CENTER FOR DEMOCRACY & TECHNOLOGY

Submitted via email to PrivacyCommittee@hq.dhs.gov

Sandra Taylor, Designated Federal Officer
Data Privacy and Integrity Advisory Committee
Department of Homeland Security
245 Murray Lane SW
Mail Stop 0655
Washington, DC 20528

February 25, 2019

Re: DHS 2019-00001, DHS Data Privacy and Integrity Advisory Council

The Center for Democracy & Technology (CDT) is a non-profit advocacy organization working to promote democratic values online and in new, existing, and emerging technologies.[1] CDT pursues this mission by supporting laws, policies, and technical tools which empower users, protect privacy, and preserve individual rights online. CDT respectfully submits these comments in response to the request for public comment[2] from the Department of Homeland Security (DHS) Data Privacy and Integrity Advisory Council (DPIAC) on its draft report *Privacy Recommendations in Connection with the Use of Facial Recognition Technology.*[3]

In this case, a very limited tasking from the DHS Privacy Office to the DPIAC has resulted in a very limited set of recommendations. The tasking, and the DPIAC report, do not grapple with the glaring reality that Congress has not authorized Customs and Border Protection (CBP) to employ facial recognition technologies against U.S. citizens, but CBP is doing it nonetheless. Facial recognition technologies have also been shown to have inaccuracies, to result in discriminatory treatment of people with dark skin, and, when authorized to be used in a limited context, to spread to other contexts without adequate scrutiny.

[1] Center for Democracy & Technology, https://cdt.org/.

[2] Department of Homeland Security, Data Privacy and Integrity Advisory Committee, (Docket No. DHS-2019-0001) 84 Fed. Reg. 2898-2899 (Feb. 8, 2019), https://www.federalregister.gov/documents/2019/02/08/2019-01682/dhs-data-privacy-and-integrity-advisory-committee.

[3] Report 2019-XX of the DHS Data Privacy and Integrity Advisory Committee (DPIAC): Privacy Recommendations in Connection with the Use of Facial Recognition Technology, https://www.dhs.gov/sites/default/files/publications/DPIAC%20DRAFT%20Biometrics%20Recommendation%20Report%20v4_02.06.2018.pdf.

Facial recognition technology may prove to be a useful tool for law enforcement like CBP, however there are other significant associated privacy and civil liberties concerns abound. As CBP acknowledged, "facial recognition poses a unique set of privacy issues. Facial images can be captured at a distance, covertly, and without consent."[4] Safeguards are needed to prevent abuse. DHS failed to take advantage of the opportunity to task DPIAC with engaging with and provide guidance on these important issues.

Our comments on this report center on four points that highlight our broader concerns with CBP's use of facial recognition technology: 1) CBP has exceeded its legal mandate by employing facial recognition technology on U.S. citizens; 2) Facial recognition technology is discriminatory and inaccurate; 3) The biometric entry-exit system is prone to mission creep; and 4) Congressional oversight and legislation is needed to address these problems.

I. Customs and Border Protection has exceeded its legal mandate by employing facial recognition technology on U.S. citizens.

The U.S. Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is congressionally mandated to deploy a biometric entry-exit system to record non-citizens' arrivals and departures to and from the United States. Congress first mandated an automated entry-exit system that would create a record for every non-U.S. citizen departing from the United States and match it with the record for the non-U.S. citizen arriving to the United States.[5] The purpose of this system was to identify individuals who overstayed their visas. Later, the 9/11 Commission recommended the adoption of a "biometrics based entry-exit system" at the nation's borders in 2004.[6] Congress codified this recommendation and directed DHS to implement the "requirement for the collection of biometric exit data for all categories of individuals who are required to provide biometric entry data."[7] The purpose of this system was to identify terrorists, individuals traveling with fraudulent documents, and visa overstays.[8] Congress passed numerous pieces of legislation in the intervening years addressing the

[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, 10 (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018.pdf.

[5] Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, 110 Stat. 3009-546 (1996).

[6] National Commission on Terrorist Attacks upon the U.S., The 9/11 Commission Report, 389 (July 22, 2004), https://www.9-11commission.gov/report/911Report.pdf ("funding and completing a biometrics-based entry-exit system is an essential investment in our national security."). Further U.S. citizens were not included as collection targets, "[a] modern border and immigration system should combine a biometric entry-exit system with accessible files on visitors and immigrants, along with intelligence on indicators of terrorist travel." *Id*.

[7] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458 (2004).

[8] *Id*. ("Congress finds that completing a biometric entry and exit data system as expeditiously as possible is an essential investment in efforts to protect the United States by preventing the entry of terrorists.").

biometric entry-exit system. The categories of targeted individuals have included various categories of non-U.S. citizens and visa waiver participants.

Despite ample opportunity to do so, in the last 15 years Congress never explicitly instructed DHS, and later CBP,[9] to include U.S. citizens in biometric entry-exit.[10] Nonetheless, CBP has deployed facial recognition technology at U.S. land, sea and air ports of entry and collected biometrics from U.S. citizens.[11] The Traveler Verification Service (TVS), CBP's cloud based facial matching service, retains both U.S. citizens' and non-citizens' photos in TVS for up to 12 hours, photos of non-immigrants and green card holders are stored for up to 14 days in an Automated Targeting System database.[12] Photos of "in-scope travelers"[13] are retained in IDENT, the central DHS-wide system for storage and processing of biometric and associated biographic information for national security, for up to 75 years.[14] CBP's biometric entry-exit system should not include U.S. citizens. The inclusion of U.S. citizens was never legally authorized, and the practice must stop immediately.

It should also be noted that CBP has not been mandated to deploy facial recognition technology on non-U.S. citizens as a part of biometric entry-exit. Other less sensitive biometrics like fingerprints could

---

[9] Congress assigned responsibility of biometric entry-exit to CBP in 2013. Consolidated and Further Continuing Appropriations Act, 2013, Pub. L. No. 113-6, 127 Stat. 198 (2013).

[10] Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, 116 Stat. 543 (2002) (called for the installation of technology at ports of entry "to allow biometric comparison of all United States visas and travel and entry documents issued to aliens); ; Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004); Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007); Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009, Pub. L. No. 110-329, 122 Stat. 3574 (2008); Consolidated and Further Continuing Appropriations Act, 2013, Pub. L. No. 113-6, 127 Stat. 198 (2013).

[11] 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, 9 (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018.pdf.

[12] *Id*.

[13] According to the applicable regulations, "in-scope travelers" are any aliens other than those specifically exempted in 8 CFR 235.1(f). Exempted populations include Canadian citizens under section 101(a)(15)(B) of the Act who are not otherwise required to present a visa or be issued a form I-94 or Form I-95; aliens younger than 14 or older than 79 on the data of admission; aliens admitted A-1, A-2, C-3 (except for attendants, servants, or personal employees of accredited officials), G-1, G-2, G-3, G-4, NATO-1, NATO-2, NATO-3, NATO-4, NATO-5, or NATO-6 visas, and certain Taiwan officials who hold E-1 visas and members of their immediate families who hold E-1 visas unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to the requirements of paragraph (d)(1)(ii); classes of aliens to whom the Secretary of Homeland Security and the Secretary of State jointly determine it shall not apply; or an individual alien to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines it shall not apply. 8 CFR 235.1(f)

[14] 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, 9 (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018.pdf.

have been operationalized. As alluded to above, CBP even acknowledged this sensitivity in its PIA, "[a]s with all biometric modalities, facial recognition poses a unique set of privacy issues. Facial images can be captured at a distance, covertly, and without consent. Further, facial images are ubiquitous, and whereas individuals may take measures to avoid fingerprint and iris collection, there are fewer ways to hide one's face."[15] In deciding to pursue facial recognition, CBP appears to have chosen the biometric easier to collect without traveler resistance, even though facial recognition can have a greater long-term invasive impact than other biometrics. "[F]acial recognition has presented CBP with the best biometric approach because it can be performed relatively quickly, with a high degree of accuracy, and in a manner perceived as less invasive to the traveler (e.g., no actual physical contact is required to collect the biometric)."[16] Numbing people to the fact that they're engaging in a security process is not a valid excuse for collecting a biometric more sensitive than fingerprints.

II. Facial recognition technology is discriminatory and inaccurate.

Research has demonstrated that facial recognition technology is discriminatory and does not perform with sufficient rates of accuracy. With respect to discrimination, the technology does not perform equally across race and gender. Error rates, either false positives or false negatives occur with greater frequency for individuals with darker skin and for women. Indeed, inspector reports reviewing CBP's technology have also identified these concerns. A September 2018 Inspector General report stated that "[f]urther, due to missing or poor quality digital images, CBP could not consistently match individuals of certain age groups or nationalities"[17] and the 2017 match rate "limited biometric confirmation to only 85 percent of all passengers processed.[18]

Commercial facial recognition software has not fared better. There exists a rich body of research calling into question the ability of many algorithms to match faces with adequate certainty, and that again the software does not evenly distribute error rates across race and gender.[19] Amazon's Rekognition software for example has been repeatedly criticized for not adequately ensuring equal performance for women, and individuals with darker skin.[20]

---

[15] *Id*. at 10.

[16] *Id*. at 4.

[17] U.S. Dep't of Homeland Sec., Office of Inspector General, OIG-18-80, Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide, 6 (Sept. 21, 2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf.

[18] *Id*.

[19] Joy Buolamwini and Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research 81:1–15, 2018, 1 http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[20] Natasha Singer, *Amazon Is Pushing Facial Technology That a Study Says Could Be Biased*, N.Y. Times (Jan. 24, 2019), https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html.

Currently the remediation for an alert of a "non-match" at airports is a manual inspection by CBP officers of the traveler's passport. Concerns about misidentification should not compound the anxiety many communities of color already experience while traveling.[21] Furthermore the consequences of an error may change over time. We discuss below that this system's mission may expand, and an error may result in a custodial interrogation, or a traveler missing their flight.

Our concerns with accuracy and discrimination may be addressed over time. Facial recognition technology has demonstrably improved over the last few years.[22] Academics and activists have brought the issue to the attention of media outlets, the government, as well as developers. We have hope that the pressure they face from these stakeholders, as well as market incentives, will help resolve these issues. In the meantime though, CBP must have its systems audited for discrimination and accuracy and provide the results to the public. If the system cannot operate at adequate levels of accuracy balanced across race and gender, CBP should not employ the technology.

III. The biometric entry-exit system is prone to mission creep.

Biometric entry-exit was authorized only for non-U.S. citizens, and its purpose was to identify non-citizen terrorists, immigration fraud and visa overstays. However, the deployment of biometric technology at airports seems to be expanding to all travelers, including citizens, and including individuals who are not even crossing the U.S. border. Individuals living in and traveling within the United States will increasingly be subjected to government use of facial recognition technology. TSA is partnering with CBP in implementing biometric entry-exit, and in September 2018 released a report *TSA Biometrics Roadmap for Aviation Security & the Passenger Experience*, which stated that TSA plans to collect the facial biometric images for travelers enrolled TSA PreCheck, and seeks to incorporate "voluntary" biometric screening for all other travelers as well.[23]

---

[21] *See e.g.,* Michael Luongo, Traveling While Muslim Complicates Air Travel, N.Y. Times (Nov. 6, 2016), https://www.nytimes.com/2016/11/08/business/traveling-while-muslim-complicates-air-travel.html; Spencer Ackerman, *TSA screening program risks racial profiling amid shaky science – study*, The Guardian (Feb. 8, 2017), https://www.theguardian.com/us-news/2017/feb/08/tsa-screening-racial-religious-profiling-aclu-study; Susan Ferriss, *Nigerian American's treatment at Dulles Airport is subject of federal lawsuit,* WaPo (Dec. 11, 2018), https://www.washingtonpost.com/local/immigration/nigerian-americans-treatment-at-dulles-airport-is-subject-of-federal-lawsuit/2018/12/10/f878038a-fc9c-11e8-ad40-cdfd0e0dd65a_story.html?noredirect=on&utm_term=.7bdb5c12f182.

[22] *NIST Evaluation Shows Advance in Face Recognition Software's Capabilities,* NIST (November 30, 2018), https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities.

[23] Transportation Security Administration, TSA Biometrics Roadmap For Aviation Security & the Passenger Experience, 12-13, (Sept. 2018), https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

Given the money, time and resources expended on biometric entry-exit thus far there will be a temptation to expand the uses to which facial recognition data is put, and those uses will extend beyond the goal of controlling entry and exit. This is already occurring:

> "CBP collects information under this process in order to verify the identities of travelers departing the United States; however, CBP uses border crossing information more broadly. CBP creates entry and exit records primarily in support of its mission to facilitate legitimate travel and enforce immigration laws, which include activities related to counterterrorism and immigration enforcement. CBP may share information with federal, state, and local authorities, which may be authorized to use the information for purposes beyond the scope of CBP's mission."[24]

Further, the government may wish to expand the system from identity-verification to lookout systems for warrants, or images of individuals who are perceived as persons of interest. Warrant databases as well as criminal record databases are error prone.[25] Connecting the two would exacerbate the negative experiences of communities of color who are already disproportionality represented in these systems due to historic racial disparities in policing.

Biometric collection was initially justified for security purposes. CBP now highlights efficiency and ease of air travel as a new justification for its collection. We already see evidence of mission creep. Airports should also not become one-stop security lookouts.

IV. Congressional oversight and legislation is needed.

Congressional oversight and legislation are needed to safeguard individuals from the privacy and civil liberties harms arising from the use of facial recognition technology. In October 2018 Congress took an important first step. Congress passed the FAA Reauthorization Act of 2018 which calls for TSA to consult with the Commissioner of CBP and prepare a report for the appropriate committees of Congress on the use of biometric technology to identify travelers. The report will arm Congress with

---

[24] 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, 13 (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018.pdf.

[25] *See e.g.*, Alen Feur, *Cleared of a Crime but Hounded by a Warrant*, N.Y. Times (March 28, 2016), https://www.nytimes.com/2016/03/29/nyregion/cleared-of-a-crime-but-hounded-by-a-warrant.html; Legal Action Rap Center, The Problem of RAP Sheet Errors: An Analysis (July 2014), https://lac.org/wp-content/uploads/2014/07/LAC_rap_sheet_report_final_2013.pdf; Elizabeth Joh, *Wrongful Arrest by Software*, Slate (Dec. 13, 2016), nhttp://www.slate.com/articles/technology/future_tense/2016/12/software_problems_are_leading_to_wrongful_arrests.html.

valuable information to guide its oversight as well legislation regulating the technology. Specifically, the report will provide assessments on the operation and security impact of using biometric technology to identify travelers, the potential effects on privacy of the expansion of the use of biometric technology and related methods to mitigate risks to privacy, and methods to analyze and address matching errors related to race, gender or race associated with biometric technology like facial recognition technology. With respect to the biometric entry-exit program specifically, assessments must be provided on error rates and the effects of biometric technologies to ensure that such technologies do not unduly burden categories of travelers, such as certain races, genders, or nationalities. CBP and TSA are to provide information on the results of audits of the technology's performance including assessments on performance with respect to race, gender and age. The report must also include "an assessment of what percentage of the detection of fraudulent identifications could have been accomplished using conventional methods," and the effects on privacy of the use of biometric technologies.[26]

This report will arm Congress with vitally needed information to evaluate some of the concerns we described above. Congressional oversight and legislation may result in:

- Mandated sufficient resources to ensure that U.S. citizens are excluded from biometric entry-exit and processed efficiently
- A Congressionally-ordered moratorium on the use of facial recognition technology by CBP until non-discrimination and accuracy goals are met
- An affirmative ban on connecting external databases like warrant databases with TVS
- An affirmative ban on mandating biometric identification for domestic air travel
- Where biometric identification is permitted, a determination to limit use of facial recognition as the biometric identifier.

The rollout of facial recognition by DHS entities is still in its nascent stages and Congress is still in a position to assess whether the benefits of using facial recognition technology are outweighed by the accompanying privacy and security risks. Perhaps an assessment may demonstrate that "biometric entry-exit" is a solution in search of a problem, and that biographic data is more than sufficient to address issues of visa overstay. Regardless, CBP's use of facial recognition technology is an issue of immediate concern that demands Congressional investigation, and subsequent regulation.

* * *

As our comment indicates, we have many concerns with CBP's use of facial recognition technology. CBP has expanded its biometric entry-exit system to U.S. citizens without congressional authorization,

[26] FAA Reauthorization Act of 2018, Pub. L. No. 115-254 (2018).

and the program is at risk of further expansion, as we detailed above. Furthermore, the facial recognition technology in use today is discriminatory, and inaccurate. We are hopeful Congress will take up this important issue.

Respectfully submitted,

Center for Democracy & Technology