CENTER FOR DEMOCRACY & TECHNOLOGY

December 21, 2020

Submitted via http://www.regulations.gov

Michael Hardin
Director, Entry/Exit Policy and Planning, Office of Field Operations
U.S. Customs and Border Protection, 5th Floor
1300 Pennsylvania Avenue NW
Washington, DC 20229

RE: Comment of the Center for Democracy & Technology in Opposition to DHS Docket Number USCBP-2020-0062, Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States

To Whom It May Concern:

The Center for Democracy & Technology is a nonpartisan, nonprofit technology policy advocacy organization dedicated to advancing individual rights in the digital age.[1] A priority for our organization is securing individual privacy from unwarranted government intrusion. In furtherance of this mission we write in opposition to U.S. Customs and Border Protection's (CBP) notice of proposed rulemaking (NPRM) to expand its authority to implement the biometric entry-exit system beyond its current pilot program, and to expand the category of "in-scope" travelers subject to a mandatory biometric collection and screening requirement to all non-U.S. citizens, including lawful permanent residents of the U.S. and children, and all U.S. citizens who do not "opt out" of such screening.[2]

Congress directed the Department of Homeland Security (DHS) and CBP to develop an entry-exit system to biometrically track the entry and exit of in-scope travelers.[3] They have mis-interpreted this command as permission to condition the entry and exit of non-U.S. citizens on their submission to screening by means of facial recognition technology. Furthermore, they have mis-interpreted this command as permission to subject U.S. citizens to screening by means of facial recognition unless they opt into alternative screening difficult to access and time-consuming to use. Finally, they have also erroneously interpreted this as permission to set the foundation for enhancing the surveillance capabilities of government agencies across the United States. We oppose this NPRM because CBP has not adequately addressed issues of privacy, equity and security in its pilot program, and because CBP has failed to adequately limit the sharing and repurposing of the data it collects.

[1] Center for Democracy & Technology, https://cdt.org/about.
[2] *Notice of Proposed Rulemaking, U.S. Customs and Border Protection, Department of Homeland Security, Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States*, 85 Fed. Reg. 74162-74193 (posted Nov. 19, 2020), https://www.federalregister.gov/documents/2020/11/19/2020-24707/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states.
[3] 8 C.F.R. § 235.1. "In-scope" travelers are defined to include all foreign nationals (including lawful permanent residents and others who reside in the United States), with exceptions for individuals younger than 14 or older than 79; certain Canadian citizens; individuals admitted on certain visas for diplomats, employees of international organizations, and NATO employees; and certain Taiwan officials.

CENTER FOR DEMOCRACY & TECHNOLOGY

I. DHS again failed to provide the public a meaningful opportunity to review and comment on this proposed rule.

Typically, the administration should allow a comment period of at least 60 days following publication of a proposed rulemaking.[4] Without explanation—for the second time this fall and on a related matter,[5]—DHS arbitrarily limited the public review and comment period for this proposed rule to 30 days. This is inadequate in the best of times. However, the ongoing COVID-19 pandemic has strained the regular operation of nonprofits, and the lives of the public. In recognition of these challenges, members of both the House of Representatives and Senate wrote to the Office of Management and Budget requesting that additional time be afforded for the public to engage with the rulemaking process stating that "[t]he right of the American people to meet with federal agencies and comment on proposed actions is invariably affected by the ongoing pandemic."[6] And so it is with this proposed rule. CBP has done itself and the public a great disservice by rushing this process. This NPRM impacts everyone who desires to or must cross the United States border as it imposes a significant condition on such activity. It also impacts the lives of everyone in the United States as the collection it proposes risks greatly enhancing the surveillance capabilities of federal, state and local government.

II. Customs and Border Protection has exceeded its mandate by employing facial recognition technology on U.S. citizens.

DHS is congressionally mandated to deploy a biometric entry-exit system to record non-citizens' arrivals to and departures from the United States and it has delegated that responsibility to CBP. The purpose of this system is to identify terrorists, individuals traveling with fraudulent documents, and visa overstays.[7] Despite ample opportunity to do so,[8] in the last 16 years Congress never explicitly instructed DHS, and

---

[4] Executive Order No. 13,563 (2011)."To the extent feasible and permitted by law, each agency shall afford the public a meaningful opportunity to comment through the Internet on any proposed regulation, with a comment period that should generally be at least 60 days." Executive Order No. 12,866 (1993). "In addition, each agency should afford the public a meaningful opportunity to comment on any proposed regulation, which in most cases should include a comment period of not less than 60 days."

[5] *Notice of Proposed Rulemaking, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services*, 85 Fed. Reg. 56338-56422 (posted Sep. 11, 2020), https://www.govinfo.gov/content/pkg/FR-2020-09-11/pdf/2020-19145.pdf.

[6] Letter from House of Representatives Committee Chairs to Honorable Russell T. Vought, Acting Director, Office of Management and Budget (April 1, 2020), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/OMB.2020.4.1. Letter re Comment Period Extension.OI .pdf. *See also* Letter from Senators to Honorable Russell T. Vought, Acting Director, Office of Management and Budget (April 8, 2020), https://www.tomudall.senate.gov/imo/media/doc/4.8.20%20United%20States%20Senate%20Letter%20to%20OMB%20Acting%20Director%20Vought%20FINAL%5b1%5d.pdf.

[7] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458 (2004)("Congress finds that completing a biometric entry and exit data system as expeditiously as possible is an essential investment in efforts to protect the United States by preventing the entry of terrorists."). *See also*, Harrison Rudolph et al, Not Ready for Takeoff, Georgetown Center on Privacy & Technology, 5 (Dec. 21, 2017), https://www.airportfacescans.com/sites/default/files/Biometrics_Report__Not_Ready_For_Takeoff.pdf.

[8] *See e.g.,* Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004); Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007); Consolidated

later CBP, to include U.S. citizens in biometric entry-exit. In fact quite the opposite: numerous statements during the House Homeland Security Committee's hearings on the Department's use of facial recognition technology repeatedly made clear that U.S. citizens are not in-scope for the biometric entry-exit system.[9] And a DHS plan to mandate U.S. citizen inclusion in the system was met with swift condemnation.[10] Nonetheless, CBP has deployed facial recognition technology at U.S. land, sea and air ports of entry, collected biometric data from U.S. citizens, and proposes to make such collection more routine with this proposed rule. The Traveler Verification Service (TVS), CBP's cloud based facial matching service, currently and per the NPRM will continue to retain U.S. citizens' photographs in TVS for up to 12 hours.[11] CBP's biometric entry-exit system should not include U.S. citizens, period.

The NPRM and CBP attempt to cure this problem by noting that U.S. citizens will be permitted to exercise a right to opt-out of the system, and that CBP will not be retaining the new photographs captured at airports.[12] Public testimonials and a government review of CBP's existing pilot programs conclude the opt-out regime is, for practical purposes, non-existent. Many U.S. citizens have found it very difficult to opt-out of CBP's existing "voluntary" facial recognition pilot programs.[13] Additionally the Government Accountability Office (GAO) found that CBP's privacy signage (which is supposed to inform the traveling public about how to opt out of the use of facial recognition screening) was not consistently

---

Security, Disaster Assistance, and Continuing Appropriations Act, 2009, Pub. L. No. 110-329, 122 Stat. 3574 (2008); Consolidated and Further Continuing Appropriations Act, 2013, Pub. L. No. 113-6, 127 Stat. 198 (2013).

[9] *See e.g*, Questioning of Honorable Bennie Thompson, Chairman of House Committee on Homeland Security, House Committee on Homeland Security, About Face: Examining The Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies (July 10, 2019), https://homeland.house.gov/activities/hearings/about-face-examining-the-department-of-homeland-securitys-use-of-facial-recognition-and-other-biometric-technologies.

[10] *See e.g*, Press Release. *Senator Markey Blasts Homeland Security Proposal to Mandate Facial Recognition of all U.S. Citizens Traveling at Airports* (Dec. 3, 2019), https://www.markey.senate.gov/news/press-releases/senator-markey-blasts-homeland-security-proposal-to-mandate-facial-recognition-of-all-us-citizens-traveling-at-airports.

[11] 85 Fed. Reg. 74164.

[12] *Id*. at 74177.

[13] *See, e.g.,* Shaw Drake, *A Border Officer Told Me I Couldn't Opt Out of the Face Recognition Scan. They Were Wrong.*, ACLU Blog (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 ("If I, carrying all the privilege of a white American lawyer, could not opt-out of the invasive technology, what chance do other travelers—and particularly people of color—have to assert their rights before an agency patterned on racial profiling and harassment?"); 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/ ("Federal agencies and airlines claim that facial recognition is an opt-out system, but my recent experience suggests they are incentivizing travelers to have their faces scanned—and disincentivizing them to sidestep the tech—by not clearly communicating alternative options."); Aaron Sankin, *Can I Opt Out of Facial Scans at the Airport?,* The Markup (Mar. 2, 2020), https://themarkup.org/ask-the-markup/2020/03/02/can-i-opt-out-of-facial-scans-at-the-airport ("Yet, refusing a facial scan, anywhere in an airport, isn't always straightforward. Some travelers who have elected to do so report delays and confusion from airport staff, making each decision to opt out a bit of a gamble when you're racing to catch a flight.").

posted, the notices were not always current or complete, and that they were at times obscured.[14] The GAO issued two recommendations to CBP to address these shortcomings which still remain open.[15]

We take note of the agency's effort to better communicate with the public about the new screening program since the GAO issued its report.[16] But we also note that in the NPRM CBP troublingly observes: "[a]s biometric collection progresses, CBP believes that it will save travelers time. If this is the case, the alternative inspection process may be a slower process than the automated process, but every effort will be made to not delay or hinder travel."[17] Coercion through delay is unacceptable. CBP should have included in the NPRM a plan to dedicate sufficient resources at ports of entry to ensure that U.S. citizens can opt out of automated biometric screening without delay. Coercion can come from multiple sources: from a mandate, from the inherent difficulty in telling a government official "no",[18] from a lack of adequate notice about one's rights, from the fear that one may miss their flight, and from the fear that one may face heightened scrutiny for exercising a right that CBP views as an annoyance or with suspicion. Exercising this right may be unfathomable for those communities already subjected to heightened scrutiny when they travel due to racial or religious profiling.[19]

III. The Proposed Collection Is Deeply Intrusive on Privacy.

a. Fingerprints would be a less intrusive, and more effective biometric identifier around which to base the biometric entry-exit system.

CBP fails to fully justify its decision to collect and match facial images as opposed to using a less sensitive biometric identifier like fingerprints. CBP claims that fingerprint scans require more time to process than facial images, and that the equipment needed is "more expensive than facial recognition" but fails to provide a breakdown of these costs in the NPRM.[20] CBP then acknowledges repeatedly throughout the NPRM that fingerprints are already collected from travelers, that the pilots conducted using fingerprint

---

[14] GAO, *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, 39-46 (Sept. 2020), https://www.gao.gov/assets/710/709107.pdf.

[15] *Id*. at 72. "Recommendation: The Commissioner of CBP should ensure that the Biometric Entry-Exit Program's privacy notices contain complete and current information, including all of the locations where facial recognition is used and how travelers can request to opt out as appropriate." "Recommendation: The Commissioner of CBP should ensure that the Biometric Entry-Exit Program's privacy signage is consistently available at all locations where CBP is using facial recognition."

[16] Jordan Smith, *CBP Launches new Biometric Entry/Exit Information Website*, MeriTalk (Sep. 18, 2020), https://www.meritalk.com/articles/cbp-launches-new-biometric-entry-exit-information-website/.

[17] 85 Fed. Reg. 74177.

[18] *See e.g.*, Roseanna Sommers & Vanessa K. Bohns, *Would You Let the Police Search Your Phone*, N.Y. Times (April 30, 2019), https://www.nytimes.com/2019/04/30/opinion/police-phone-privacy.html.

[19] *See e.g.*, NPR Staff, *'Flying While Muslim': Profiling Fears After Arabic Speaker Removed From Plane*, NPR (April 20 2016), https://www.npr.org/2016/04/20/475015239/flying-while-muslim-profiling-fears-after-arabic-speaker-removed-from-plane; Zolan Kanno-Youngs, Mike Baker & Mariel Padilla, *U.S. Stops Dozens of Iranian-Americans Returning From Canada*, N.Y. Times (Jan. 5, 2020), https://www.nytimes.com/2020/01/05/us/politics/iranian-americans-border.html; Spencer Ackerman, *TSA Screening program risks racial profiling amid shaky science-study*, The Guardian (Feb. 8, 2017), https://www.theguardian.com/us-news/2017/feb/08/tsa-screening-racial-religious-profiling-aclu-study.

[20] 85 Fed. Reg. 74191.

screening were effective, and that the agency will continue to collect fingerprints.[21] Additionally in the NPRM, CBP attempts to justify the decision to move to face image capture by stating that fingerprint scanning is "more intrusive than taking a picture" and therefore presents "additional privacy concerns."[22] This is not the case, and even CBP elsewhere acknowledges the heightened sensitivity of using facial images in its Privacy Impact Assessment on TVS, "[a]s with all biometric modalities, facial recognition poses a unique set of privacy issues. Facial images can be captured at a distance, covertly, and without consent. Further, facial images are ubiquitous, and whereas individuals may take measures to avoid fingerprint and iris collection, there are fewer ways to hide one's face."[23] Fingerprints cannot be captured covertly and at the scale permitted by facial recognition technology. One need only peer at how China has leveraged facial recognition technology to oppress its minority Uighur population to understand the difference.[24] Instead of truly grappling with the long term privacy consequences of facial image capture and screening *en mass* at the border, the agency appears to have chosen the biometric easier to collect without traveler resistance. CBP observes that "[f]acial recognition has presented CBP with the best biometric approach because it can be performed relatively quickly, with a high degree of accuracy, and in a manner perceived as less invasive to the traveler (e.g., no actual physical contact is required to collect the biometric)."[25] Numbing people to the reality that they're engaging with a security process is not a valid excuse for collecting a biometric identifier more sensitive than fingerprints. Finally, fingerprint matching is a more mature science, and presents fewer concerns about the impact of aging or environmental factors on accuracy, nor does it raise the concerns about undemocratic and discriminatory inaccuracy raised by facial recognition technology that are discussed in this comment in Section IV.

b. Facial images captured by CBP at airports are vulnerable to broad sharing agreements.

The data CBP proposes to capture to facilitate identity verification will have a long shelf life, and will be put to far broader uses than ensuring a traveler carrying a passport is the passport's true owner. Facial images captured per this NPRM, including from green card holders, will be added to DHS's Automated Biometric Identification System database (IDENT), where the images will be stored for 75 years and subject to over broad routine sharing.[26] Indeed the textual changes to the regulation CBP seeks to introduce in the NPRM invite such overbreadth:, "DHS may require an alien to be photographed when departing the United States to determine his or her identity or for other lawful purposes."[27] The facial images will be available to other DHS agencies including Immigration and Customs Enforcement, which

[21] 85 Fed. Reg. 74173.
[22] 85 Fed. Reg. 74191.
[23] U.S. Dep't of Homeland Sec., U.S. Customs and Border Protection, *Privacy Impact Assessment for the Traveler Verification Service, DHS/CBP/PIA-0056*, 10 (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018.pdf.
[24] Paul Mozur, *One-Month, 500,000 Scans: How China Is Using A.I. To Profile a Minority*, N.Y. Times (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racialprofiling.html;
[25] U.S. Dep't of Homeland Sec., U.S. Customs and Border Protection, *Privacy Impact Assessment for the Traveler Verification Service, DHS/CBP/PIA-0056*, 10.
[26] U.S. Dep't of Homeland Sec., *Privacy Impact Assessment for the Automated Biometric Identification System (IDENT), DHS/NPPD/PIA-002*, 25 (Dec. 7, 2012), https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf.
[27] 85 Fed. Reg. 74192.

has pursued its own unregulated use of facial recognition technology,[28] as well as other federal agencies across the United States government and state and local law enforcement.[29] The collection and sharing of these images coupled with facial recognition technology will permit the government to track where people go, with whom they associate, and infer sensitive information about them. The technology's use on images captured from a protest could reveal one's political preferences, and from images captured at a place of worship one's religion. In short, absent guardrails,[30] CBP is building the foundation for a vast, unregulated surveillance apparatus in the United States—an apparatus which may chill the exercise of fundamental rights. And by compelling the collection of face images from lawful permanent residents and other non-U.S. citizens per this NPRM, CBP is also setting the stage for a U.S. surveillance environment that is particularly capable of identifying and tracking immigrants and communities of color, who are already targets of disproportionate policing and government scrutiny.[31] DHS in particular has proposed a particularly harrowing vision of the future of its activities, including implementing a program of "continuous vetting" that would subject immigrants to "continued and subsequent evaluation" by the government.[32] The NPRM fails to address the surveillance friendly environment CBP is building, nor are these concerns mitigated by CBP's existing PIA for the TVS.

c. The collection described in the NPRM presents inherent security risks.

The data CBP seeks to compel leaves the data subjects vulnerable if that information is inappropriately accessed. Unlike passwords or even social security numbers, biometric information cannot be changed if it is compromised in a data breach. Once a person's biometric information is obtained by an unauthorized party, it is obtained irrevocably. In the hands of a third party entity, this data could result in identity fraud, or other harms. And there is reason to doubt the government's ability to safeguard personal information. For example, the Office of Personnel Management breach in 2015 resulted in the

---

[28] U.S. Dep't of Homeland Sec., U.S. Immigration and Customs Enforcement, *Privacy Impact Assessment for the ICE use of Facial Recognition Services, DHS/ICE/PIA-054* (May 13, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf; Drew Harwell & Erin Cox, *ICE has run facial-recognition searches on millions of Maryland drivers*, WaPo (Feb. 26, 2020), https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/.

[29] U.S. Dep't of Homeland Sec., *Privacy Impact Assessment for the Automated Biometric Identification System (IDENT), DHS/NPPD/PIA-002*, 3.

[30] That we describe in Section V.

[31] *See e.g.*, Dominic-Madori Davis, *FBI reportedly used top spy plane to monitor Black Lives Matter protests*, Business Insider (Jun. 21, 2020), https://www.businessinsider.com/fbi-used-spy-plane-to-monitor-black-lives-matter-protests-2020-6; Chantal Da Silva, *Documents on Fed Surveillance of BLM Protests Spark Privacy Concerns*, Newsweek (Aug. 16, 2020), https://www.newsweek.com/documents-fed-surveillance-blm-protests-spark-privacy-concerns-1525372; Joan Friedland, *The Trump Administration is Collecting Massive Amounts of Data for Its Immigrant Surveillance and Deportation Machine*, NILC (Aug. 22, 2018), https://www.nilc.org/2018/08/22/information-vacuuming-immigrants-and-citizens/.

[32] *Collection and Use of Biometrics by U.S. Citizenship and Immigration Services*, 85 Fed. Reg. 56338-56422 (posted Sep. 11, 2020) https://www.govinfo.gov/content/pkg/FR-2020-09-11/pdf/2020-19145.pdf (a recent DHS proposed rule to massively expand the categories of persons subject to biometrics collection, expand the types of biometric identifiers that may be compelled, and expand the purposes for which such data is compelled); Comment of the Center for Democracy & Technology in response to 85 Fed. Reg. 56338-56422 (Oct. 12, 2020), https://cdt.org/wp-content/uploads/2020/10/2020-10-12-CDT-Comment-in-Response-to-DHS-Docket-No-USCIS-2019-0007.pdf.

disclosure of sensitive information about 22.1 million people, including 1.1 million sets of fingerprints.[33] In 2019 at DHS, a database of 184,000 facial recognition images collected by Customs and Border Protection in Texas was hacked and misused.[34] At least 19 of the images were posted on the dark web. In a report on the incident, the DHS Inspector General found that CBP did not satisfy its own security obligations, thereby creating the situation that led to the data breach, and the Inspector General acknowledged that "this incident may damage the public's trust in the Government's ability to safeguard biometric data."[35] According to the GAO, as part of its review of CBP's biometric entry exit system, CBP has not yet fulfilled all of its cybersecurity requirements, and has not yet completed necessary cybersecurity resiliency testing.[36] And in the midst of submitting this comment, DHS and other federal agencies are dealing with a newly discovered sophisticated cyber breach that has significantly compromised many government systems.[37] None of this builds confidence in DHS's ability to keep secure a massive biometric database, nor is this issue adequately addressed in the NPRM.

Additionally, in order to meet the challenges of scale and integration into airport environments, CBP relies on airlines to capture and submit photos of travelers for identity verification.[38] As a condition of these partnerships, CBP requires the airlines to sign business agreements which prohibit the retention of traveler photos taken on behalf of CBP. A recent GAO report found that CBP had "audited only one of its more than 20 airline partners" to assess compliance with CBP's privacy requirements, and that CBP "did not have a plan to ensure all partners are audited."[39] According to the same report in general "CBP has not yet developed a plan that identifies the time frames for auditing all contractors and vendors for compliance with privacy and security requirements."[40] The GAO issued a recommendation on this score, which like the others it has recently issued, remains open.[41] CBP's plans for expansion rely heavily on these private partnerships and the challenges with auditing for compliance will only grow. The NPRM fails to detail how CBP can or will address this challenge.

---

[33] Ellen Nakashima, *Hacks of OPM databases compromised 22.1 million people, federal authorities say*, WaPo (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

[34] Drew Harwell & Geoffrey Fowler, *U.S. Customs and Border Protection says photos of travelers were taken in a data breach*, WaPo (Jun. 10, 2019), https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/.

[35] *Review of CBPs Major Cybersecurity Incident during a 2019 Biometric Pilot*, Office of Inspector General (Sept. 21, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

[36] GAO, *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, 3, 85 (Sept. 2020).

[37] Jack Stubbs et al., *U.S. Homeland Security, Thousands of Businesses Scramble After Suspected Russian Hack*, Reuters (Dec. 14, 2020), https://www.reuters.com/article/global-cyber/u-s-homeland-security-thousands-of-businesses-scramble-after-suspected-russian-hack-idUSKBN28O1Z3; David Sanger & Nicole Perlroth, *More Hacking Attacks Found as Officials Warn of 'Grave Risk' to U.S. Government*, N.Y. Times (Dec. 17, 2020), https://www.nytimes.com/2020/12/17/us/politics/russia-cyber-hack-trump.html.

[38] 85 Fed. Reg. 74173.

[39] GAO, *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, 36 (Sept. 2020).

[40] *Id*. at 48.

[41] *Id*. at 72. "Recommendation: The Commissioner of CBP should direct the Biometric Entry-Exit Program to develop and implement a plan to conduct privacy audits of its commercial partners', contractors', and vendors' use of personally identifiable information."

IV. Expansion from the pilot phase is unwarranted given the outstanding uncertainty that the biometric entry-exist system can meet its stated goals.

In order to create a system that tracks visa overstays, uniform biometric collection must exist at 328 air, land and sea ports of entry.[42] CBP's proposal to expand this program beyond the pilot at 15 commercial airport ports of entry is premature as it currently has no plan for biometric collection at private airports or land and sea ports, and it has yet to demonstrate that its use of facial recognition provides an equitable experience for all who travel.

a. CBP has not developed a nation-wide strategy for implementing a biometric entry-exit system, and has not addressed government-identified privacy and security shortcomings in its pilot program.

CBP does not yet have a plan for a uniform biometric entry-exit system across air, land and sea ports of entry. CBP proposes to move forward with the installation of its facial recognition system across all airports within the next five years, and "[f]or land and sea ports of entry and private aircraft, CBP plans to continue to test and refine biometric exit strategies with the ultimate goal of implementing a comprehensive biometric entry-exit system nationwide."[43] In the absence of a tested and compatible solution at land and sea ports, it is not appropriate for CBP to forge ahead across all airports, and cement a collection and matching program that it may not be possible to operationalize at land and sea ports. CBP's current authorizing regulation permits testing at sea, air and land ports of entry, and indeed the NPRM describes CBP's various pilots at these environments.[44]

Additionally, as referenced throughout this comment, the Government Accountability Office recently evaluated CBP's biometric entry exit system and identified several shortcomings with the execution of the program. There are still 6 outstanding recommendations that need to be addressed related to issues of privacy and security.[45] Expanding the program before addressing these problems is also premature.

b. CBP must prove that facial recognition technology provides an equitable experience for everyone, including for people of color, women, young people and transgender individuals.

Government and private testing of popular commercial facial recognition algorithms have exposed undemocratic demographic effects—specifically the fact that the technology is less accurate when used on images of people of color and women, as compared to white persons and men. According to a study by the National Institute of Science and Technology (NIST), Black and Asian people are up to 100 more times likely to be misidentified by a facial recognition system than white men, depending on the

---

[42] U.S. Customs and Border Protection, *At Ports of Entry* (last accessed Dec. 20, 2020), https://www.cbp.gov/border-security/ports-entry - :~:text=CBP provides security and facilitation,of entry throughout the country.
[43] 85 Fed. Reg. 74175.
[44] *Id*. at 74169-74173.
[45] GAO, *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, 72 (Sept. 2020).

algorithm and use case.[46] Additionally, CBP proposes to subject children under the age of 14 to this system. The same NIST study found that the vast majority of more than 100 facial recognition algorithms had a higher rate of mistaken matches among children as compared to adults.[47] Finally, studies have demonstrated the facial recognition technology is less accurate when used on transgender, gender nonconforming, and transitioning individuals.[48]

We acknowledge that as of March 2020 CBP began using one of the better performing algorithms that NIST tested in its 2019 report identifying demographic effects in facial recognition algorithms.[49] However, NIST's tests were conducted in a lab, not in the field. And the accuracy of a facial recognition system depends greatly on environmental and human factors, the hardware, and the thresholds that are set by the operator. Operational testing is therefore needed to reflect the true accuracy of the deployment. In December 2018, NIST entered into an agreement with CBP to specifically assess the accuracy of its algorithm, including the impacts of gender, ethnicity and age on matching accuracy in the field. NIST is to provide recommendations to CBP related to the algorithm the agency uses, optimal thresholds. According to a GAO report, NIST's work was delayed by the pandemic, and a new completion date for this study is unknown.[50]

Other operational field testing raises doubts about the program's ability to work as intended. A September 2018 Inspector General report observed that "due to missing or poor quality digital images, CBP could not consistently match individuals of certain age groups or nationalities" and the 2017 match rate "limited biometric confirmation to only 85 percent of all passengers processed."[51] And more recently the same GAO review described throughout this comment observed the use of CBP's facial recognition program during boarding procedures for five departing flights. For one of these flights, CBP's program "was unable to match approximately 25 percent of travelers, even after repeated attempts."[52] An August 2019 test of one of CBP's programs did conclude that the CBP was able to correctly match

[46] Patrick Grother, Mei Ngan, Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280, Nat'l Inst. of Standards and Technology (December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[47] *Id*.
[48] Jesse Damiani, *New Research Reveals Facial Recognition Software Misclassifies Transgender, Non-Binary People*, Forbes (Oct. 19, 2019), https://www.forbes.com/sites/jessedamiani/2019/10/29/new-research-reveals-facial-recognition-software-misclassifies-transgender-non-binary-people/?sh=67fd9f38606b.
[49] Patrick Grother, Mei Ngan, Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280, Nat'l Inst. of Standards and Technology (December 2019).
[50] GAO, *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, 52 (Sept. 2020).
[51] U.S. Dep't of Homeland Sec., Office of Inspector General, OIG-18-80, *Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide*, 6 (Sept. 21, 2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf.
[52] GAO, Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues, 53 (Sept. 2020).

98% of travelers.[53] However, on a typical day in 2019, a 2% error rate would have spelled inconvenience or worse for over 20,000 travelers.[54]

There are other outstanding questions about the implementation of this technology. The current plan for this system is that in the case of a no-match determination, a traveler will be directed to an officer for a manual review of their documents. A no-match determination by computer may influence human screeners' decisions. Research conducted by NIST and others has shown that people are likely to believe computer-generated results[55] raising the risk that human screeners will hesitate to overturn a false no-match finding by the algorithm. No testing appears to have been done, or is being planned to study this aspect of the human-technology interaction, and such study is needed.

The consequence for travelers in the case of algorithmic errors, human bias, or an inability of the camera to capture an image of them are significant: if they are not accurately identified they may be delayed, miss their flight, or face a custodial interrogation. A key element of this program remains cloaked in uncertainty and CBP should withdraw this proposal until it can prove that its technology works and provides an equitable experience for all. This includes waiting for NIST to conclude its testing of CBP's system, described above.

V. CBP's Biometric Entry-Exit System is prone to mission creep and is in need of guardrails.

We have significant concerns if the program moves forward as contemplated in the NPRM. CBP has not proffered any measures to limit the function of this system to identity verification, or prevent the distribution and repurposing of facial images collected throughout DHS and other government entities. And given the money, time and resources expended on biometric entry-exit thus far there will be a temptation to expand the uses to which the images and facial recognition technology is put, and those uses will extend beyond the goal of verifying the identification of travelers. This is already occurring:

> "CBP collects information under this process in order to verify the identities of travelers departing the United States; however, CBP uses border crossing information more broadly. CBP creates entry and exit records primarily in support of its mission to facilitate legitimate travel and enforce immigration laws, which include activities related to counterterrorism and immigration enforcement. CBP may share information with federal, state, and local authorities, which may be authorized to use the information for purposes beyond the scope of CBP's mission."[56]

---

[53] *Id*. at 51.

[54] U.S. Customs and Border Protection, *On a Typical Day in Fiscal year 2019, CBP…* (last accessed Dec. 21, 2020), https://www.cbp.gov/newsroom/stats/typical-day-fy2019#:~:text=PROCESSED%3A,international%20air%20passengers%20and%20crew.

[55] John J. Howard et al., *Human-Algorithm Teaming in Face Recognition: How Algorithm Outcomes Cognitively Bias Human Decision-Making*, PLOS ONE (2020), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0237855.

[56] U.S. Dep't of Homeland Sec., U.S. Customs and Border Protection, *Privacy Impact Assessment for the Traveler Verification Service, DHS/CBP/PIA-0056*, 13.

And the language in the proposed changes in this NPRM points to this direction of travel. CBP seeks to amend the existing regulations to broadly justify the collection of biometric data from all non-U.S. citizens:

> **§ 215.8 Requirements for biometrics from aliens on departure from the United States**
> 1) Photographs. DHS may require an alien to be photographed when departing the United States to determine his or her identity **or for other lawful purposes**.[57] (bold added)

The NPRM includes nothing that would bar the government from expanding the system from identity-verification to a lookout system for warrants, terrorist watchlists, or images of individuals who are perceived as persons of interest. [58] Warrant databases as well as criminal record databases are error prone.[59] Connecting the two systems would exacerbate the negative experiences of communities of color who are already disproportionality represented in these systems due to historic racial disparities in policing and increase the risks to travelers of a mistaken match. We urge CBP to strip out in the proposed regulation the "or for other lawful purposes" language cited to above as disproportionately intrusive and unnecessary for the system it is developing. And if the NPRM is approved we urge CBP to limit the sharing and use of data collected at ports of entry to verify that the traveler presenting for entry or exit at a port of entry is the true owner of the travel document they carry. Border crossing screening should not supercharge the surveillance capabilities of other elements of government.

Additionally, CBP suggests in the NPRM that the Transportation Security Agency's (TSA) adoption of its facial recognition system would be a cost saving and an added benefit of the rule.[60] It would be wildly inappropriate for the TSA to adopt CBP's system for domestic air travel. Setting aside the question of whether or not facial recognition technology is accurate and equitable, generally, TSA lacks the same authority as CBP to compel this data from all domestic travelers. Furthermore, CBP's is not a model of identity verification the TSA should adopt. Instead, if this is an area of interest for the agency, TSA should only consider designs that process a 1:1 match between a live photograph of the passenger and the photo on their identification document, without the retention of the live photograph. We understand this is one of the pilots TSA is testing.[61] CBP and leadership at DHS are discouraged from seeking to justify this NPRM by securing TSA's adoption of the system in domestic airports.

---

[57] 85 Fed. Reg. 74192.

[58] Homeland Security Advisory Council, *Final Report of the Biometrics Subcommittee*, 35 (Nov. 12, 2020) https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf.

[59] See e.g., Alen Feur, *Cleared of a Crime but Hounded by a Warrant*, N.Y. Times (March 28, 2016), https://www.nytimes.com/2016/03/29/nyregion/cleared-of-a-crime-but-hounded-by-a-warrant.html; Legal Action Rap Center, *The Problem of RAP Sheet Errors: An Analysis* (July 2014), https://lac.org/wpcontent/uploads/2014/07/LAC_rap_sheet_report_final_2013.pdf; Elizabeth Joh, *Wrongful Arrest by Software*, Slate (Dec. 13, 2016), nhttp://www.slate.com/articles/technology/future_tense/2016/12/software_problems_are_leading_to_wrongful_arrests.html.

[60] 85 Fed. Reg. 74189.

[61] U.S. Dep't Homeland Sec., Transportation Security Administration, *Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Verification, DHS/TSA/PIA-046(b)* (June 3, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa046b-tdc-june2020.pdf.

CENTER FOR
DEMOCRACY
& TECHNOLOGY

* * *

Biometric identity verification technology may enhance the speed, integrity and security of air travel. These would be benefits for the government and the public alike. However, as DHS's biometric entry-exit system is currently designed, the benefits the public might one day reap are not at all worth the high cost. DHS's is the first biometric screening checkpoint in the United States. It is precedent setting, and unfortunately a big bloated model of how not to design and administer a biometric screening process. We oppose this NPRM and urge you to withdraw it. Questions about this comment can be directed to the Center for Democracy & Technology's Policy Counsel, Mana Azarmi at mazarmi@cdt.org or Senior Counsel and Director of the Freedom, Security & Technology Project, Gregory Nojeim at gnojeim@cdt.org.

Sincerely,

Mana Azarmi
Gregory Nojeim

Center for Democracy & Technology