epic.org ELECTRONIC PRIVACY INFORMATION CENTER

Statement of Jeramie D. Scott

Senior Counsel, Electronic Privacy Information Center (EPIC)

Hearing on "Assessing CBP's Use of Facial Recognition Technology"

Before the

House Committee on Homeland Security
Subcommittee on Border Security, Facilitation, & Operations
United States House of Representatives

July 27, 2022

Chairwoman Barragán, Ranking Member Higgins, and members of the Subcommittee, thank you for holding this hearing and for the opportunity to testify today on CBP's use of facial recognition technology. My name is Jeramie Scott, Senior Counsel at the Electronic Privacy Information Center, or simply EPIC. EPIC is an independent nonprofit research organization in Washington, DC, established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.

EPIC has long history of work on facial recognition and the privacy and civil liberties issues the technology raises, particularly with respect to Custom and Border Protection's (CBP's) use of facial recognition.[1] The attention is warranted and necessary because facial recognition is a dangerous surveillance technology whose risks increase as the government expands its implementations in any form, including for identity verification. The technology poses serious threats to our privacy, our civil liberties, our constitutionally protected rights, and our democracy. Facial recognition has accuracy and bias issues that are most likely to impact marginalized groups. But, even a perfectly accurate and unbiased facial recognition system poses fundamental risks to a democratic society when widely deployed.

In my testimony I will discuss the issues with facial recognition in general, CBP's use of facial recognition as part of its Biometric Entry-Exit program, the many issues with this program, and the threat CBP's use of facial recognition poses to individuals and our society.

[1] *See e.g.*, Comments of EPIC to U.S. Customs and Border Protection Dept., Collection of Advance Information From Certain Undocumented Individuals on the Land Border, Docket ID: USCBP-2021-0038 (Nov. 29, 2021), https://epic.org/wp-content/uploads/2021/11/EPIC-Comments-DHS-Advance-Collection-Photos-Border-Nov-2021.pdf, Comments of EPIC to the Transportation Security Admin., Intent to Request Revision of Agency Information Collection Activity Under OMB Review: TSA PreCheck, Docket ID: TSA-2013-0001 (June 22, 2020), https://epic.org/apa/comments/EPIC-TSA-PreCheck-FRT-Comment-June2020.pdf; Comments of EPIC to the Dept. of Homeland Security, Agency Information Collection Activities: Biometric Identity, Docket No. 1651-0138 (Jul. 24, 2018), https://epic.org/apa/comments/EPIC-CBP- Vehicular-Biometric-Entry-Exit-Program.pdf; EPIC v. CBP (Biometric Entry/Exit Program), https://epic.org/foia/dhs/cbp/biometric-entry-exit/default.html (EPIC obtained a report which evaluated iris imaging and facial recognition scans for border control); EPIC Statement to U.S. House Comm. on Homeland Security, "Border Security, Commerce and Travel: Commissioner McAleenan's Vision for the Future of CBP" (Apr. 24, 2018), https://epic.org/testimony/congress/EPIC-HHSC-CBP-Apr2018.pdf; Comments of EPIC to the Dept. of Homeland Security, Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Citizenship and Immigration Services—018 Immigration Biometric and Background Check (IBBC) System of Records, Docket Nos. DHS-2018-0002 and DHS-2018-0003 (Aug. 30, 2018), https://epic.org/apa/comments/EPIC-DHS-Immigration-Biometric- Database.pdf; Comments of EPIC to the Dept. of Homeland Security, Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States (Dec. 21, 2020), https://epic.org/documents/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the- united-states/.

I. Facial Recognition Technology is Inaccurate and Biased

Facial recognition systems have been deployed by both government agencies and private companies with little to no oversight, despite many questions regarding their effectiveness.[2] A 2019 National Institute of Standards and Technology ("NIST") study of facial recognition tools—which are typically "AI-based"[3]—found that the systems were up to 100 times more likely to return a false positive for a non-white person than for a white person.[4] Specifically, NIST found that "for one-to-many matching, the team saw higher rates of false positives for African American females," a finding that is "particularly important because the consequences could include false accusations."[5] A separate study by Stanford University and MIT, which looked at three widely deployed commercial facial recognition tools, found an error rate of 34.7% for dark-skinned women compared to an error rate of 0.8% for light-skinned men.[6] A review of Rekognition—an Amazon-owned facial recognition system marketed to law enforcement—revealed indications of racial bias and found that the system misidentified 28 members of U.S. Congress as convicted criminals.[7] Yet CBP is relying on this flawed technology to protect our borders.

II. CBP's Biometric Entry-Exit Program

CBP has implemented one of the largest deployments of facial recognition technology in the country through its Biometric Entry-Exit program. According to CBP, 238 airports use facial recognition for entry and 32 airports have facial recognition deployed for exit.[8] Another 13 seaports use facial recognition and almost all the processing facilities for pedestrians and buses along the northern and southern border deploy facial recognition.[9] And since 2017, CBP has used

[2] David Freeman Engstrom, Daniel E. Ho, Catherine M. Sharkey, & Mariano-Florentino Cuéllar, *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies* 6 (Feb. 2020), https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf.

[3] Nat'l Inst. Standards & Tech., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* 14 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[4] Nat'l Inst. Standards & Tech., *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

[5] *Id.*

[6] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* Proceedings of Machine Learning Research 81:1–15 (2018), https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/.

[7] Russell Brandom, *Amazon's facial recognition matched 28 members of Congress to criminal mugshots*, The Verge (July 26, 2018), https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition.

[8] CBP, *Introducing Biometric Facial Comparison*, https://biometrics.cbp.gov.

[9] *Id.*

facial recognition on over 100 million travelers.[10] Further, the agency has "the ultimate goal of implementing a comprehensive biometric entry-exit system nationwide"[11]

The backbone of CBP's Biometric Entry-Exit program is the agency's Traveler Verification Service (TVS). TVS is a cloud-based information technology that handles the actual facial recognition comparison.[12] TVS uses biometric templates created from existing photographs obtained from several sources including U.S. passport and U.S. visa photos from the State Department, images captured during entry inspection, and other encounters with the Department of Homeland Security where a photograph is taken.

CBP leverages these photographs to build specific galleries of photographs for entry and exit points.[13] For example, for commercial flights, where CBP knows ahead of time who will be on a given flight, the agency builds a gallery of photos based on expected passengers. At the borders where people may be crossing on foot or in their own vehicles, "CBP will build galleries using photographs of "frequent" crossers for that specific port of entry, taken at that specific port of entry, that become part of a localized photographic gallery."[14] These photo galleries are used by TVS to create the face prints or biometric templates used for facial recognition identification.[15] Where CBP has implemented the Biometric Entry-Exit program, the agency applies facial recognition identification to all travelers, including U.S. citizens.[16] The implementation of the Biometric Entry-Exit program has been a slow and long process—one fraught with issues in the program's administration, lack of clear rationale, and questionable authority. Despite the issues, CBP submitted a Notice of Proposed Rulemaking in November 2020 to make permanent the agency's implementation of a biometric entry-exit system that utilizes facial recognition identification. The CBP's efforts to expand the use of facial recognition through the Biometric Entry-Exit program lacks the necessary authority to collect biometrics on U.S. citizens, unnecessarily expands the program beyond its apparent purpose, and creates an unregulated facial recognition infrastructure likely to be exploited by the government in the future.

III. Congress never gave CBP the legal authorization to collect biometric data from US citizens

CBP lacks the legal authorization to collect biometric data from U.S. citizens. As part of its implementation of "an integrated automated entry and exit data system . . . of aliens entering

[10] CBP, *Introducing Biometric Facial Comparison*, https://biometrics.cbp.gov.
[11] *Notice of proposed rulemaking on "Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States,"* 85 Fed. Reg. 74162, 74163 (Nov. 19, 2020), https://www.govinfo.gov/content/pkg/FR-2020-11-19/pdf/2020-24707.pdf.
[12] DHS, *Privacy Impact Assessment for the Traveler Verification Service* 4-6 (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/PIA%20for%20Traveler%20Verification%20Service.pdf (hereinafter ("PIA".)
[13] *Id.* at 5**.**
[14] *Id.* at 5.
[15] *Id.* at 6.
[16] U.S. citizens are able to opt-out of facial recognition identification but as described below the opt-out is not meaningful and has not always been honored by CBP agents.

and departing the United States," CBP has proposed collecting not only biometric information from noncitizens crossing the U.S. border, but also biometric information from U.S. citizens.[17] In support of its decision to collect this information, CBP reports that it had identified several "imposters" who had attempted to enter the United States using U.S. travel documents that did not belong to them.[18] In addition, CBP justifies the collection of biometric information from U.S. citizens by stating that photos of U.S. citizens used for face verification would only be stored for 12 hours after confirmation of a person's identity.[19]

CBP's justifications for collecting biometric information from U.S. citizens are insufficient, however, as Congress has only authorized CBP to deploy a biometric entry/exit program for noncitizens. Evidence that Congress limited its authorizations to noncitizens is found in numerous prior statutes establishing an entry/exit system—some of which are cited by CBP itself in its notice of proposed rulemaking, and none of which mention U.S. citizens. As authority for its proposed rule to collect the biometric data, CBP relies on the 2016 Consolidated Appropriations Act.[20] In that statute, Congress instructed the DHS Secretary to submit to Congress a plan to "implement[] . . . the biometric entry and exit data system described in section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004" and allocated funding towards that implementation.[21]

Context and statutory language make it clear that Congress never intended to authorize CBP to collect biometric information from citizens. For one, the Intelligence Reform and Terrorism Prevention Act referenced in the 2016 Appropriations Act applies only to noncitizens. The statute authorized collecting biometric exit data for "all categories of individuals who are required to provide biometric entry data, regardless of the port of entry where such categories of individuals entered the United States."[22] After this authorization, the subsequent section of the Act grants the DHS Secretary with the authority "to integrate all databases and data systems that process or contain information *on aliens* . . ."[23]

Moreover, all existing statutes that identify categories of people "required to provide biometric entry data" apply only to noncitizens.[24] These statutes include the "Illegal Immigration Reform and Immigrant Responsibility Act of 1996," in which Congress authorized collection of biometrics at the border from noncitizens crossing the U.S. border.[25] It also includes a statute passed in 2007, which required DHS to "establish an exit system" that includes biometric

[17] Collection of Biometric Data from Aliens upon Entry to and Departure from the United States, 85 Fed. Reg. 74,162 (Nov. 19, 2020); *see also* Collection of Biometric Data from Aliens upon Entry to and Departure from the United States; Re-Opening of Comment Period, 86 Fed. Reg. 8,878 (Feb. 10, 2021).
[18] 85 Fed. Reg. at 74, 167.
[19] *Id.* at 164.
[20] *Id.* at 74, 164-65.
[21] Pub. L. 114-113, 129 Stat. 2242, 2493, 3006 (2015).
[22] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 7208(d) (2004).
[23] *Id.* at § 7208(e) (emphasis added).
[24] *See* Harrison Rudolph et al., Not Ready for Takeoff: Face Scans at Airport Departure Gates, Geo. Ctr. on Privacy & Tech 7 (2017).
[25] H.R. Rep. No. 104-828 (1996) § 104 (amending 8 U.S.C. 1101(a)(6)); *see also* 8 U.S.C. 1101(a)(6).

collection for "every alien participating in the visa waiver program."[26] In fact, none of the entry-exit system statutes that CBP cites to justify its proposed rule mention U.S. citizens.[27]

IV. CBP has failed from the beginning of program to provide a reasonable justification for the expansion of the Biometric Exit program

From the start, CBP's justifications for implementing the Biometric Exit system have changed and expanded. Recording biometric data from non-citizens leaving the United States was briefly mentioned as a recommendation of the 9/11 Commission.[28] The 9/11 Commission only discussed the possibility of biometric border screening in passing and did not explain how such a system could meaningfully improve national security.

In the years after the 9/11 Commission Report, DHS moved slowly to implement a biometric exit system, in part because DHS components could identify no rationale for the program. In 2012, an internal DHS Science and Technology Directorate evaluation found that "significant questions remained" on "(3) the additional value biometric air exit would provide compared with the current biographic air exit process, and (4) the overall value and cost of a

[26] Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53, § 711(i)(1)-(2), 121 Stat. 266, 345 (2007).

[27] In its November 2020 notice of proposed rulemaking, Collection of Biometric Data from Aliens upon Entry to and Departure from the United States, 85 Fed. Reg. 74,162, 74,165 (Nov. 19, 2020), CBP cites to the following statutory authorities "requir[ing] DHS to take action to create an integrated entry-exit system." Each of these statutes—except for the last statute, which is the general statute establishing the CBP agency—do not mention U.S. citizens in relation to their discussion of the entry/exit system:

- Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104-828, 110 Stat. 3009-546 (authorizing collection of biometric identification from noncitizens crossing the U.S. border);
- Section 205 of the Visa Waiver Permanent Program Act of 2000, Public Law 106-396, 114 Stat. 1637, 1641 (calling for the implementation of "a fully automated entry and exit control system that will collect a record of arrival and departure *for every alien*" under the visa waiver program (emphasis added);
- Section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107-56, 115 Stat. 272, 353 (instructing the Executive Branch to "expedite" implementation of the entry/exit data system specified in the Illegal Immigration Reform and Immigrant Responsibility Act of 1996);
- Section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), Public Law 107-173, 116 Stat. 543, 552 (requiring federal officials to "establish a database containing the arrival and departure data from machine-readable visas, passports, and other travel and entry documents *possessed by aliens*" (emphasis added));
- Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, 121 Stat. 266, 338 (concerning "modernization of the visa waiver program");
- Section 802 of the Trade Facilitation and Trade Enforcement Act of 2015, Public Law 114-125, 130 Stat. 122, 199 (6 U.S.C. 211(c)(10)) (establishing CBP).

[28] National Commission on Terrorist Attacks upon the U.S., The 9/11 Commission Report 387-390 (July 22, 2004), available at https://www.9-11commission.gov/report/911Report.pdf (hereinafter "9/11 Commission Report").

biometric air exit capability."[29] After responsibility for Biometric Exit was assigned to CBP in 2013, the agency settled on a rationale of using the program to prevent visa overstays, but at the time there was no evidence that collecting biometrics on departure from the US would address this problem.[30] CBP has since been able to quantify the effectiveness of using only biographic identifiers for non-citizens exiting the US, stating that collecting biographic information is "accurate for approximately 98-99% of foreign travelers who entered under a visa (or the visa waiver program)."[31]

Although CBP has forged ahead in implementing Biometric Exit, agency analysts are skeptical of the value of the program to this day. In 2017, a senior DHS official could not tell the DHS Data Privacy and Integrity Advisory Committee how Biometric Exit would improve the immigration system and claimed vague "immigration and counterterrorism benefits."[32] But CBP has repeatedly disclaimed any possible counterterrorism benefits of Biometric Exit.[33] A 2020 report from the Homeland Security Advisory Committee described biographic data collection as sufficient for visa overstay enforcement and objected that, "even if a marginal case could be made for biometric exit, it has never been evaluated on a cost benefit basis."[34] However, CBP's response to this longstanding and cogent analysis makes little sense. In the face of purported difficulties with separating out U.S. citizens from Biometric Exit, the agency threw up its hands

[29] As summarized in U.S. Government Accountability Office, GAO-16-358T, Actions Needed by DHS to Address Long-Standing Challenges in Planning for a Biometric Exit System: Before the Subcommittee on Immigration and the Nat'l Interest, Committee on the Judiciary, U.S. Senate, 115th Cong. 8 (Jan. 20, 2016) (Statement of Rebecca Gambler, Director Homeland Sec. and Justice), https://www.gao.gov/assets/680/674704.pdf.

[30] *See* Written testimony of U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement for a House Committee on Homeland Security, Subcommittee on Border and Maritime Security hearing titled "Fulfilling A Key 9/11 Commission Recommendation: Implementing Biometric Exit" (Sept. 23, 2013), https://www.dhs.gov/news/2013/09/26/written-testimony-cbp-and-ice-house-homeland-security-subcommittee-border-and.

[31] Homeland Security Advisory Council (HSAC), Subcommittee on Biometrics, Final Report of the Biometrics Subcommittee at 30 (Nov. 12, 2020), https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf.

[32] U.S. Department of Homeland Security, DPIAC Meeting Minutes 5 (Sept. 19, 2017), https://www.dhs.gov/sites/default/files/publications/DPIAC%20Meeting%20Minutes-Sept%2019%202017.pdf ("Q(LG): does this solve your problem with overstaying/ terrorism? A(MH): not our role to question duly passed laws from Congress. We think it gives us immigration and counterterrorism benefits. We trust in Congress and 9/11 Commission.").

[33] Homeland Security Advisory Council (HSAC), Subcommittee on Biometrics, Final Report of the Biometrics Subcommittee at 30 (Nov. 12, 2020), https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf ("Unlike biometric entry, biometric exit has little to do with preventing terrorist attacks." and "Neither CBP nor DHS has ever assessed that a biometric exit capability is needed for national security or counter-terrorism purposes.").

[34] *Id.*

and claimed that imposing facial recognition on both citizens and non-citizens was the only solution.[35]

V. CBP has failed to properly administer its Biometric Entry-Exit program

CBP's implementation of the Biometry Entry/Exit program has consistently fallen below baseline standards for privacy articulated in DHS's Fair Information Privacy Principles (FIPPs).[36] The FIPPs set benchmarks for data collection and use that DHS must meet to comply with the Privacy Act of 1974.[37] The FIPPs comprise eight mandates: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability/Auditing.[38] By DHS policy, the FIPPs "must be considered whenever a DHS program or activity raises privacy concerns or involves the collection of personally identifiable information from individuals, regardless of their status."[39] If CBP cannot meet their own metrics for ensuring privacy when using facial recognition then the agency should not collect that data.

a. CBP failed to meet the FIPPs of Transparency and Individual Participation by not providing adequate notice of facial recognition programs

The Government Accountability Office (GAO) previously investigated CBP's Biometric Entry/Exit program.[40] In a September 2020 report, the GAO found four major shortcomings in CBP's Biometric Entry/Exit program. Together, these failures demonstrate that CBP is either unable or unwilling to take basic steps to protect individuals' privacy, often falling short of DHS's own FIPPs.

First, the GAO found that CBP routinely failed to provide adequate notice and opt out procedures. At the time of the GAO's investigation, CBP's online resources on facial recognition programs had incomplete information and did not list all of the locations where CBP had deployed facial recognition.[41] Similarly, CBP did not provide enough information for call center employees to answer questions about facial recognition.[42] The call center was often offline, and when GAO could get through, operators did not know which air and land ports were using facial recognition.[43]

[35] *Id.* "In an effort to comply with Congressional mandates, CBP's choice to pursue facial recognition specifically, as opposed to any of the various other biometric modalities, was largely a consequence of an unavoidable reality."

[36] Hugo Teufel III, The Fair Information Practice Principles: Framework for Privacy Policy at the Dept. of Homeland Security Memorandum Number 2008-01, Dep't. of Homeland Sec. (Dec. 29, 2008), https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

[37] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

[38] DHS FIPPs Memorandum, supra note 36, at 4.

[39] DHS FIPPs Memorandum, supra note 36.

[40] U.S. Gov't Accountability Off., GAO-20-568 Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues (Sept. 2020) (hereinafter GAO Facial Recognition Report), https://www.gao.gov/products/GAO-20-568.

[41] *Id*. at 39.

[42] *Id*. At 39-40.

[43] *Id*.

Second, signs at airports were consistently outdated and contradictory. The GAO found that signs within a single airport contained contradictory information on data retention policies.[44] CBP claimed their failure to update signage was justified by the prohibitive cost of printing signs.[45] CBP has not prioritized updating posted notices to reflect current procedures and data retention protocols. CBP appears unconcerned with providing accurate and meaningful notice to travelers.

Third, the GAO faulted CBP for providing inadequate information on how travelers could opt-out of facial recognition identity verification.[46] CBP's signs mentioned an opt-out but did not describe what "alternative procedures" travelers would have to go through in lieu of facial recognition.[47] Throughout its implementation of Biometric Entry/Exit CBP has provided vague and inconsistent descriptions of alternative screening procedures. In 2018, EPIC obtained documents through a FOIA lawsuit revealing that CBP had developed a detailed opt-out and alternative screening procedure.[48] But the agency did not describe that procedure to the public.[49] This critique echoes the Data Privacy and Integrity Advisory Committee's report from 2019 which recommended basic improvements to CBP's written notices to improve readability, ensure adequate time for consideration, and explain opt-out procedures.[50] CBP has for years been on notice that the agency needs to provide and publicize a clear opt-out procedure, but the agency has failed to do so.

Fourth, CBP and its corporate partners routinely failed to post signs or obscured notices on facial recognition. The GAO observed that "facial recognition signs were not consistently posted or were posted in such a way that they were not easily seen by travelers."[51] Where CBP delegates responsibility for posting signs to commercial airlines, the GAO found that the agency did not enforce or monitor this requirement.[52] As a result, required signs are often missing. The GAO also observed signs that were difficult to read because they were posted far away from travelers and written in small print.[53] Facial recognition notices are also often blocked by other

[44] *Id*. at 40.
[45] *Id*.
[46] *Id*. at 41.
[47] *Id*.
[48] U.S. Customs and Border Prot., Traveler Verification Service: Standard Operating Procedure at 9 (June, 2017), https://epic.org/foia/dhs/cbp/biometric-entry-exit-alt-screening-procedures/Traveler-Verification-Service-SOP-June2017.pdf; U.S. Customs and Border Prot., Biometric Air Exit: Standard Operating Procedure (Mar. 2019), https://epic.org/foia/dhs/cbp/biometric-entry-exit-alt-screening-procedures/Biometric-Air-Exit-SOP-Mar2019.pdf.
[49] *See* EPIC v. CBP (Biometric Entry-Exit Alternative Screening Procedures), https://epic.org/documents/epic-v-cbp-biometric-entry-exit-alternative-screening-procedures/.
[50] DHS Data Privacy and Integrity Advisory Committee, Report 2019-01 of the DHS Data Privacy and Integrity Advisory Committee (DPIAC): Privacy Recommendations in Connection with the Use of Facial Recognition Technology at 4-5 (Feb. 26, 2019) (hereinafter DPIAC Facial Recognition Recommendations), https://www.dhs.gov/sites/default/files/publications/Report%202019-01_Use%20of%20Facial%20Recognition%20Technology_02%2026%202019.pdf.
[51] GAO Facial Recognition Report at 42.
[52] *Id*.
[53] *Id*. at 44.

signs so that they could not be read.[54] CBP claims that their Biometric Entry/Exit staff is small, and cannot ensure signs are posted so they rely on local airport agents.[55] Yet CBP's airport agents told the GAO that they did not check signs, and were not required to do so.[56] CBP has historically been unable to ensure that travelers receive adequate, or often any, notice that they can opt out of one of the most invasive technologies in use today.

By not providing travelers meaningful notice and the time to consider their options, the GAO found that CBP has not met its requirements under the FIPPs of Transparency and Individual Participation.[57] While providing notice may not be the strongest step CBP can take to protect individuals' personally identifiable information, it is the easiest. If CBP cannot or will not take the basic steps necessary to provide travelers with adequate notice of facial recognition, then the agency's ability to provide more substantive protection is dubious at best.

CBP's failure to provide notice of its facial recognition policies has caused real privacy harms. The GAO received reports of incidents of individuals "being told by CBP officers and airline agents that opting out would lead to additional security scrutiny, increased wait times, and could be grounds to deny boarding."[58] Although CBP claims to provide opt-out procedures which do not inconvenience or prejudice travelers, the agency is clearly failing to adequately inform its employees and the general public of these procedures. At every turn, CBP has failed to adequately implement its opt-out procedures.

b. *CBP has not performed necessary audits to ensure facial recognition images are secure.*

In its review, the GAO found that CBP "has not audited most of its partners and has not developed a plan for future audits."[59] CBP's agreements prohibit corporate partners from retaining images for their own purposes and require partners to expediently delete images, but CBP does not adequately ensure those contract terms are followed.[60] CBP has allowed its partners to use facial recognition technology for identification since 2017.[61] It took three years for the agency to perform its first audit of an airline.[62] As far as I am aware, the agency still has not audited a cruise line. In that time, over 7 million passengers have submitted to facial recognition by more than 20 airlines and cruise lines.[63] More than 95% of CBP's corporate

[54] *Id.*
[55] *Id.* at 43.
[56] *Id.*
[57] *Id.* at 46.
[58] GAO Facial Recognition Report at 42; *see also* Shaw Drake, *A Border Officer Told Me I Couldn't Opt Out of the Face Recognition Scan. They Were Wrong.*, ACLU (Dec. 5, 2019), https://www.aclu.org/news/immigrants-rights/a-border-officer-told-me-i-couldnt-opt-out-of-the-face-recognition-scan-they-were-wrong/.
[59] *Id.* at 46.
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] *Id.*

partners have never received an audit. The agency has no idea if its partners are taking individuals' images for their own purposes or complying with data retention requirements.

The GAO's findings echo DPIAC's findings, in which the Committee stressed that "it is important to ensure transparency in the process, strong contractual guidelines, auditing, and rigor in the process of ensuring the FIPPs are adhered to."[64] The DPIAC called for thorough audits as a necessary step to protect particularly sensitive facial recognition images.[65] Yet despite the DPIAC's urgings, CBP has performed only one audit of its commercial partners and seemingly has no plan in place for further audits of either its commercial partners or its contractors. This amounts to willful blindness on the part of the agency. CBP's failure to perform necessary audits for years displays a callous disregard for individuals' privacy, even after the agency suffered a serious data breach of its facial recognition systems.

c. *CBP has been unable to safeguard facial recognition images.*

Recent data breaches and hacks within CBP and across the federal government demonstrate that CBP is incapable of safeguarding sensitive personal information such as facial recognition images. In 2016 the U.S. Government Accountability Office warned that "[c]yber-based intrusions and attacks on federal systems have become not only more numerous and diverse but also more damaging and disruptive."[66] The GAO called on DHS to enhance cybersecurity protection in key areas including intrusion detection and prevention. At the time DHS had not even put in place an adequate process for sharing information on intrusions and potential malicious activity.[67] Since that time DHS and its subcomponents have not shown that they are capable of adequately safeguarding personally identifiable information, particularly biometric data.

In 2019 a data breach at CBP subcontractor Perceptics, LLC exposed approximately 184,000 images of travelers from a CBP Biometric Entry/Exit pilot.[68] Perceptics staff were able to violate several DHS security and privacy protocols to download the images used for facial recognition without CBP's IT security controls preventing the unauthorized action or sounding an alarm.[69] When Perceptics, LLC was subsequently hacked, outside agents had access to those 184,000 images and an additional 105,000 license plate images.[70] At least 19 facial recognition images were released on the dark web.[71] DHS's Office of the Inspector General found that, "Perceptics was able to make unauthorized use of CBP's biometric data, in part because CBP did

[64] DPIAC Facial Recognition Report at 10.
[65] *Id*. at 10-12.
[66] U.S. Gov't Accountability Office, DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System (Jan. 2016), https://www.gao.gov/assets/680/674829.pdf.
[67] *Id*. at 27.
[68] Joseph Cuffari, Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot, Dep't of Homeland Sec. Off. of Inspector Gen. (Sept. 21, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf .
[69] *Id*. at 6.
[70] *Id*. at 8.
[71] *Id*. at 13.

not implement all available IT security controls, including an acknowledged best practice."[72] OIG concluded that CBP "[d]id not adequately fulfill its responsibilities for IT security".[73]

Data breaches are common across the federal government—often exposing the PII of millions to exploitation and abuse. But data that is never collected in the first place is not at risk of breach. CBP should not unnecessarily collect sensitive personally identifiable information on millions of travelers when the agency cannot even protect the data it currently holds.

VI. The expansion of CBP's Biometric Entry-Exit program creates a powerful and dangerous tool of surveillance for the federal government

Through the Biometric Entry-Exit program, CBP can access millions photos of US citizens through the State Department. Additionally, DHS retains millions of photos in its IDENT database that are accessible to CBP. As part of the Biometric Entry-Exit system, CBP has created a cloud-based facial recognition system that allows the agency to easily connect the system to its own cameras or the cameras of its partners to perform facial identification. One of the main reasons CBP chose to use facial recognition is that the images were easy to obtain and facial recognition technology is easy to apply to existing systems. The result is an expansion of an infrastructure that could easily be used for mass surveillance and/or a universal digital ID controlled by the government.

a. CBP's Biometric Entry-Exit program creates a ubiquitous, universal ID controlled by the government

The continued use of facial recognition identification through CBP's Biometric Entry-Exit program puts the U.S. on a path towards a ubiquitous and universal form of identification that will destroy anonymity and give the government complete control over identification. No longer will an individual have any control over their identification and have choice when to identify themselves or not. A facial recognition identification system leveraging hundreds of millions of photos held by the government will give CBP and other government agencies the power to identify individuals whether or not that individual consents and regardless if the government has legitimate grounds for wanting to identify the individual. And there will be little recourse.

Our face's geometry that is used to create the face prints for facial recognition is unique to each person and for the most part can't be changed. And unlike other forms of biometric recognition or identity verification, facial recognition can easily be applied covertly, from a distance, and without our consent or knowledge. Because our faces are generally exposed and photographs are required for government identifications like passports, it is virtually impossible to insulate ourselves from facial recognition technology. Once the government has a person's faceprint, it creates a unique risk of unprecedented and persistent surveillance—one that allows the government to identify and track people without their knowledge.

[72] *Id*. at 12.
[73] *Id*.

b. *Unless regulations are put in place to limit the Biometric Entry-Exit system, it will continue to expand beyond its original, claimed purpose*

The current lack of regulation of biometrics and the associated technologies, particularly facial recognition technology, means there are little to no barriers to the continued expansion beyond the original purpose of the facial recognition identification system used for the Biometric Entry-Exit program. The Biometric Entry-Exit program itself demonstrates how the lack of regulation of biometrics has allowed the government to use biometrics as it sees fit. Without consent or notice and a general lack of transparency at the beginning, CBP was able to obtain access to the millions of passport photos held by the State Department. CBP regular takes these photos to create biometric templates to use as part of their facial recognition identification system. There is no way to opt out of having your photo used this way and no one agreed to this.

Furthermore, the Biometric Entry-Exit program has continued to expand beyond its claimed original purpose to address visa overstays. CBP has made clear that it intends to expand the use of TVS, the backbone of its facial recognition identification system, for things like checking in for a flight. In a document obtained by EPIC through the Freedom of Information act, CBP described an airport process where every step from dropping off baggage, moving through TSA checkpoints, and boarding planes is mediated by facial recognition scans.[74] Additionally, FOIA documents obtained by EPIC show that other subcomponents of DHS, including Immigration and Customs Enforcement, the United States Secret Service, and the United States Coast Guard, will be able to leverage CBPs facial recognition identification system for their own mission operations.[75] There is no regulation is place that would stop CBP from continuing to expand access to its facial recognition identification system and leverage it for additional purposes.

VII. CBP's other uses of facial recognition technology

It is worth noting that the Traveler Verification Service used as part of the Biometric Entry-Exit program is not the only CBP-owned facial recognition system. According to a GAO report, CBP's Automated Targeting System (ATS) is another system that incorporates facial recognition technology.[76] ATS has over 15 million photos in its database, including passport photos and state identification photos.[77] The ATS facial recognition system is used on individuals who 1) want to enter or exit the U.S., 2) apply to CBP programs to travel to U.S., or 3) are "subjects of interest who require additional research and analysis."[78] It is not clear who falls under this third category.

[74] Dep't. of Homeland Security, Biometric Pathway: Transforming Air Travel (Dec. 1, 2016), *available at* https://epic.org/wp-content/uploads/foia/dhs/cbp/biometric-entry-exit/Biometric-Pathway.pdf.

[75] Dep't of Homeland Security, Capability Analysis Study Plan for Biometric Entry-Exit (Jan. 23, 2017), *available at* https://epic.org/wp-content/uploads/foia/dhs/cbp/biometric-entry-exit/Capability-Analysis-Study-Plan.pdf.

[76] Government Accountability Office, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, 50 (June 2021), https://www.gao.gov/assets/gao-21-518.pdf.

[77] *Id.* at 50.

[78] *Id.* at 50.

Additionally, CBP has used facial recognition systems "owned by federal, state, local, and non-governmental entities."[79] We know that at least one of the non-governmental entities is Clearview AI. According to reporting, CBP had close to 280 Clearview accounts registered that ran nearly 7,500 searches.[80] Clearview AI is one of the most controversial and dangerous implementations of facial recognition technology. Clearview secretly scraped billions of images from social media and other websites to create a massive biometric database.[81]

VIII. Recommendations

The safest and best thing for CBP to do would be for the agency to voluntarily cease using facial recognition technology. This would eliminate the risk of CBP's facial recognition infrastructure being used for more pervasive surveillance or as a ubiquitous identification system.

But Congress should also act. Though I recognize it has not been referred to this Committee, EPIC recommends that Congress enact H.R. 3907, the Facial Recognition and Biometric Technology Moratorium Act of 2021.[82] This bill would generally prohibit the use of facial recognition technology by CBP and other federal agencies except for instances where Congress has explicitly authorized the use of the technology and provided robust protections. The Act would ensure there are protections against racial and gender bias and for privacy and First Amendment-protected rights. The Act would implement strong auditing and accountability requirements. In short, the Act would guarantee the type of protections that are currently lacking in CBP's use of facial recognition technology and force Congress to carefully consider if CBP should implement facial recognition technology, and if so, how.

At minimum, Congress should put in place the following requirements for CPB's use of facial recognition technology:

- The use of a one-to-one facial recognition identification system that does not require a database or connection to the cloud;[83]
- A prohibition on the use of facial recognition services (e.g. Clearview) provided by third-parties;

[79] *Id.* at 48**.**
[80] Ryan Mac, Caroline Haskins, and Logan McDonald, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA* Buzzfeed News (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.
[81] Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[82] H.R. 3907, 117th Cong. (2021) (the Facial Recognition and Biometric Technology Moratorium Act of 2021 prohibits federal agencies from using biometric surveillance systems without explicit authorization from Congress.)
[83] CBP has successfully tested the use of one-to-one facial recognition systems. A one-to-one system does not require a massive biometric database and virtually eliminates data breach risks and chance of that the system will be used beyond the original purpose.

- Prohibit CBP or other components of DHS or other law enforcement entities from using CBP's facial recognition system for generalized investigative leads;
- Require CBP to only use its facial recognition system for identity verification as part of the Biometric Entry-Exit program and prohibit any other uses; and
- Require annual audits of CBP facial recognition system from an independent third party.

If the Biometric Entry Exit program is to remain in operation, these safeguards are critical to protect civil liberties, civil rights, and the security of sensitive biometric data.

IX. Conclusion

Facial recognition technology is a growing threat to our privacy, our civil liberties, and to our democratic values. EPIC urges Congress to address this technology in a meaningful way.

Thank you for the opportunity to testify today.