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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

DEPARTMENT OF HOMELAND SECURITY DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

DHS Data Privacy and Integrity Advisory Committee; Committee Management; Notice of Federal Advisory Committee Meeting

[Docket No. DHS–2018–0066]

December 10, 2018

By notice published November 9, 2018 the Department of Homeland Security ("DHS") notified the public of an upcoming meeting of the DHS Data Privacy and Integrity Advisory Committee ("DPIAC") on December 10, 2018 and invited comments.[1] The DPIAC "provides advice at the request of the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that relate to personally identifiable information, as well as data integrity and other privacy-related matters."[2] The proposed agenda for the meeting includes a privacy office update, as well as an update on the Biometric Travel Security Initiative and a subcommittee report on biometric facial recognition.[3]

[1] *DHS Data Privacy and Integrity Advisory Committee,* 83 Fed. Reg. 56,089-090 (Nov. 9, 2018) https://www.gpo.gov/fdsys/pkg/FR-2018-11-09/pdf/2018-24597.pdf.
[2] DHS, *Data Privacy and Integrity Advisory Committee*, https://www.dhs.gov/privacy-advisory-committee (last visited Dec. 4, 2018).
[3] DHS, *Agenda: DHS Data Privacy and Integrity Advisory Committee, Monday Dec. 10, 2018*, https://www.dhs.gov/sites/default/files/publications/DPIAC%20Public%20Meeting_FINAL%20Agenda_11.05.2018%20%28002%29.pdf (last visited Dec. 4, 2018).

EPIC urges the DPIAC to advise the CBP to 1) halt the implementation of its facial recognition program until Congress passes proper regulatory safeguards to protect against the misuse of facial recognition and other biometric surveillance techniques; and 2) conduct notice-and-comment rulemaking on the biometric entry/exit program and any other implementation of facial recognition that impacts American citizens.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and protect privacy, the First Amendment, and constitutional values.[4] EPIC has a particular interest in preserving the right of people to engage in First Amendment protected activities without the threat of government surveillance.

I. CBP's Biometric Entry/Exit Program

Without legal authority or the opportunity for public comment, the U.S. Customs and Border Protection has deployed facial recognition technology in U.S. airports, sea ports, and land ports of entry and collected biometric identifiers from American travelers.[5] Further, the agency plans to "incrementally deploy biometric capabilities across all modes of travel — air, sea, and land — by fiscal year 2025."[6] According to the most recent Privacy Impact Assessment ("PIA"), the Traveler Verification Services ("TVS") retains both U.S. citizens' and non-citizens' photos in the TVS Cloud Matching Service for up to 12 hours, photos of non-immigrant aliens and lawful permanent residents are stored for up to 14 days in an Automated Targeting System database, and photos of "in-scope travelers"[7] are retained in IDENT for up to 75 years.[8] CBP integrates

[4] EPIC, *About EPIC* (2018), https://epic.org/epic/about.html.
[5] U.S. Customs and Border Protection, Biometrics, https://www.cbp.gov/travel/biometrics (last visited Dec. 5, 2018) [hereinafter CBP Biometrics website].
[6] OIG Report, *supra* note 2, 7.
[7] "In-scope travelers" are any aliens other than those specifically exempted in 8 CFR 235.1(f).
[8] 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_2.pdf [hereinafter TVS Nov. 2018 PIA].

information from flight manifests provided by airlines with photographs obtained from State Department databases to prepare "galleries" to match with photos captured at ports of entry.[9] "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[.]"[10] CBP uses its own equipment as well as that of private firms, other government agencies, and foreign governments to capture face images.[11]

This vast biometric collection program exposes Americans and other travelers to substantial privacy risks. The problem begins when the State Department, without legal authority, transferred facial images collected for passport applications to the CBP. This largely immutable biometric information is then used to conduct government surveillance unrelated to the purpose for which the photos were collected. The legislation this program purports to implement does not authorize this activity,[12] and there is currently no federal legislation to regulate the use of facial recognition or other biometric surveillance techniques in these circumstances. *As such, the DPIAC should recommend that the program cease immediately*.

II. DPIAC's privacy recommendations are flawed and fail to address the full risks posed by CBP's use of facial recognition.

The draft report begins with the faulty premise that "one-to-few" facial recognition use at ports of entry is necessary to national security.[13] The U.S. is the only country in the world to

[9] 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].
[10] TVS Nov. 2018 PIA, 5.
[11] TVS Nov. 2018 PIA, 7-8.
[12] Letter from Sens. Edward J. Markey and Mike Lee to Sec'y Kirstjen Nielsen, Dep't of Homeland Sec., 1-2 (Dec. 21, 2017), *available at* https://www.markey.senate.gov/imo/media/doc/DHS%20Biometrics%20Markey%20Lee%20.pdf.
[13] Draft of Report 2018-01 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/Report%202018-01-Draft%20Report%20on%20Privacy%20Recommendations%20in%20Connection%20with%20the%20Use%20of%20Facial%20Recognition%20Technology.pdf (last visited Dec. 5, 2018) [hereinafter DPIAC Draft Report].

believe that facial recognition and image retention is necessary for airport security. In Europe[14] and even China,[15] a photo ID is presented for an instantaneous match against an image displayed or stored on the ID itself. Israel's biometric entry program is voluntary, and matches information supplied by passengers that is either stored in a passport chip or provided directly on a one-off basis.[16] In Malaysia, passengers have the option to enroll in the program by submitting their Malaysian ID card or passport to be used for facial recognition by a specific airline.[17] Australia's program operates similarly.[18]

Unlike the U.S., other governments do not create a "gallery" by pulling photos obtained by the government for other purposes. The legislation this program purportedly implements authorized the use of biometrics to only identify visa overstays, track immigration matters, and match visa waiver recipients against watch lists. 8 U.S.C. § 1365a(b); 8 U.S.C. § 1365b(g), (h); 8 U.S.C. § 1187(i)(1), (2). No mention of the collection of U.S. citizens' biometric information appears in these acts of legislation.

The report fails to address the fundamental problem of using photos collected for one purpose (to apply for a visa or passport) and subsequently using those photos for another purpose

[14] Northern Ireland Direct Government Services, *Using ePassport gates at airport border control*, https://www.nidirect.gov.uk/articles/using-epassport-gates-airport-border-control (last visited Dec. 6, 2018); Arvind Jayaram, *UK's ePassport gate immigration facility to be extended to Singaporeans from summer of 2019*, Straits Times, Dec. 4, 2018, https://www.straitstimes.com/world/europe/uks-epassport-gate-immigration-facility-to-be-extended-to-singaporeans-from-summer-of; Zak Doffman, *Opening Of UK ePassport Gates Is Great News For US Travelers*, Forbes, Oct. 30, 2018, https://www.forbes.com/sites/zakdoffman/2018/10/30/opening-of-uk-epassport-gates-is-great-news-for-us-travelers/.

[15] Taylor Bragg, *Facial recognition is widely adopted in China's airports*, Techwire Asia, Apr. 11, 2018 https://techwireasia.com/2018/04/facial-recognition-is-widely-adopted-in-chinas-airports/.

[16] Yasmin Yablonko, *Expert: Israeli airport passport machines vulnerable*, Globes, Apr. 1, 2018, https://en.globes.co.il/en/article-expert-israeli-airport-passport-machines-vulnerable-to-cyberattack.

[17] Lainey Loh, *AirAsia's facial recognition system: Convenience or concern?*, Travel Wire Asia. Feb. 7, 2018, https://travelwireasia.com/2018/02/airasias-facial-recognition-system-convenience-concern/.

[18] Qantas, Facial Recognition, https://www.qantas.com/us/en/travel-info/travel-advice/facial-recognition.html (last visited Dec. 6, 2018); Sarah Clark, *Qantas uses NFC to pre-enrol passengers for biometric boarding service*, NFC World, Nov. 20, 2018, https://www.nfcworld.com/2018/11/20/358573/qantas-uses-nfc-to-pre-enrol-passengers-for-biometric-boarding-service/; Rohan Pearce, *Sydney Airport collaborates with Qantas for facial recognition trial*, Computerworld, July 5, 2018, https://www.computerworld.com.au/article/643375/sydney-airport-collaborates-qantas-facial-recognition-trial/.

(to conduct a border check). While the most recent PIA for the program assures U.S. citizens that their images captured by CBP will be deleted after the prescribed time limit,[19] the transfer of the photos obtained by the State Department to the CBP lacks legal authority and is in violation of the federal Privacy Act.[20]

And this program is not voluntarily. There is no way to opt-out of the CBP facial recognition program. EPIC knows for a fact that the procedures described in the DPIAC report regarding the alternative method of screening (i.e. a manual check of travel documents) is in fact not the agency's practice. And the underlying problem remains: personal data is automatically transferred from the State department to another agency without legal authority. By the time the passenger attempts to assert the right to "opt out," the passenger's photo has already been pulled from the State Department database into a gallery to be used by DHS for facial recognition.

Further, as the report notes, at land ports of entry where passengers are photographed in vehicles at-speed, there is a high risk that passengers will not even know the photo capture and matching is taking place.[21] This risk is amplified by the fact that CBP plans to create galleries of images of "frequent crossers."[22] So, Americans legally crossing the border may have their images captured while inside their vehicles and then put into a database to track their movements.

In a mere two paragraphs, the report dismisses the well-documented disparity of facial recognition accuracy along age, racial, ethnic, and gender lines, citing a Microsoft blogpost as its only evidence that facial recognition technology has improved.[23] Recent research confirms that

[19] TVS Nov. 2018 PIA, 9.
[20] *See* 5 U.S.C. § 552a(b).
[21] DPIAC Draft Report, 5.
[22] TVS Nov. 2018 PIA, 5.
[23] DPIAC Draft Report, 9.

this is still a major issue.[24] The DPIAC's draft issues no recommendation to address this problem, despite the fact that in September 2018, the DHS Office of Inspector General raised the concern that "CBP could not consistently match individuals of certain age groups or nationalities" and the 2017 match rate was a "low 85-percent[.]"[25] The report's treatment of this automated discrimination is woefully inadequate. *Discrimination through automation cannot be tolerated, so even a small disparity in effectiveness is sufficient reason to shut the program down.*

III. With no federally mandated safeguards in place, Americans will be increasingly subject to facial recognition without their consent and without their knowledge

There is no federal regulation or legislation preventing DHS from using facial recognition technology it develops, the photos it has captured, and the databases it creates as part of this program for other purposes. Facial recognition is the biometric identifier most easily used for mass surveillance; indeed, as DPIAC's report notes, "facial recognition systems can be used to identify people in photos, videos, or in real-time."[26] Facial recognition software paired with cameras aimed toward public spaces in China is used to censor and shame individuals as part of a campaign for social control through mass surveillance.[27] The infrastructure already exists in the U.S. to conduct similar mass surveillance through the use of facial recognition, and the U.S. government's slide toward these techniques runs directly against American values.

The Secret Service has already begun use of facial recognition technology to monitor parts of the White House and surrounding area, including "an open setting, where individuals are

[24] 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.
[25] OIG Report, DHS OIG HIGHLIGHTS.
[26] DPIAC Draft Report, 2.
[27] Simon Denyer, *China's Watchful Eye*, Wash. Post, Jan. 7, 2018, https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/; Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, N.Y. Times, July 8, 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

free to approach from any angle."[28] The PIA for this program states, "individuals who do not wish to be captured by White House Complex CCTV and cameras involved in this pilot may choose to avoid the area."[29] That is, of course, absurd as few people will even be aware they are subject to facial recognition. The use of facial recognition technology at a site where hundreds of demonstrations, vigils, protests, and marches occur annually[30] also raised particular alarm for the protection of the First Amendment. As we warned the DC City Council in 2008:

> There is also a rapid evolution underway that makes surveillance far more intrusive than most people understand. Already you are seeing the use of facial recognition that will make it possible to identify people in public places. People enjoy privacy in public spaces because of anonymity. These new techniques are intended precisely to destroy that very real form of privacy.[31]

The DPIAC must recommend that DHS immediately cease implementation of this program until Congressional legislation sets out clear limitations. Once federal safeguards are established, any implementation of facial recognition by DHS that impacts large amounts of citizens, including CBP's biometric entry/exit program, should be required to conduct a notice-and-comment rulemaking.

IV. Conclusion

For the foregoing reasons, CBP's unauthorized and unregulated implementation of facial recognition technology at ports of entry creates grave privacy and security risks. Accordingly, the DPIAC should advise DHS to immediately end the use of facial recognition as part of this program.

---

[28] DHS, Privacy Impact Assessment for the Facial Recognition Pilot, DHS/USSS/PIA-024, 2 (Nov. 26, 2018) https://www.dhs.gov/sites/default/files/publications/privacy-pia-usss-frp-november2018.pdf [hereinafter Secret Service PIA].
[29] Secret Service PIA, 4.
[30] White House Historical Association, President's Park: A History of Protest at the White House, https://www.whitehousehistory.org/presidents-park-a-history-of-protest-at-the-white-house.
[31] Marc Rotenberg, Testimony to Comm. On Public Safety and the Judiciary of the D.C. Council on "Video Interoperability for Public Safety," 2 (June 2, 2008), https://epic.org/privacy/surveillance/dccouncil_cctv060208.pdf.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President and Executive Director

/s/ Jeramie D. Scott
Jeramie D. Scott
EPIC National Security Counsel

/s/ Ellen Coogan
Ellen Coogan
EPIC Domestic Surveillance Fellow