individuals.[26] It is unacceptable for DHS to implement a technology with a documented racial bias without proving that such a bias has been eliminated. Moreover, use of face recognition for immigration enforcement raises further risks of a disproportionate impact on already marginalized groups.

The agency continues to expand the use of face recognition beyond what was ever authorized by Congress. In fact, the Biometric Entry-Exit program itself is an example of mission creep. The program leverages the photos provided by passport applicants to the State Department, who provided the photos for the specific purpose of obtaining a passport, only to see those photos used in conjunction with face recognition technology to create a digital ID. Additionally, the State Department then disclosed the biometric data to other agencies, including DHS, and there was nothing a passport holder could do to prevent the disclosure. And, there is nothing an individual could do to stop DHS from further disseminating their biometric data.

DHS' use of face recognition lacks the safeguards needed to prevent overcollection, overly broad uses, widespread dissemination, and unnecessarily long retention. Moreover, DHS has failed to show that less invasive alternatives could not be used. DHS has moved forward with face recognition with a focus on justifying its implementation and not a focus on whether, given the risks, the technology should be implemented.

Conclusion

Face recognition is an especially dangerous technology in need of strict limits on its use, robust transparency, oversight, and accountability. It is imperative that Congress suspend DHS' use of face recognition until Congress fully debates what, if any, proposed uses should move forward.

If you have questions, please contact Jeramie D. Scott, EPIC Senior Counsel, at jscott@epic.org.

Sincerely,

Access Now
ACLU
American-Arab Anti-Discrimination Committee (ADC)
Algorithmic Justice League
Center for Democracy & Technology
Center for Digital Democracy
Center on Privacy & Technology at Georgetown Law
Constitutional Alliance
Consumer Action
Consumer Federation of America
Council on American-Islamic Relations (CAIR)
Cyber Privacy Project

[26] Joy Buolamwini (MIT Media Lab) and Timnit Gebru (Microsoft Research), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

Defending Rights & Dissent
Demand Progress
Electronic Frontier Foundation
Electronic Privacy Information Center
Fight for the Future
Free Press Action
FreedomWorks
Government Accountability Project
Immigrant Rights Clinic of the University of California at Irvine School of Law
Liberty Coalition
MediaJustice
Mijente
National Immigration Law Center
National Workrights Institute
New America's Open Technology Institute
Open MIC (Open Media and Information Companies Initiative)
OpenTheGovernment
Patient Privacy Rights
Privacy Times
Project on Government Oversight
Project South
Public Citizen
Restore The Fourth
TechFreedom
Tri-State Coalition for Responsible Investment