PROJECT ON GOVERNMENT OVERSIGHT

December 20, 2020

Re: Collection of Biometric Data from Aliens upon Entry to and Departure from the United States (docket number USCBP-2020-0062-0001), proposed by Customs and Border Protection

The Project On Government Oversight (POGO) submits the following comment in opposition to the proposed rule USCBP-2020-0062-0001, titled, "Collection of Biometric Data from Aliens upon Entry to and Departure from the United States," issued by Customs and Border Protection (CBP) and published in the Federal Register on November 19, 2020.

POGO is a nonpartisan independent watchdog that investigates and exposes waste, corruption, abuse of power, and when the government fails to serve the public or silences those who report wrongdoing. We champion reforms to achieve a more effective, ethical, and accountable federal government that safeguards constitutional principles. The Constitution Project at POGO strives to protect individuals from improper and overbroad surveillance, including unchecked face recognition surveillance. For the following reasons, POGO opposes the proposed rule and urges CBP to withdraw it.

The proposed rule seeks to expand CBP's biometric entry-exit system—which identifies individuals using face recognition—by moving out of the pilot phase and permitting the Department of Homeland Security (DHS) to install biometric systems at all airports, seaports, and land ports, and requiring participation in the system by all noncitizens entering and exiting the country. We believe this system poses serious risks to civil rights and civil liberties, and that it does so unnecessarily, given the less-invasive alternatives that have thus far gone largely unexamined by CBP, notably a one-to-one face verification system.

Unless and until CBP fully considers such options, we believe the use of biometric entry-exit systems should be halted rather than expanded. While travelers crossing the border and traveling on flights do face some reasonable limits to privacy, we believe that CBP, in its use of any biometric entry-exit system, must do more to ensure misidentification harms are minimized, disparate impact is prevented, and potential mission creep is prevented.

POGO has worked for years to highlight the limits of face recognition technology and the dangers it can pose to civil rights and civil liberties.[1] Many of these risks extend to and are exacerbated by biometric entry-exit systems.

Misidentification Creates a Broad Set of Risks

One of the most significant risks posed by face recognition technology is misidentification. Most notably, face recognition tends to misidentify women and people of color at a higher rate than other

[1] Task Force on Facial Recognition Surveillance, Project On Government Oversight, *Facing the Future of Surveillance* (March 4, 2019). https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/

Project On Government Oversight
1100 G Street, NW, Suite 500
Washington, DC 20005
202.347.1122
pogo@pogo.org
www.pogo.org

people, as shown in studies by the National Institute of Standards and Technology (NIST); researchers from the Massachusetts Institute of Technology, Microsoft, and the AI Now Institute; the American Civil Liberties Union; and an FBI expert.[2] Just last year, the National Institute of Standards and Technology found that some systems were 100 times more likely to misidentify people of East Asian and African descent than white people.[3] And although some algorithms and systems perform more accurately and better mitigate this harm, it continues to be a trend for the technology.

Face recognition is also highly dependent upon a variety of factors. Bad lighting, indirect angles, distance, poor camera quality, and low image resolution all undermine the reliability of matches. In order to minimize the risk of errors, CBP should first ensure that any type of biometric screening it deploys is conducted with effective, uniform standards on how individuals' photos are being taken.

CBP offers conflicting data regarding the accuracy of its systems. In testimony earlier this year, then-Deputy Assistant Executive Commissioner John Wagner stated, "Facial comparison technology can match more than 97 percent of travelers."[4] However CBP describes its systems as possessing a substantially different error rate in defending them on a public explainer webpage, stating, "NIST found that with high quality photos, the most accurate algorithm can identify matches with only a 0.2 percent error rate."[5] But even the more optimistic metric—which does not account for increased likelihood of error for people of color—would yield frequent misidentifications, with 188 per day on average at hubs such as New York City's John F. Kennedy International Airport if all international travelers used this system.[6]

---

[2] Patrick Grother, Mei Ngan, Kayee Hanaoka, National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280 (December 19, 2019), 2. https://doi.org/10.6028/NIST.IR.8280; Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research*, vol. 81 (2018). http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Joy Buolamwini and Inioluwa Deborah Raji, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products," AIES '19: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society (2019). https://www.media.mit.edu/publications/actionable-auditing-investigating-the-impact-of-publicly-naming-biased-performance-results-of-commercial-ai-products/; Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots," American Civil Liberties Union, July 26, 2018. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognitionfalsely-matched28; Brendan Klare et al., "Face Recognition Performance: Role of Demographic Information," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6 (December 2012). http://openbiometrics.org/publications/klare2012demographics.pdf.

[3] Grother, Ngan, Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, 2. [see note 2]

[4] *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II: Hearing before the House Committee on Homeland Security*, 116th Cong. (February 6, 2020) (testimony of John Wagner, Deputy Assistant Executive Commissioner for Office of Field Operations, Customs and Border Protection). https://homeland.house.gov/imo/media/doc/Testimony-Wagner2.pdf

[5] Customs and Border Protection, "Biometric Exit Frequently Asked Questions (FAQs)," updated May 15, 2020. https://www.cbp.gov/travel/biometrics/biometric-exit-faqs (accessed December 17, 2020)

[6] In 2019, John F. Kennedy International Airport handled 34.3 million international passengers. At the 0.2% error rate described on the CBP website, this would yield 68,600 misidentifications annually and an average of 188 at the airport per day if all international travelers used the CBP face recognition system. At the higher 3% error rate Wagner describes in his testimony, the expected number of misidentifications at the airport would jump to over 1 million annually, with an average of 2,819 misidentifications each day. The Port Authority of New York and New Jersey, *2019 Annual Airport Traffic Report* (May 18, 2020). https://www.panynj.gov/airports/en/statistics-general-info.html

The agency's refusal to account for the significance of the misidentification problem—especially when expanding use of face recognition to a greater scale and new situations—creates serious risks.

Misidentifications can lead to acute harms for travelers. If a face recognition system incorrectly labels a passenger as not included in a flight manifest—meaning a false negative, where it fails to accurately match the passenger with their photo—personnel may be more likely to treat that individual with suspicion, and subject them to additional screening measures. "Automation bias," in which individuals place undue levels of trust in recommendations from computers and automated systems, is a well-documented phenomenon in general,[7] and for face recognition in particular.[8] This creates especially significant risks in the context of law enforcement and security.[9] However, we have not seen CBP take any steps to educate and train personnel on automation bias to ensure that agents do not—either explicitly or subconsciously—treat a non-match in the biometric entry-exit system as basis for suspicion.

Travelers subject to additional screening because of erroneous face recognition non-matches could be met with a variety of harms, such as unjustified searches, questioning, and temporary detainment, which could cause them to miss flights. Such risks make it reckless to expand the biometric entry-exit system. And the fact that these harms are more likely to be borne by people of color—as they are more likely to be misidentified—constitutes an unacceptable violation of civil rights.

Additionally, CBP should not discount the risk of false positives, in which a face recognition system error results in an unauthorized individual being cleared for a flight.[10] The potential for such errors presents serious national security concerns.

Advocates of expanding the current biometric entry-exit system without taking the time to further consider other options may emphasize that only noncitizens will be required to participate. However, many rights—such as equal protection against discriminatory government activities—extend to citizens and noncitizens alike. And apart from the question of whether use of the system infringes upon constitutional rights, failing to evaluate the best means of limiting misidentifications is bad policy for ensuring security and efficient travel. Finally, given the challenges associated with opting

---

[7] Raja Parasuraman and Dietrich H. Manzey, "Complacency and Bias in Human Use of Automation: An Attentional Integration," *Human Factors*, vol. 52, no. 3, June 2010: 381-410. https://www.depositonce.tu-berlin.de/bitstream/11303/8923/1/Parasuraman_Manzey_2010.pdf

[8] "Many agencies state that no one is arrested solely on the basis of a face recognition match … In reality, my research has found that this is not always the case. Agencies in multiple jurisdictions have relied almost exclusively on the results of a face recognition system to identify someone for arrest, greatly increasing the risk of misidentification." *Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties*: *Hearing before the House Committee on Oversight and Reform*, 116th Cong. (May 22, 2019) (testimony of Clare Garvie, Senior Associate, Center on Privacy & Technology at Georgetown Law). https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-GarvieC-20190522.pdf

[9] Alexander Babuta and Marion Oswald, Royal United Services Institute for Defence and Security Studies, *Data Analytics and Algorithmic Bias in Policing*, 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831750/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf

[10] It is important to distinguish and account for the risk of both false negatives/rejects (meaning improperly registering an individual as not authorized to board a flight) and false positives/accepts (meaning improperly registering an individual as authorized to board a flight).

out of the system, the likely impact on U.S. citizens under the planned expansion should not be disregarded.[11]

Mission Creep Could Lead to Pervasive Surveillance

In addition to the harms this system can currently cause to travelers—and those it would cause on an expanded scale if the proposed rule is enacted—the biometric entry-exit system creates a serious risk of mission creep, which could threaten the constitutional rights enjoyed by travelers in the United States, including U.S. citizens. CBP has already shifted its airport face recognition systems from scanning against a gallery composed from a single flight manifest to conducting airport-wide scans of all incoming travelers.[12] CBP is also considering implementing even broader databases for use in conducting face recognition scans against photo galleries composed of "frequent" travelers who are expected to cross at land ports.[13] And the Department of Homeland Security is currently seeking to incorporate real-time biometric scanning of crowds for identifications at airports.[14] It seems inevitable that if CBP continues to use and expand face recognition systems, surveillance operations with missions that are entirely separate from flight safety will begin piggybacking off these systems and use their face recognition infrastructure for other purposes.

CBP Should Consider Less Invasive Alternatives

Given these risks, CBP should consider alternatives to its current biometric entry-exit system. The congressional mandate for this program merely requires the use of biometrics, but in no way requires the use of face recognition. CBP has previously stated that use of other biometric identifiers, such as fingerprints, is impractical because they make the process more cumbersome for travelers.[15] However, CBP has not provided any research or data to demonstrate the degree to which such a system would add difficulty to boarding logistics and impact passengers; it is vital to know the

---

[11] Allie Funk, "I Opted Out of Facial Recognition at the Airport—It Wasn't Easy," *Wired*, July 2, 2019. https://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/

[12] "In order to biometrically identify the traveler, TVS [Traveler Verification Service] automatically creates a template from the image and uses the template to query against a gallery of known identities, based on the manifests for all incoming flights for that day." Customs and Border Protection, "Collection of Biometric Data from Aliens upon Entry to and Departure from the United States," 85 Fed. Reg. 74,162 (November 19, 2020). https://www.regulations.gov/document?D=USCBP-2020-0062-0001

[13] "However, CBP is developing processes that would enable the use of TVS at the land border. For example, CBP may briefly retain local galleries of travelers who have recently crossed at a given POE [port of entry] and are expected to cross again within a given period of time. … If CBP does not have access to APIS [Advance Passenger Information System] manifest information, such as for pedestrians or privately owned vehicles at land ports of entry, CBP will build galleries using photographs of 'frequent' crossers for that specific POE, taken at that specific POE, that become part of a localized photographic gallery." Customs and Border Protection, "Collection of Biometric Data from Aliens upon Entry to and Departure from the United States." [see note 12]

[14] In March 2020, the Department of Homeland Security announced the agency would "now focus on the technical challenge of reliably identifying small, free-flowing groups of individuals in crowded environments, like airports or ports of entry," an indication of a desire to move to real-time face recognition for airport identifications. Department of Homeland Security, "News Release: DHS S&T Announces Third Biometric Technology Rally," March 2, 2020. https://www.dhs.gov/science-and-technology/news/2020/03/02/news-release-st-announces-third-biometric-technology-rally; This announcement echoes a 2019 *CNet* report, which stated that "Airlines and the Transportation Security Agency also are testing facial recognition cameras throughout airports, meaning you might someday be able to travel without interacting with another human being at all." Laura Hautala, "Facial recognition can speed you through airport security, but there's a cost," *CNet*, March 21, 2019. https://www.cnet.com/news/facial-recognition-can-speed-you-through-airport-security-but-theres-a-cost/

[15] *About Face* (testimony of John Wagner). [see note 4]

intensity of such issues if we are to effectively weigh them against both accuracy and constitutional safeguards.

And even setting aside the potential of using entirely different biometric identifiers, there is a potentially less harmful alternative that CBP has not given sufficient consideration as it seeks to expand biometric entry-exit: one-to-one face verification. In place of a face recognition system that matches travelers against either a flight manifest or hundreds or tens of thousands of individuals traveling through an airport on a given day, CBP could implement a system that is limited to one-to-one face verification, which would confirm that a traveler matches with their ticket information or photo ID. Such a measure could improve accuracy,[16] and would guard against mission creep that endangers privacy. The Transportation Security Administration has been testing such a system, demonstrating that airport security can limit biometric systems to one-to-one identity verification while limiting the impact on privacy.[17]

Before moving forward to expand and entrench a face recognition biometric entry-exit system, it is essential for CBP to effectively assess the costs and benefits—to civil rights and civil liberties, to accuracy and security, and to efficiency of travel procedures—of all options. By numerous measures, the planned system is more prone to error than a face verification system or other various forms of biometrics would be. CBP should withdraw the proposed rule and halt all efforts to expand face recognition for entry-exit. The agency should instead focus its efforts on testing, examining, and gathering data on less problematic alternatives, such as one-to-one face verification.

If you have any questions, I can be reached at jlaperruque@pogo.org.

Sincerely,

Jake Laperruque
Senior Counsel
Project On Government Oversight

[16] A comparative analysis should account for differences in error rates between recognition and verification for both false negatives/rejects (meaning improperly registering an individual as not authorized to go onto a flight) and false positives/accepts (meaning improperly registering an individual as authorized to go onto a flight). Additionally, it should examine both overall comparative error rates and comparative error rates based on demographics.

[17] "TSA is testing 1:1 (one to one) facial matching capabilities by integrating biometric capture with Credential Authentication Technology (CAT) machines to verify a live image capture against the image on a credential (e.g., passport or ID photo). TSA is exploring this as a solution for the general traveler population. 1:1 facial matching does not require a database of pre-staged images, since the passenger's ID contains the reference photo to which their live face will be matched." Transportation Security Administration, "Biometrics Technology." https://www.tsa.gov/biometrics-technology (accessed December 10, 2020)