epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

U.S. CUSTOMS AND BORDER PROTECTION

DEPARTMENT OF HOMELAND SECURITY

Agency Information Collection Activities: Biometric Identity

[Docket No. 1651-0138]

October 28, 2024

By notice published on September 26, 2024, U.S. Customs and Border Protection (CBP) proposes to revise and extend its existing program for collecting biometric information from individuals crossing American land borders.[1] CBP proposes to increase the number of respondents whose biometrics are collected in vehicles "[i]n order to enhance national security" and "improv[e] the information resources available" to border officials.[2]

Pursuant to the agency's request for comments, the Electronic Privacy Information Center (EPIC) submits these comments opposing CBP's revision and extension of this information collection, particularly the use of facial recognition technology. EPIC understands the CBP's Congressional mandate to implement a biometric entry and exit (BE-E) program.[3] However, facial recognition technology is too unreliable, invasive, and dangerous to use without strict, privacy-protective guardrails. Its unregulated implementation puts privacy and civil liberties at risk and disproportionately harms marginalized communities. CBP's proposed collection is unnecessary

[1] CBP, *Agency Information Collection Activities; Revisions; Biometric Information*, 89 Fed. Reg. 78884, 78884 (2024).
[2] *Id*.
[3] *See* Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, § 110 (1996); Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 7208 (2004).

and its expansive system risks mission creep. CBP does not address these shortcomings or provide enough information to evaluate its impact.

Therefore, EPIC urges CBP to end its use of facial recognition technology and to suspend the further implementation of the BE-E program and any consideration of moving forward with facial recognition until there is a robust public conversation on the use of biometrics as a form of digital identification and Congressional regulations providing safeguards for the use of biometrics, particularly facial recognition, as a form of digital identification.

I. EPIC's Interest

EPIC is a public interest research center in Washington, D.C. Established in 1994, EPIC works to focus public attention on emerging civil liberties issues and protect privacy, the First Amendment, and democratic values.[4] EPIC has a longstanding interest in privacy issues stemming from facial surveillance and biometric identifiers.[5] Biometric information is a form of generally immutable personal information obtained from an individual's physical characteristics, such as face prints, fingerprints, iris features, and more. Biometric identification uses these characteristics to identify individuals. Improper collection, access, use, and retention of this information can contribute to identity theft, inaccurate identifications, and infringement on constitutional rights. To prevent abuse, strict limitations must be placed on the collection and use of biometric information. EPIC works to defend the rights of non-citizens,[6] oppose government use of facial

[4] EPIC, *About EPIC*, https://epic.org/epic.about.html.
[5] *See* EPIC, Face Surveillance and Biometrics, EPIC.org, https://epic.org/issues/surveillance-oversight/face-surveillance/ (last accessed Oct. 23, 2024).
[6] *See* Dana Khabbaz, *DHS's Data Resevoir: ICE and CBP's Capture and Circulation of Location Information* (Aug. 2022), https://epic.org/documents/dhss-data-reservoir-ice-and-cbps-capture-and-circulation-of-location-information/; EPIC Comments to DHS: Advance Collection of Photos at the Border (Nov. 29, 2021), https://epic.org/documents/epic-comments-to-dhs-advance-collection-of-photos-at-the-border/; EPIC Comments to DHS on Collection of Biometric Data from Aliens Upon Entry to and Departure From the United States (Dec. 21, 2023), https://epic.org/documents/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states/.

recognition systems,[7] and place common-sense limitations on other uses of biometric information.[8]

II. Facial recognition technology is unreliable and has inherent dangers that are heightened by the likelihood of mission creep.

CBP has radically expanded its face-based biometric collection since 2017. As of October 2024, it has deployed facial recognition technology at 163 land ports of entry for pedestrians.[9] After completing some initial testing of facial recognition in vehicles, CBP now proposes to expand the BE-E program to capture travelers' biometrics in an estimated 2,000,000 vehicles crossing land borders each year.[10] Using cameras placed in driving lanes, the agency attempts to photograph vehicle occupants travelling under 20 miles per hour (known as "at speed").[11] These photos are then sent to the cloud, where CBP's Traveler Verification System (TVS) deploys facial recognition to match the traveler to a pre-existing biometric templates in the system's gallery.[12]

---

[7] *See, e.g.*, Comments of EPIC to the Department of Homeland Security, Agency Information Collection Activities: Biometric Identity, (Jul. 24, 2018), https://epic.org/documents/agency-information-collection-activities-biometric-identity/; Comments of EPIC to the Transportation Security Administration, Intent to Request Revision of Agency Information Collection Activity Under OMB Review: TSA PreCheck (Jun. 22, 2020), https://epic.org/apa/comments/EPIC-TSA-PreCheck-FRT-Comment-June2020.pdf; Comments of EPIC to the U.S. Commission on Civil Rights, Civil Rights Implications of the Federal Use of Facial Recognition Technology (Apr. 8, 2024), https://epic.org/wp-content/uploads/2024/04/EPIC-Comment-to-OMB-re-PIAs-April-2024-with-Appendix-1.pdf.

[8] *See, e.g.,* Testimony of EPIC to the Maryland Senate Finance Committee on Maryland SB169: Biometric Identifiers (Feb. 7, 2023), https://epic.org/documents/maryland-sb169-biometric-identifiers/; EPIC, Comments to the Office of the Privacy Commissioner of Canada Regarding the Update to Guidance on Handling Biometric Information (Jan. 12, 2024), https://epic.org/documents/comments-of-epic-to-the-office-of-the-privacy-commissioner-of-canada-regarding-the-update-to-guidance-on-handling-biometric-information/.

[9] Land Crossings: CBP Biometrics, CBP.gov, https://www.cbp.gov/travel/biometrics/land-crossings (last accessed Oct. 28, 2024).

[10] *Agency Information Collection Activities; Revisions; Biometric Information*, 89 Fed. Reg. at 78886 (2024).

[11] *See, e.g.*, CBP, *Test to Collect Facial Images From Occupants in Moving Vehicles at the Anzalduas Port of Entry (Anzalduas Biometric Test)*, 83 Fed. Reg. 56862, 56862 (Nov. 14, 2018); DHS, *Collection of Biometric Data from Aliens Upon Entry to and Departure From the United* States, 85 Fed. Reg. 74162, 74174-77 (Nov. 19, 2020, *codified at* 8 C.F.R. Sec 215; Testimony of Rebecca Gambler before the House of Representatives' Committees on Border Security, Facilitation, and Operations, and on Homeland Security, GAO-22-106154 at 5 (Jul. 27, 2022), https://www.gao.gov/assets/gao-22-106154.pdf; DHS, *Privacy Impact Assessment for the Traveler Verification Service*, DHS-CBP-PIA-056, at 33-35 (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

[12] *See, e.g.*, CBP, *Test to Collect Facial Images From Occupants in Moving Vehicles at the Anzalduas Port of Entry (Anzalduas Biometric Test)*, 83 Fed. Reg. 56862, 56862 (Nov. 14, 2018); DHS, *Collection of Biometric Data from*

Facial recognition is an inherently dangerous and privacy-invasive surveillance technology that has shown itself to be unreliable and biased. Its use is a threat to democratic values and Constitutional rights and could easily lead to mission creep. For these reasons, EPIC urges CBP to discontinue its use of facial recognition technology.

a. Facial Recognition Technology is Unreliable—Particularly for Marginalized Groups.

Facial recognition has shown itself to be unreliable time and again. According to a study by NIST this year, commercial algorithms (which are often made available to law enforcement, including CBP[13]) had a false negative rate of anywhere from 0.12% to 50% when using front-facing, well-lit photos.[14] Error rates were at least 20% when more realistic photos were used, like those taken at ports of entry.[15] These problems are particularly acute for members of marginalized groups, who are already overpoliced and misidentified at significantly higher rates.[16]

A recent OIG report claimed that TVS had a technical match rate of 98.8% for pedestrians at land borders.[17] CBP also contracted with NIST to produce a report analyzing the capabilities of

---

Aliens Upon Entry to and Departure From the United States, 85 Fed. Reg. 74162, 74174-77 (Nov. 19, 2020, *codified at* 8 C.F.R. Sec 215; DHS, *Privacy Impact Assessment for the Traveler Verification Service*, DHS-CBP-PIA-056, at 33-35 (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

[13] *See* GAO, Facial Recognition Technology: Federal Agencies Should Take Action to Implement Training, and Policies for Civil Liberties, GAO-23-105607 at 3 (Sept. 2023), https://www.gao.gov/assets/gao-23-105607.pdf. Further, DHS has been linked to the notorious Clearview AI. *Id*. at 13. As a subagency of DHS that accesses DHS' biometric databases, this raises the likelihood that CBP does, or could, access Clearview AI.

[14] Patrick Grother, Mei Ngan, & Kayee Hanaoka, *Face Recognition Technology Evaluation (FRTE) Part 2: Identification*, NIST 5 (Sept. 18,. 2024), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

[15] *Id*.

[16] *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* Proceedings of Machine Learning Research 81:1-15 (2018), https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf (finding that that, while the maximum error rate for lighter-skinned males is 0.8%, it is 34.7% for darker-skinned females). *See also* Patrick Grother, Mei Ngan, & Kayee Hanaoka, Face Recognition Vender Test Part 3: Demographic Effects, NIST (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (finding that Black people were 100 times more likely on average to be misidentified than white people).

[17] Joseph Cuffari, *DHS Needs to Improve Its Screening and Vetting of Asylum Seekers and Noncitizens Applying for Admission into the United States*, DHS Office of the Inspector General, OIG-24-27 at 5 (Jun. 7, 2024).

TVS, which returned a similarly high accuracy rate.[18] However, these numbers are irrelevant to CBP's expansion to vehicles. OIG's figure was based on 1:1 matching, where a person's live photo is compared to a travel document.[19] NIST's report conducted 1:N matching, but this merely compared the live photo to a small gallery of known travelers at airports.[20] In contrast, attempts to identify vehicle occupants travelling at speed work without a passenger manifest. Instead, the live photo (when the agency manages to capture a usable one)[21] must be compared against a pool of millions of unknown individuals. This is worsened further by conditions such as windshield grime and glare, passengers laying down or facing away from the camera, and passengers wearing obstructive clothing such as masks or sunglasses all dampen the system's efficacy and risk misidentification.

b. Expansion of a Facial Recognition Network Contributes to Privacy Harms and Mission Creep and Threatens to Diminish Constitutional Values.

Even if the technical issues cleared up, the dangers posed by facial recognition would not. Facial recognition is a tool of total surveillance that invades a person's privacy in public and private spaces and substantially chills key democratic freedoms. Further, imperfect security opens individuals up to having their biometric templates stolen and used by bad actors. In light of these

[18] *See* Patrick Grother, Austin Hom, et al., *Face Recognition Vendor Test Part 7: Identification for Paperless Travel and Immigration*, NIST 3-5 (Jul. 2021), https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8381.pdf.
[19] Joseph Cuffari, *DHS Needs to Improve Its Screening and Vetting of Asylum Seekers and Noncitizens Applying for Admission into the United States*, DHS Office of the Inspector General, OIG-24-27 at 5 (Jun. 7, 2024) (stating that the system "compares a traveler's live photo [to a gallery or a travel document photo]"). In a PIA, DHS explained that pedestrians at land borders undergo 1:1 facial matching. DHS, *Privacy Impact Assessment for the Traveler Verification Service*, DHS-CBP-PIA-056, at 33 (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.
[20] *See* Patrick Grother, Austin Hom, et al., *Face Recognition Vendor Test Part 7: Identification for Paperless Travel and Immigration*, NIST 2.
[21] *See* Sam Biddle, Homeland Security Still Dreams of Face Recognition at the Border, The Intercept (Aug. 27, 2024), https://theintercept.com/2024/08/27/face-recognition-border-surveillance-dhs/; DHS Office of Inspector General, *DHS Needs to Improve Its Screening and Vetting of Asylum Seekers and Noncitizens Applying for Admission into the United States*, OIG-24-27 at 10 (Jun. 7, 2024); CBP, Land Border Integration Division Anzalduas Technology Demonstration (May 16, 2022), https://www.documentcloud.org/documents/25075396-land-border-integration-division-anzalduas-technology-demonstration.

concerns, and the heightened likelihood of mission creep, CBP should pause its extension of facial recognition to vehicles.

First, CBP has not demonstrated its ability or willingness to safeguard sensitive personal information, including facial recognition images. Under CBP's current collection, biometric information of US citizens is retained for up to 12 hours, noncitizens up to 14 days, and "in-scope" individuals for 75 years.[22] This leaves ample time for compromise. As EPIC detailed in our comments on the 2020 BE-E expansion, the federal government (especially DHS and its subcomponents) is no stranger to data breaches.[23] Indeed, CBP experienced a major breach in 2019 when a subcontractor violated DHS protocols and downloaded approximately 184,000 face images and another 105,000 license plate images.[24]

CBP does not appear any better prepared to protect biometric information today. In 2022, GAO found that CBP had begun to audit its partners at air ports of entry, but not land or sea.[25] While the agency has implemented encryption practices and restricted removable media devices, its work to address vendor compliance is limited to privacy awareness trainings, contract terms, and updates to DHS' Privacy Incident Handling Guidance.[26] These are not enough, particularly given CBP's lack of a detailed description of its technology, vendors, or plans for implementation at each port.

---

[22] DHS, *Privacy Impact Assessment for the Traveler Verification Service*, DHS-CBP-PIA-056, at 10, 21.
[23] EPIC, Comments to CBP on the Collection of Biometric Data from Aliens upon Entry to and Departure From the United States, 8-11 (Dec. 21, 2020), *available at* https://epic.org/documents/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states/.
[24] *See* 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.
[25] Testimony of Rebecca Gambler before the House of Representatives' Committees on Border Security, Facilitation, and Operations, and on Homeland Security, GAO-22-106154 at 16.
[26] CBP, *CBP Privacy Evaluation of the Traveler Verification Service in Support of the CBP Biometric Entry-Exit Program*, CBP Privacy Evaluation 22-001 16-17 (Aug. 15, 2022).

Second, CBP's expansion of facial recognition at the border has serious risks of mission creep – when an agency seeks to leverage existing tools and data for new purposes beyond the agency's original reason for collection. In previous vehicle at speed tests, CBP has stated that biometrically-enabled vehicle lanes are clearly labeled[27] (although it has had trouble ensuring this in the past).[28] Even so, facial recognition deployed in vehicles that do not stop opens the possibility of using the technology on individuals without their knowledge or consent. Further, the system used by CBP (itself built on mission creep as photos from other, unrelated encounters are included in the gallery) could equally be deployed within the interior of the United States. Indeed, facial recognition is becoming more widespread, having been used to surveil protestors and make (often) wrongful arrests.[29] While CBP does not have public plans to use its system within the US, it engages in data sharing with other federal departments,[30] has contracts that include access to citizens' data,[31] and has played a role in monitoring protests.[32] The conditions are ripe for mission

[27] *See, e.g.*, CBP, *Test to Collect Facial Images From Occupants in Moving Vehicles at the Anzalduas Port of Entry (Anzalduas Biometric Test)*, 83 Fed. Reg. 56862, 56862 (Nov. 14, 2018); CBP, *CBP Announces a Facial Biometric Test for Inbound Vehicle Travelers at Mariposa Port of Entry*, CBP.gov (May 16, 2024), https://www.cbp.gov/newsroom/local-media-release/cbp-announces-facial-biometric-test-inbound-vehicle-travelers-mariposa.

[28] For a discussion of this, see EPIC, Comments to CBP on the Collection of Biometric Data from Aliens upon Entry to and Departure From the United States, 4-7 (discussing GAO's 2020 report finding major shortcomings in CBP's signage and notice of opt-out procedures).

[29] *See*, *e.g.*, GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, GAO-21-518 (Jun. 2021), https://www.gao.gov/assets/gao-21-518.pdf; Katie Hawkinson, *In Every Reported Case Where Police Mistakenly Arrested Someone Using Facial Recognition, That Person has Been Black*, Bus. Insider (Aug. 6, 2023), https://www.businessinsider.com/in-every-reported-false-arrests-based-on-facial-recognition-that-person-has-been-black-2023-8; Thaddeus L. Johnson et al., *Facial Recognition Systems in Policing and Racial Disparities in Arrests*, 1, 9 (Oct. 2022), https://www.sciencedirect.com/science/article/abs/pii/S0740624X22000892.

[30] *See* Joseph Cuffari, *DHS Needs to Improve Its Screening and Vetting of Asylum Seekers and Noncitizens Applying for Admission into the United States*, at 6-7.

[31] Suzanne Smalley, *Customs and Border Protection Acquired 'Huge Amount of Surveillance Power',* the Record (Nov. 16, 2023), https://therecord.media/cbp-lexisnexis-risk-solutions-contract-surveillance.

[32] Tonya Riley, *US Border Agency's Data Broker Deal Masks Spy Tools, Critics Say*, Bloomberg Law (Nov. 16, 2023), https://news.bloomberglaw.com/privacy-and-data-security/us-border-agencys-data-broker-deal-masks-spy-tools-critics-say.

creep. The likelihood of creep is heightened even further by the lack of federal regulation on the collection, use, and dissemination of biometric data.[33]

Finally, facial recognition risks serious constitutional harms. As a tool that enables constant surveillance, it substantially chills key freedoms under the First Amendment. Particularly for vehicle at speed deployment, using facial recognition to identify occupants means having a detailed record of a person's associations. What's more, considering CBP's involvement in surveillance of protests and concerns of mission creep, facial recognition may significantly deter freedoms of speech and protest as people fear identification (or misidentification) and retaliation for their involvement.

The use of facial recognition at the border has real consequences for everyone—US citizens and non-citizens alike—and will disproportionately impact marginalized groups. In light of the security concerns and the dangers of mission creep and chilling constitutional rights, CBP should pause its extension of facial recognition at the border.

III. CBP is under no obligation to use facial recognition technology and should suspend its use of the technology until Congress considers the implications of biometric Digital IDs and implements appropriate safeguards and restrictions.

First, CBP does not require facial recognition to fulfill its mission and mandate. EPIC acknowledges that CBP is mandated by Congress to create a BE-E program.[34] However, nothing in these statutes requires the use of facial recognition.[35] Further, facial recognition is not required to fulfill CBP's mission to "[p]rotect the American people, safeguard our borders, and enhance the

[33] Jeramie D. Scott, *Facial recognition is here – but privacy protections are not,* The Hill (July 13, 2017), http://thehill.com/blogs/pundits-blog/technology/341906-opinion-facial-recognition-surveillance-is-here-butprivacy.
[34] *See* CBP, *Agency Information Collection Activities; Revisions; Biometric Information*, 89 Fed. Reg. at 78885. *See also* Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, § 110 (1996); Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 7208 (2004).
[35] Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, § 110 (1996); Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 7208 (2004).

nation's economic prosperity."[36] As discussed above, contrary to protecting American people, facial recognition is inherently dangerous and risks violating their privacy and civil liberties. CBP may continue to use other methods, as it has done for years, without taking risks of this proportion or violating its statutory mandate.

Second, CBP should pause its expansion of the BE-E program and not consider the use of facial recognition until congressional safeguards and restrictions are in place. To date, no federal statutes or regulations are in place for the collection, storage, use, or dissemination of biometric information. This means that there are no laws requiring the necessary transparency, oversight, and accountability to ensure that people's privacy, civil liberties, and civil rights are protected.[37] Further, CBP has not released adequate information to the public on its collection, use, or security of biometric data to assess the adequacy of its systems or hold it accountable. Facial recognition poses too great a threat to allow unchecked expansion. There must be congressional safeguards in place before CBP considers subjecting millions of people to facial recognition.

Finally, CBP should refrain from using facial recognition for identity matching until we have a robust, public discussion on digital IDs. CBP's expansion of facial recognition as a means of identity verification raises the likelihood that facial templates become used as a digital ID—one controlled by the government. Using face templates as IDs removes control from individuals and places it with the government, which will have even further ability to identify individuals without consent or knowledge. Further, the threat of mission creep looms even closer as CBP's expansion of facial recognition acts as a tacit endorsement of face verification for other agencies and private

[36] About CBP, CBP.gov, https://www.cbp.gov/about (last accessed Oct. 24, 2024).
[37] *See* Jeramie D. Scott, *Don't Take It at Face Value: Why TSA's Implementation of Facial Recognition is More Dangerous than You Think*, EPIC.org (Jun. 30, 2023), https://epic.org/dont-take-it-at-face-value-why-tsas-implementation-of-facial-recognition-is-more-dangerous-than-you-think/; Kayla Canne, *TSA will now take your photo before you fly. Why privacy advocates say you should opt out.,* AOL (Aug. 3, 2024), https://www.aol.com/tsa-now-photo-fly-why-230007513.html?guccounter=1.

entities who are under no obligation to maintain a responsible level of security and oversight. We must have a greater conversation on the uses, risks, and implications of facial recognition and face print-based digital IDs. CBP should not continue its expansion unless and until such a conversation takes place.

IV. Conclusion

EPIC recommends that CBP immediately suspend the expansion of the BE-E program and any further consideration of the use of facial recognition technology until regulations are implemented by Congress to provide appropriate safeguards.

Respectfully submitted,

/s/ Jeramie D. Scott
Jeramie D. Scott
Director, Project on Surveillance Oversight

/s/ Abigail Kunkler
Abigail Kunkler
EPIC Law Fellow

Electronic Privacy Information Center (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)