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 the

United States Customs and Border Protection Department

Collection of Advance Information From Certain Undocumented Individuals on the Land Border

86 Fed. Reg. 53667 / Docket No: USCBP-2021-0038

November 29, 2021

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Customs and Border Protection Department's (CBP) proposed information collection, Collection of Advanced Information From Certain Undocumented Individuals on the Land Border.[1] CBP proposes to amend the existing data collection by requiring photographs for undocumented individuals who submit personal information for early processing prior to their arrival at the border.

EPIC urges CBP to 1) reverse the proposed information collection so that photographs are not required from undocumented individuals who wish to participate in the advanced collection of information prior to their arrival at the border, 2) create meaningful limitations on the use of photographs submitted by undocumented individuals through this program, and 3) fully explain in future proposed information collections the necessity of additional data point collection.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving the Privacy

---

[1] 86 Fed. Reg. 83667, https://www.federalregister.gov/documents/2021/09/28/2021-20988/collection-of-advance-information-from-certain-undocumented-individuals-on-the-land-border.

Act safeguards enacted by Congress.[2] EPIC also has an ongoing interest in CBP and DHS's use of machine learning and artificial intelligence on the databases containing personal information as well as DHS's use of biometrics, particularly the use of facial recognition.[3]

I. CBP should not solicit photographs from undocumented individuals prior to their arrival at the border

Under the current information collection program set in place in May of 2021, undocumented individuals can elect to submit certain identifying information to CBP prior to their arrival at the border.[4] Other information, including a photograph, is optional and may be included at the discretion of the individual. The proposed revision would change the current advanced collection process by requiring photographs to participate.

---

[2] *See, e.g.*, Comments of EPIC to the Department of Homeland Security, Correspondence Records Modified System of Records Notice, Docket No. DHS-2011-0094 (Dec. 23, 2011), http://epic.org/privacy/1974act/EPIC-SORN-Comments-FINAL.pdf; Comments of EPIC to the Department of Homeland Security, 001 National Infrastructure Coordinating Center Records System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2010-0086, DHS-2010-0085 (Dec. 15, 2010), http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0086_0085.pdf; Comments of EPIC to the Department of Homeland Security, Terrorist Screening Database System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2016-0002, DHS-2016-0001 (Feb. 22, 2016), https://epic.org/apa/comments/EPIC-Comments-DHS-TSD-SORN-Exemptions-2016.pdf.

[3] *See e.g.*, Comments of EPIC to the Transportation Security Administration, 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 Department 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 Committee 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 Department 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 Department 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/.

[4] 86 Fed Reg. 53667.

Information, including facial photographs, submitted during the advance collection process or in person at the border is not stored on-site at the border. Rather, it is placed in a special database in CBP's Automated Targeting System (ATS). ATS is a software tool for collecting, searching, and comparing information across federal databases.[5] ATS uses facial recognition technology to vet individuals with the Traveler Verification Service (TVS).[6] Any photograph of an undocumented individual submitted through the application is also saved as a biometric template into TVS.[7]

Upon their arrival at the border, CBP takes a photograph of the undocumented individual. Once procured, this new photograph is searched against the TVS gallery to identify the individual in ATS.[8] If unsuccessful, CBP can identify an individual by manually searching ATS for their biographic data.[9] Once complete, CBP imports the individual's ATS profile to a Unified Secondary System (USEC) and begins secondary processing.[10] "In secondary [processing], the officers will review the advanced data collected for accuracy, edit the data and save the information . . . ."[11] The advanced collection of information process is one means of speeding up border crossings for migrants but is not necessary to facilitate the border crossing process.

Mandatory collection of photographs for facial recognition provides the limited benefit of avoiding a "manual" search for an individual's profile (e.g. typing the individual's name into a database). However, expanding CBP's use of facial recognition and storing more facial recognition templates comes with serious risks to migrants. These risks may include:

---

[5] Dept. of Homeland Sec., Privacy Impact Assessment Update for the Automated Targeting System, DHS/CBP/PIA-006(e) (Jan. 13, 2017), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp006-ats-may2021.pdf.
[6] *Id.*
[7] OFF. OF MGMT. & BUDGET, SUPPORTING STATEMENT, COLLECTION OF ADVANCED INFORMATION FROM CERTAIN UNDOCUMENTED INDIVIDUALS ON THE LAND BORDER, 1651-NEW (2021), https://omb.report/icr/202104-1651-001/doc/111314801.
[8] *Id.*
[9] *Id.*
[10] *Id.*; *see also* USEC PIA, *supra* note 5.
[11] OMB Supporting Statement, *supra* note 7.

- **Racial Bias in Facial Recognition Technology:** There is a potential for racial bias in accuracy results for non-white and non-male individuals.[12] Failure to match an individual to their profile at the border can slow down the immigration process. A false match subjecting an individual to law enforcement action within the country could have much more serious consequences, including wrongful arrest and police violence.

- **Data Breach:** CBP has not demonstrated that the agency is capable of properly safeguarding facial recognition images. A CBP data breach in 2019 allowed 184,000 facial images to be exposed and 19 to be posted to the dark web.[13] CBP should not collect any facial recognition images before addressing known risks of data theft or data breach.

- **Law Enforcement Abuse:** Turning over facial recognition images to CBP makes those images widely available to federal law enforcement, and often state police, for facial recognition searches. These images can be used to target and wrongfully surveil immigrant communities.

Collecting photos before migrants get to the border is unnecessary because CBP employees have an alternate and lower-risk means to find individual's information in ATS. According to DHS documentation, without the photograph, the individuals' information can be looked up manually by a CBP officer.[14] This manual method of identifying individuals does not pose the same risks associated with facial recognition technology and does not require substantially greater effort from CBP.

---

[12] *See e.g.,* Patrick Grother, Mei Ngan, and Kayee Hanaoka, NISTRIR8280 Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (Dec. 2019), http://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[13] Joseph Cuffari, Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Plot, Dep't of Homeland Sec. Off. of Inspector Gen. (Sep. 21, 2020).
[14] OFF. OF MGMT. & BUDGET, SUPPORTING STATEMENT, COLLECTION OF ADVANCED INFORMATION FROM CERTAIN UNDOCUMENTED INDIVIDUALS ON THE LAND BORDER, 1651-NEW (2021), https://omb.report/icr/202104-1651-001/doc/111314801.

II. CBP should set meaningful limits on the use of any photographs obtained from undocumented individuals.

Information that migrants turn over to cross the border should be used only for the limited purpose of facilitating immigration. Immigrants have no meaningful choice in whether to turn over data in exchange for admission to the United States. CBP should recognize the power dynamics inherent in this collection and that individuals turn over their information solely for immigration purposes. The agency can build credibility and trust with the migrant community by implementing meaningful purpose limitation practices on the personal data that they collect. In addition to adopting purpose limitations, CBP should establish a limited retention schedule for photographs submitted by undocumented individuals.

Under the current scheme, photographs submitted in the advanced application are swept into DHS's vast system of biometric databases. Once submitted to ATS through the One Mobile Application, the undocumented individual's photograph and templatized TVS copy can be run against federal databases for purposes other than identification. For example, photographs submitted through the Application can be run against the TVS gallery, which syncs with other federal databases to provide the status of an applicant's immigration proceeding.

CBP can reduce the potential harms from a data breach by expediently deleting photos after being used for identification at the border. By deleting these images regularly, CBP would cut down on the risk of repeating a loss like that experienced in 2019 when a cyber breach resulted in exposure of biometric information. With fewer images in CBP's galleries, fewer individuals are at risk from a data breach. CBP would also disincentivize data theft by reducing the black-market value of their facial recognition databases.

A tight retention schedule would also reduce the risk of abusive and wrongful uses of facial recognition images. The less time that CBP retains the photographs, the more likely it is that the images

will be used solely for the intended identification purposes, rather than expanding use for general law enforcement purposes.

III. CBP has not provided a sufficient justification for continuing to require photographs from undocumented individuals.

The original information collection was implemented in reaction to the CDC's 2020 Order *Suspending the Right To Introduce Certain Persons From Countries Where a Quarantinable Communicable Disease Exists*,[15] which CBP claims created a backlog of undocumented travelers at the border. [16] It has now been more than 6 months since CBP implemented the original advance notice information collection, on "an emergency basis on May 3, 2021."[17] The proposed revised information collection would cement a workaround of CBP's normal immigration process implemented in the face of an imminent crisis on the Southern Border. CBP has had sufficient time to clear the backlog at the border and to implement Covid-19 mitigation practices. The agency should not use a transient emergency to initiate or make permanent a new form of data collection that threatens the privacy and civil liberties of migrants.

CBP justified the initial emergency information collection based on claims that: (1) the Southwest Border has a high rate of positive COVID tests and COVID-related deaths; (2) the normal process would impose an impracticable delay; (3) without it, delays at the border will increase the risk of COVID-19 transmission; and (4) COVID-19 is a national emergency.[18] The new information collection policy was only intended to last as long as the CDC Order was in place "or as long as required to clear the residual backlog of undocumented travelers" resulting from the Order.[19]

---

[15] 85 Fed. Reg. 65806, https://www.federalregister.gov/documents/2020/10/16/2020-22978/order-suspending-the-right-to-introduce-certain-persons-from-countries-where-a-quarantinable.
[16] OMB Supporting Statement, *supra* note 7.
[17] 86 Fed Reg. 53667, https://www.federalregister.gov/documents/2021/09/28/2021-20988/collection-of-advance-information-from-certain-undocumented-individuals-on-the-land-border.
[18] Emergency Memo, *supra* note 1.
[19] *Id*.

In the revised information collection, CBP claims that deploying facial recognition is still necessary because photographs may help their officers identify undocumented individuals once NGOs and IOs are "no longer facilitating" migrant registration the border.[20] But, CBP acknowledges that these organizations will continue to assist some undocumented individuals, although individuals will now be able to "participate on their own."[21] And vaccinations are now readily available to CBP officers and border communities. The agency should not use the claimed risk of Covid exposure to justify the expansion of biometric technologies when vaccinations, social distancing, and masks can all substantially reduce that risk without risking privacy and civil liberties.

In addition, CBP should provide clear data on the efficiency of this information collection. To date, CBP has not published data on the speed of their immigration processes to support the agency's contention that facial recognition is necessary to facilitate the entry of migrants. To justify an intrusive collection of information, the agency should do more than give its word that identity verification is the sticking point in the agency's process to admit migrants. Under the current information collection, photographs are optional and individuals can be searched for manually, rather than relying on facial recognition. CBP provides no explanation as to why this process is insufficient, apart from vague references to the need for efficiency. They have given no statistics on the time reduced through the collection and photographic identification process, especially as it relates to photographs submitted by undocumented individuals ahead of time. CBP should provide more information to allow the public to properly weigh in on the agency's proposed information collection practices.

---

[20] *Id.*
[21] *Id.*

Conclusion

EPIC urges CBP to at a minimum reverse the proposed changes to the agency's advance notice information collection for migrants and further to switch over to solely manual information retrieval without the aid of facial recognition. Immigration to the U.S. should not force individuals to turn over information that the government does not need to facilitate their entry but can be used for abusive surveillance practices. Please address any questions to EPIC Law Fellow Jake Wiener at wiener@epic.org.

Respectfully Submitted,

Jeramie Scott
Jeramie Scott
Senior Counsel

Jake Wiener
Jake Wiener
EPIC Law Fellow

Bailey Walker
Bailey Walker
EPIC Clerk