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

U.S. CUSTOMS AND BORDER PROTECTION

DEPARTMENT OF HOMELAND SECURITY

Agency Information Collection Activities: Biometric Identity

[Docket No. 1651-0138]

July 24, 2018

By notice published May 25, 2018 U.S. Customs and Border Protection ("CBP") proposes to revise and extend an existing collection of information, titled "Agency Information Collection Activities: Biometric Identity."[1] CBP proposes to develop a biometric based entry and exit system "in order to verify identity, determine admissibility of those seeking entry into the United States, confirm exit from the United States for the purpose of tracking aliens who have overstayed their visa or are otherwise illegally present in the United States, prevent visa fraud, and identify known or suspected criminals or terrorists."[2]

Pursuant to the agency's request for comments, the Electronic Privacy Information Center ("EPIC") submit these comments to urge CBP to (1) suspend the implementation of the Biometric Entry/Exit program pending (2) a public report on the program that addresses why the program is needed as well as whether less privacy-invasive alternatives can achieve the operational goals and

[1] *Agency Information Collection Activities: Biometric Identity,* 83 Fed. Reg. 24326 (May 25, 2018), https://www.federalregister.gov/documents/2018/05/25/2018-11287/agency-information-collection-activities-biometric-identity (hereinafter "notice").

[2] *Id.*

(3) Congressional regulations are passed providing safeguards for the use of biometrics. EPIC believes CBP should not implement any biometric program until the privacy and security problems identified are adequately resolved. EPIC opposes the revision and extension of this information collection.

I. EPIC's Interest

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.[3] EPIC has a particular interest in privacy issues related to biometric identifiers.[4] Biometric data is personally identifiable information that cannot be changed when compromised. Improper collection of this information can contribute to identity theft, inaccurate identifications, and infringement on constitutional rights. Strict limits on biometric data is the best practice to prevent abuse.

EPIC regularly files Freedom of Information Act ("FOIA") requests and files lawsuits seeking records documenting biometric identification programs.[5] EPIC has filed a FOIA lawsuit to obtain documents related to CBP's Biometric Entry/Exit program.[6] More recently, EPIC submitted an urgent FOIA request to the Department of Homeland Security seeking the Privacy Impact Assessment for the "Homeland Advanced Recognition Technology," a proposed system that will integrate biometric identifiers across the federal government and serve as the primary biometric

[3] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[4] EPIC, *Biometric Identifiers*, https://epic.org/privacy/biometrics/.
[5] *See e.g., 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 v. FBI (Biometric Data Transfer Agreements), https://epic.org/foia/fbi/biometric-mou/ (EPIC has obtained several memorandum of understanding regarding the transfer of biometric identifiers between the FBI and the Department of Defense).
[6] *EPIC v. CBP (Biometric Entry/Exit Program)*, EPIC, https://epic.org/foia/dhs/cbp/biometric-entry-exit/default.html.

database for the Biometric Entry/Exit program.[7] EPIC also regularly submits public comments to federal agencies and to Congress advising on the privacy issues caused by the collection of biometrics.[8] And earlier this month EPIC filed an amicus brief[9] with the Illinois Supreme Court in *Rosenbach v. Six Flags Entertainment Corp.,* about the collection of a child's biometric data in violation of the Illinois Biometric Information Privacy Act.[10]

II. EPIC FOIA Documents Reveal CBP Is Creating a Massive and Invasive Biometric Tracking System

EPIC has filed several FOIA requests concerning CBP's Biometric Entry/Exit program. In June 2016, EPIC filed a FOIA request seeking records pertaining to the 1:1 Facial Recognition Air Entry Pilot and the 1-to-1 Facial Comparison Project.[11] In March 2017, an EPIC FOIA request sought records pertaining to CBP's testing of iris and facial recognition at a pedestrian land border.[12] And in October 2017, EPIC resubmitted a FOIA request seeking records pertaining to CBP's biometric exit programs.[13]

The documents EPIC obtained through these FOIA requests and subsequent litigation reveal the invasiveness of the Biometric Entry/Exit program. Additionally, the documents foreshadow the

[7] EPIC FOIA Request (June 18, 2018), https://epic.org/foia/dhs/pia/EPIC-18-06-18-DHS-FOIA-20180618-Request.pdf.

[8] *See, e.g.*, 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; EPIC Comments to FBI, Revision of a Currently Approved Collection-CJIS Name Check Form (1-791) (Jan. 8, 2018), https://epic.org/apa/comments/EPIC-Comments-FBI-NGI-Name-Based-Background-Check.pdf (advising the FBI to limit its use of fingerprint-based background checks in favor of name-based background checks for noncriminal purposes).

[9] Brief of Amicus Curiae EPIC, *Rosenbach v. Six Flags Entm't Corp.,* 2018 WL 1382797 (Ill.), https://epic.org/amicus/bipa/rosenbach/EPIC_Amicus_Rosenbach.pdf.

[10] EPIC, *Rosenbach v. Six Flags*, https://epic.org/amicus/bipa/rosenbach/.

[11] EPIC FOIA Request (June 14, 2016), https://epic.org/foia/dhs/cbp/biometric-entry-exit/EPIC-16-06-15-DHS-FOIA-20160615-Request.pdf.

[12] EPIC FOIA Request (Mar. 2, 2017), https://epic.org/foia/dhs/cbp/biometric-entry-exit/EPIC-17-03-02-CBP-FOIA-20170302-Request.pdf.

[13] EPIC FOIA Request (Oct. 17, 2017), http://epic.org/foia/dhs/cbp/biometric-entry-exit/EPIC-17-10-17-CBP-FOIA-20171017-Request.pdf.

heightened issues of conducting facial recognition through car windshields at a land port of entry where any one of millions of people could be crossing the border that particular day verses conducting facial recognition on a very small and known set of people prior to boarding a flight.

According to FOIA documents obtained by EPIC, CBP plans to implement biometric entry/exit for all travel modes and ports of entry (air, land, and sea).[14] Furthermore, CBP envisions providing "biometrics matching capability for use by the travel industry and DHS components . . . to transform traveler experience from initial encounter through checkpoints to entry/exit."[15] The result threatens to be a massive biometric surveillance network that will continue to expand as the infrastructure to conduct real-time facial recognition grows. This notice and request for comments regarding CBP's plan to collect biometric information from vehicles represents a problematic step in the expansion of the Biometric Entry/Exit program.

The facial recognition match rate at airports, despite ideal conditions, fails to correctly identify everyone. CBP has already implemented biometric entry/exit at several airports. The "exit" portion of the program uses facial recognition to confirm the identity of each traveler prior to that person boarding an international flight. To do this, CBP builds a biometric gallery containing only the listed passengers for that flight. The images in the database come from passport photos and photos for U.S. visas. These photos are compared against a real-time photo of the traveler to confirm the person's identity. Despite these ideal conditions, facial recognition cannot identify everyone. The problem will be far worse for facial recognition of passengers in vehicles because not only are their environmental conditions to deal with (e.g. glare of the windshield), the pool of possible matches goes from hundreds of known and previously screened airline passengers to millions of unknown

[14] *See* Memorandum re: U.S. Customs and Border Protection Biometric Entry-Exit Concept of Operations 000029, https://epic.org/foia/dhs/cbp/biometric-entry-exit/CBP-Biometric-Entry-Exit-Concept-of-Operations.pdf.
[15] *Id.*

individuals since there is no prior list of each traveler before they cross land borders as there is with international flights. Indeed, Colleen Manaher, CBP executive director of planning, program analysis and evaluation stated in an interview that if the technology is able to identify fifty percent of the in-car passengers it would be a "home run."[16] EPIC FOIA documents showed that the use of facial recognition at a pedestrian land border did not perform operational matching at a "satisfactory" level.[17]

The plans of CBP to include the capability to search biometric watch lists[18] will exacerbate the problem of using facial recognition and disproportionately impact minorities. Studies have shown that facial recognition has significantly higher error rates for darker-skinned individuals. One study found that while the maximum error rate for lighter-skinned males is 0.8%, it is 34.7% for darker-skinned females.[19] This is unacceptable in any context, but is especially problematic in this context because it may have the effect of making immigration determinations based on skin color.

The increased use and continued dissemination of biometric information increases privacy and security risks and the potential for mission creep. The system that the CBP has proposed for border security could equally be deployed within the interior of the United States, raising widespread concern about government surveillance of public spaces.[20] The extensive storage of biometrics increases the risk of harm posed by potential security breaches. These are just some of issues raised

[16] Jeremy Schwartz, *Biometric Pilot Will Scan Travelers in Real Time at Texas-Mexico Border*, Government Technology (Feb. 2, 2018), http://www.govtech.com/public-safety/Biometric-Pilot-Will-Scan-Travelers-in-Real-Time-at-Texas-Mexico-Border.html.

[17] U.S. Customs and Border Protection, *Southern Border Pedestrian Field Test Summary Report* 8 (Dec. 2016), https://epic.org/foia/dhs/cbp/biometric-entry-exit/Southern-Border-Pedestrian-Field-Test-Report.pdf.

[18] U.S. Department of Homeland Security U.S. Customs and Border Protection, *Biometric Entry-Exit Program Concept of Operations* 000039 (June 27, 2017), https://epic.org/foia/dhs/cbp/biometric-entry-exit/CBP-Biometric-Entry-Exit-Concept-of-Operations.pdf.

[19] Joy Buolamwini (MIT Media Lab) and Timnit Gebru (Microsoft Research), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[20] *See generally*, Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, NY Times (July 8, 2018), https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

by what is publicly known about CBP's Biometric Entry/Exit program but additional issues rise out of what we don't know about CBP's current proposal to collect biometrics from vehicles.

III. CBP's Current Proposal to Collect Biometrics from Vehicles Fails to Provide the Public with Adequate Information About the Program

The Federal Register notice leaves many relevant questions unanswered about the implementation of the collection and the accuracy of the technology used. In-car facial recognition technology has more potential technical problems than regular facial recognition technology. The system must be able to distinguish windshield reflections from faces of passengers and detect the faces of passengers sitting in the backseat of the car who may be obscured. If people are wearing sunglasses, hats, or other headwear that an officer would normally ask them to remove before using facial recognition technology they would be unable to do so without stopping the car. There are also variations from the car that could cause errors, such as windshield tint. Additionally, passengers may not be looking up and toward the camera, so the image captured could be a profile or in-motion. Has CBP tested the facial recognition technology it intends to use under all of these conditions? What will CBP do if it cannot capture a clear image of all passengers while they are in their car?

It is not clear from the notice what databases CBP will use to compare to the facial scans captured at the border. CBP will run these scans against databases of visas and other travel documents of non-citizens, but will CBP also use databases of U.S. citizens? How does CBP plan to handle the fact that they will not know beforehand who is going to be crossing the border like they do at airports. What is CBP protocol if the facial scan does not match anyone in a citizen or alien database? How long does CBP plan to retain the biometrics collected from vehicles? Will the biometric data collected from vehicle scans be combined with data in license plate reader databases?

IV. Implementing a Massive Facial Recognition Network Will Disproportionally Impact Marginalize Groups and Lead to Mission Creep

The use of facial recognition as part of the Biometric Entry/Exit program poses significant risks to privacy and civil liberties. The technology can be used on unsuspecting people from a distance in a covert manner and on a mass scale. Similarly, facial recognition can easily be applied to large amounts of pictures and videos posted online. Facial recognition gives the government the power to identify individuals whenever it wants and without the consent of the individual.

The implementation of a large-scale biometric surveillance network also runs a serious risk of mission creep. The program itself is built on mission creep as it takes photos handed over to the State Department for the explicit purpose of obtaining a passport and now uses the photos for a new biometric entry/exit program that leverages facial recognition. The probability of mission creep is heightened by the fact that there are few laws that regulate the collection, use, dissemination, and retention of biometric data.[21] As FOIA documents obtained by EPIC show and this Notice confirms, CBP envisions expanding the Biometric Entry/Exit program far beyond its current implementation at airports.

Ubiquitous identification eliminates an individual's ability to control their identities and poses specific risk to the First Amendment rights of free association and free expression. The agency will also assume specific obligations under the Privacy Act for the collection and use of this personal identifiable information. The use of facial recognition at the border has real consequences for U.S. citizens as well as non-U.S. citizens and will disproportionately impact marginalize groups.

V. Conclusion

EPIC recommends that CBP promptly conduct a public report analyzing whether there is an actual need for the program that justifies the privacy risks associated with the use of biometrics. Specifically, the public report should address the possibility of using less privacy-invasive

[21] 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-but-privacy.

alternatives to biometric identification that will meet operational needs, including a cost-benefit analysis that contains a comparison of the likelihood and cost of a data breach between the Biometric Entry/Exit program and alternatives that do not use facial recognition or other biometrics. Finally CBP should immediately suspend the implementation of the Biometric Entry/Exit program pending the results of the public report and until regulations are implemented by Congress providing appropriate safeguards for the use of biometrics.

Sincerely,

/s/ *Marc Rotenberg* Marc Rotenberg EPIC President	/s/ *Jeramie Scott* Jeramie Scott EPIC National Security Counsel
/s/ *Christine Bannan* Christine Bannan EPIC Administrative Law and Policy Fellow	