December 21, 2020

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

Submitted via http://www.regulations.gov

Comment of Civil Society Organizations in Opposition to 85 Fed. Reg. 74162, Docket No. USCBP-2020-0062, RIN 1651-AB12, Doc. No. 2020-24707, Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States

Dear Regulations Docket Clerk:

The American Civil Liberties Union (ACLU), ACLU of Illinois, ACLU of Massachusetts, ACLU of New York, ACLU of Northern California, ACLU of San Diego & Imperial Counties, ACLU of Texas, ACLU of Washington, Advocacy for Principled Action in Government, Defending Rights & Dissent, Electronic Frontier Foundation, Fight for the Future, The Freedom to Read Foundation, Immigrant Legal Resource Center, National Immigration Law Center, and Open MIC (Open Media & Information Companies Initiative) submit this comment in strong opposition to the above-referenced Notice of Proposed Rulemaking (NPRM), published at 85 Fed. Reg. 74162 (proposed Nov. 19, 2020).

For several reasons, the Department of Homeland Security (DHS) should immediately rescind its proposed regulations, which would massively expand the government's use of facial recognition technology, endangering the rights of tens of millions of immigrants and visitors to the United States. First, the proposed regulations exceed DHS's authority, because Congress never intended to authorize DHS to use face recognition on people entering and leaving the United States. Second, the proposed regulations would enable the government's surveillance and tracking of people on an unprecedented scale—with the harms disproportionately affecting immigrants and communities of color. Third, facial recognition technology is prone to error—and, again, the harms disproportionately affect people of color, as well as people who are transgender, young, or elderly. Fourth, DHS's proposed deployment of facial recognition technology is not justified by the government's stated goals. Finally, DHS's proposed authorization of other, unspecified forms of future biometric collection presents profound risks to privacy and civil liberties.

DHS's current regulations authorize Customs and Border Protection (CBP) to require "fingerprints, photograph(s) or other specified biometric identifiers" from certain categories of non-U.S. citizens seeking admission to the United States, known as "in-scope" travelers.[1] The

[1] 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

regulations also authorize CBP to require "fingerprints, photograph(s) or other specified biometric identifiers" from these travelers upon departure from the United States through pilot projects at land border ports and up to 15 air and seaports.[2] Today, when in-scope travelers arrive in the United States, CBP collects their fingerprints to biometrically verify their identity. Most non-U.S. citizens arriving in the United States are also "subject to being photographed" by CBP.[3] In contrast, when travelers depart the United States, CBP does not routinely inspect them.

Over the past several years, CBP has tested the use of facial recognition technology on travelers entering and departing from the United States, and it now seeks to dramatically expand its use of this technology.[4] Under the text of the new proposed regulations, *all* non-U.S. citizens —including children—may be required to be photographed upon both entry *and* departure from the United States.[5] While this would represent a significant expansion of CBP's authority, the agency's immediate plans, as described in the NPRM, go even farther than the text of the proposed regulations would suggest.[6]

In practice, CBP will not merely photograph travelers. Instead, according to the NPRM, CBP intends to collect "faceprints"—precise measurements of the unique facial geometry of each non-U.S. citizen traveler.[7] These faceprints are mathematical representations of individuals' faces that CBP will collect and store in a DHS database for up to 75 years, where they may be used not only by DHS, but by foreign governments and federal, state, and local law enforcement to identify individuals for a variety of purposes, far removed from the reasons for CBP's initial collection. The NPRM explains that CBP also intends to apply a face-matching algorithm to non-U.S. citizen travelers, which will compare a traveler's faceprint to a gallery of other images of the traveler in the government's possession.

The face surveillance envisioned by the NPRM would pose grave risks to privacy and civil liberties—including harms from law enforcement agencies in the United States and foreign government agencies with which faceprints are shared. Facial geometry is biologically unique to each person and it is largely immutable. Unlike other forms of identity verification, faceprints can be collected covertly, at a distance, and without consent. And because people's faces are typically exposed, it is virtually impossible to insulate ourselves from unjustified surveillance and resulting harms. Once the government acquires a person's faceprint and associates that

---

79; certain Canadian citizens; individuals admitted on certain visas for diplomats, employees of international organizations, and NATO employees; and certain Taiwan officials.

[2] 8 C.F.R. § 215.8(a).

[3] Collection of Biometric Data from Aliens Upon Entry to and Departure From the United States, 85 Fed. Reg. 74162, 74175 (Nov. 19, 2020).

[4] DHS, *TSA and CBP: Deployment of Biometric Technologies, Report to Congress* 3, https://www.tsa.gov/sites/default/files/biometricsreport.pdf.

[5] The sole exception is for non-citizen U.S. nationals, *i.e.*, individuals born in American Samoa or on Swains Island to parents who are not citizens of the United States. *See* 85 Fed. Reg. 74178.

[6] 85 Fed. Reg. 74163.

[7] *Id.*

information with a name and other identifying details, it creates a risk of a unique and unprecedented form of persistent surveillance, one that allows the government to identify and track people without their knowledge. CBP's collection of faceprints could enable systematic surveillance by other government agencies and foreign governments. It could expose where people go, who they associate with, and even what they believe, based on the religious services, protests, or meetings they attend.

Critically, the harms of this surveillance technology will disproportionately affect immigrants and communities of color. Several recent studies have shown that facial recognition technology results in a higher rate of false identifications for people of color. For example, in December 2019, the National Institute of Standards and Technology (NIST) released results from a comprehensive study of facial recognition systems, concluding that Black and Asian people were up to 100 times more likely to be misidentified than white men, depending on the algorithm and other factors.[8] In the border context, face-matching errors could lead to lengthy interrogations, missed flights, and even wrongful deportations. Moreover, faulty facial recognition technology could provide a pretext for subjecting people of color and religious minorities to additional screening and harassment. And regardless of the accuracy of CBP's face-matching technology, DHS's retention and sharing of travelers' faceprints for up to 75 years will facilitate unjustified law enforcement scrutiny of immigrant and other communities subject to the proposed regulations.

Our concerns are heightened in light of CBP's record, including its role in family separation, history of detaining people in horrific conditions, use of lethal force, and racial and religious profiling. It is not difficult to imagine faulty facial recognition technology and face-matching errors leading CBP agents to detain elderly and other vulnerable individuals at airports for hours without access to a lawyer, to subject people to extensive questioning about their political opinions and views, and to conduct searches of individuals' devices in violation of the Fourth Amendment.

The NPRM is also premature. Under an agreement with CBP, NIST is currently evaluating the accuracy of an algorithm similar to the one that CBP has been using in its face surveillance pilot programs. NIST's study will analyze the impacts of gender, ethnicity, and age on matching accuracy. Although NIST had anticipated that its work would be complete in the spring of 2020, its results have been delayed by the coronavirus pandemic. The proposed regulations should not be rushed forward before NIST completes its assessment of the potential discriminatory impact of CBP's face-matching algorithm.

In addition, the NPRM is defective because DHS published it under the purported authority of Chad Wolf, Acting Secretary of Homeland Security, and a federal court has ruled

[8] NIST, *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software; *see also* GAO, *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues* 76 (Sept. 2020) ("GAO Report"), https://www.gao.gov/assets/710/709107.pdf.

that Mr. Wolf's appointment as Acting Secretary was unlawful.[9] Three other federal courts have concluded that Mr. Wolf's appointment as Acting Secretary was likely unlawful, and on that basis, have preliminarily enjoined DHS policy changes proposed under his authority.[10] Given the defects in Mr. Wolf's appointment, he cannot exercise the authority of the Acting Secretary, and, accordingly, the NPRM has no legal effect.

At bottom, CBP's deployment of this novel technology is out of proportion to any legitimate government purpose. CBP officials have explained that one of the primary purposes behind the deployment of facial recognition technology is to comply with a congressional mandate to create a biometric entry-exit system.[11] However, as discussed below, Congress never intended to authorize DHS to collect *faceprints*, let alone mandated it. In addition, in December 2019, the Director of the Office of Test and Evaluation for DHS reviewed CBP's facial recognition tests for departing flights, and concluded that the program "did not provide clear, measurable benefits to CBP's existing operations at airports," and "did not change or enhance the day-to-day capabilities of CBP officers."[12] In the NPRM, DHS asserts that the ability to confirm the departure of foreign nationals will help the agency "detect overstays and aliens who are or were present in the United States without having been admitted or paroled."[13] At the same time, the NPRM acknowledges that most overstays are brief and accidental.[14] In this context, the use of face recognition is plainly disproportionate. The NPRM also fails to adequately evaluate the costs and benefits of collecting faceprints relative to fingerprints, which are less prone to abusive and far-reaching forms of government surveillance.

CBP's proposed use of face surveillance at airports, sea ports, and the land border would put the United States on an extraordinarily dangerous path toward the normalization of this surveillance, and raises profound civil liberties concerns. The deployment of this society-changing technology is unnecessary and unjustified.

I. The proposed regulations exceed DHS's authority because Congress never intended to authorize DHS to collect faceprints as part of an entry-exit system.

The proposed regulations exceed DHS's authority because Congress never intended to authorize DHS to collect faceprints as part of an entry-exit system. Although Congress has required DHS to establish an entry-exit system that uses "biometric" data, it has never defined "biometric" in this context to encompass the collection of faceprints. The primary statute at issue, 8 U.S.C. § 1365b, was passed in 2004—more than a decade before facial recognition

[9] *Batalla Vidal v. Wolf*, No. 16CV4756NGGVMS, 2020 WL 6695076, at *9 (E.D.N.Y. Nov. 14, 2020).

[10] *Immigrant Legal Res. Ctr. v. Wolf*, No. 20-CV-05883-JSW, 2020 WL 5798269, at *9 (N.D. Cal. Sept. 29, 2020); *Casa de Maryland, Inc. v. Wolf*, No. 8:20-CV-02118-PX, 2020 WL 5500165, at *23 (D. Md. Sept. 11, 2020); *Nw. Immigrant Rights Project v. United States Citizenship & Immigration Servs.*, No. CV 19-3283 (RDM), 2020 WL 5995206, at *13 (D.D.C. Oct. 8, 2020).

[11] GAO Report 56.

[12] *Id.* at 55.

[13] 85 Fed. Reg. 74164.

[14] *Id.*

technology was ready for CBP testing in the airport environment.[15] By requiring, in 2004, the creation of an entry-exit system that uses "biometric" data, Congress plainly did not intend to authorize DHS's collection of any and all biometrics in perpetuity, in known and unknown forms. Indeed, as explained below, statutory reporting requirements that Congress established in 2018 make clear that CBP's deployment of face recognition would constitute an "expansion" of the biometrics collection authorized in 2004.[16]

Moreover, unlike the collection of fingerprints, the collection of faceprints grants the government extraordinary and unprecedented powers to conduct persistent, secret surveillance of public movements. *See infra* Sections II & IV. The widespread adoption of facial recognition technology would fundamentally change the nature of freedom and privacy in this country. For this reason alone, CBP should not deploy this technology without express authorization from Congress.

In 1996, Congress required the Attorney General to establish an integrated, electronic entry-exit system applicable to foreign nationals, and in 2000, it reiterated that requirement. *See* 8 U.S.C. § 1365a; *see also* 110 Stat. 3009–546; 114 Stat. 337. In 2001, as part of the Patriot Act, Congress specified that the Attorney General and Secretary of State should focus on the utilization of "biometric technology" in the entry-exit system. 115 Stat. 272, 353. In 2004, Congress specified that the entry-exit system should require the collection of "biometric exit data" and use an identity number "tied to an applicant's biometric algorithm." 8 U.S.C. § 1365b(d), (g)(2). Congress also transferred responsibility for implementing the biometric entry-exit system to DHS, and in subsequent years, required DHS to submit a comprehensive plan for the entry-exit system required under the 2004 law.[17]

In none of these statutes (nor any other tangential statute cited in the NPRM) did Congress expressly authorize the collection of faceprints as part of the entry-exit system. In fact, as part of the 2001 Patriot Act, Congress equated "biometric identifiers" with fingerprints. It required the Attorney General and other officials to conduct a study on the feasibility of using a "biometric identifier (fingerprint) scanning system" at points of entry into the United States to enhance the ability of immigration officials to "identify aliens who may be wanted in connection with criminal or terrorist investigations." 115 Stat. 272, 395.[18]

Requirements that Congress enacted in 2018 show that CBP's collection of faceprints would constitute a biometrics expansion, beyond what Congress authorized in 2004. In 6 U.S.C. § 1118, in a section titled "Biometrics expansion," Congress required CBP to study and prepare a

[15] *Id.* (citing 8 U.S.C. § 1365b).

[16] 6 U.S.C. § 1118.

[17] In 2016, Congress required DHS to submit a "comprehensive plan for implementation of the biometric entry and exit data system as required under this heading in Public Law 114-4." 129 Stat. 2242, 2493. The relevant portion of Public Law 114-4 requires DHS to submit its plan for the entry-exit system "required under section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (8 U.S.C. § 1365b)."

[18] Similarly, as part of the 1996 act referenced above, Congress specified that border crossing identification cards should include "a biometric identifier (such as the fingerprint or handprint of the alien)." 8 U.S.C. § 1101(a)(6).

report addressing several concerns about the potential expanded use of biometrics, and in particular facial recognition technology—including error rates by race, gender, and age; burdens on travelers; and the effects of facial recognition technology on privacy. These are precisely the type of reporting requirements that one would expect before Congress authorized CBP's deployment of a novel, unproven technology. Congress also confirmed that this reporting requirement concerning the potential expansion of biometric collection should not be read as *authorizing* that expansion. In particular, it confirmed that CBP's authority to collect "biometrics" is limited to the authority granted by 2004 statute. *See* 6 U.S.C. § 1118(b) ("Nothing in this section shall be construed to permit the Commissioner of U.S. Customs and Border Protection to facilitate or expand the deployment of biometric technologies, or otherwise collect, use, or retain biometrics, not authorized by any provision of or amendment made by the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458; 118 Stat. 3638) . . . .").[19] The clear implication of 6 U.S.C. § 1118(b) is that the collection of faceprints was not, in fact, authorized by Congress in 2004. If the 2004 statute had authorized the use of facial recognition technology as part of an entry-exit system, then 6 U.S.C. § 1118(b) would be superfluous.

The NPRM also cites several provisions of the Immigration and Nationality Act as a statutory basis for the collection of faceprints.[20] But none of those provisions authorize the collection of particular forms of biometric data, with the exception of fingerprints. *See* 8 U.S.C. § 1303(a). And DHS cannot rely on general statutory text authorizing the Department to collect "evidence" concerning immigration, 8 U.S.C. § 1357(b), to justify intrusive forms of biometric collection that were not specifically authorized by Congress.

The lack of express authorization for the collection of faceprints is unsurprising. As the NPRM acknowledges, "[t]he facial recognition technology required to reliably implement biometric exit processes into existing traveler flows has not been available until recently"—yet the primary statutory authority that DHS relies upon was enacted in 2004.[21] Indeed, according to the NPRM, DHS did not deploy facial recognition technology as part of entry-exit procedures until 2015. That year, DHS specified in the Federal Register for the first time that its biometric collection encompassed the collection of "facial and iris images" in addition to "photographs."[22] The fact that DHS itself distinguished between these two categories makes plain that any implicit congressional authorization for DHS's collection of "photographs" does not encompass the acquisition of *faceprints*.

---

[19] Section 1118(b) similarly confines CBP's collection of biometric data to the authority granted by the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53; 121 Stat. 266 (8 U.S.C. § 1187). In pertinent part, that Act requires DHS to "establish an exit system" that uses biometric information to confirm that participants in the visa-waiver program have left the country. 8 U.S.C. § 1187(i)(2). It contains no reference to faceprints or facial recognition technology.

[20] *See* 85 Fed. Reg. 74165.

[21] 85 Fed. Reg. 74170, 74164.

[22] Test to Collect Biometric Information at the Otay Mesa Port-of-Entry, 80 Fed. Reg. 70241 (Nov. 13, 2015).

II. The NPRM fails to account for profound harms to privacy and creates new risks of misuse.

The NPRM completely fails to account for the fact that CBP's deployment of facial recognition technology would threaten civil liberties on a massive scale, by undermining travelers' privacy and creating new risks of surveillance and abuse. In the NPRM, CBP observes that travelers subject to face recognition may "perceive" a loss of privacy,[23] but the harms are not merely perceptual ones. By collecting and retaining faceprints for up to 75 years, and by sharing this information with foreign governments, contractors, and federal, state, and local law enforcement, CBP would create a vast surveillance and tracking apparatus—one that would operate far beyond the U.S. border. CBP's collection of faceprints could enable systematic surveillance by other government agencies and expose where people go, who they associate with, and even what they believe, based on the religious services, protests, or meetings they attend. And it would invariably lead to increased government scrutiny, surveillance, and investigation of immigrants and people of color.

Under the proposed regulations, faceprints collected by CBP would feed into a broader ecosystem of DHS data, and would facilitate surveillance by foreign governments and law enforcement agencies across the country. CBP would add travelers' faceprints to DHS's expansive Automated Biometric Identification System database (IDENT), which stores data ranging from names and nationalities to fingerprints, personal physical details, and data from DHS or law enforcement encounters—resulting in comprehensive, detailed profiles of individuals.[24] DHS, including Immigration and Customs Enforcement (ICE), can then use faceprints collected by CBP, together with the accompanying profiles, during agents' subsequent interactions with travelers, and numerous other government agencies can access this data as well.[25]

CBP's acquisition of tens of millions of faceprints each year opens the door to wide-ranging surveillance by governments and private actors, with significant implications for constitutional rights.[26] Face recognition could be deployed on photos or videos going back years—or even on live video—to identify people who attended, for instance, religious services,

---

[23] 85 Fed. Reg. 74186.

[24] *See, e.g.*, DHS, Privacy Act: IDENT System of Records, 72 Fed. Reg. 31080, 31081 (June 5, 2007). DHS is currently building a new biometrics database, called Homeland Advanced Recognition Technology (HART), to replace IDENT. HART will, at a minimum, contain biometric, biographic, and encounter information and will enable enhanced data-sharing with other DHS components and other domestic and international agencies. *See* Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART) Increment 1 PIA DHS/OBIM/PIA-004 31-34 (Feb. 24, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf (describing several privacy risks associated with the database that, according to DHS, have been only "partially mitigated" or not mitigated at all).

[25] *See, e.g.*, DHS, Privacy Impact Assessment for the Automated Biometric Identification System (IDENT), DHS/NPPD/PIA-002 3–5 (Dec. 7, 2012); 85 Fed. Reg. 56349.

[26] Jay Stanley, *ACLU White Paper: U.S. Customs & Border Protection's Airport Face Recognition Program* (Feb. 2020), https://www.aclu.org/other/aclu-white-paper-cbps-airport-face-recognition-program.

political fundraisers, Black Lives Matter protests, or gunshows.[27] The government has already deployed this technology to surveil demonstrators exercising their First Amendment rights at protests.[28]

The Trump administration's actual and attempted policies in the immigration context highlight the dangers of faceprint collection. For example, ICE has run thousands of faceprint searches on state driver's license databases unbeknownst to license holders,[29] and it recently signed a contract with Clearview AI, a company that has amassed the faceprints of billions of individuals without their knowledge or consent.[30] CBP's collection, retention, and sharing of facial recognition data with ICE could facilitate the deportation of countless undocumented people—people who have built families, careers, businesses, and communities in our country over many years, sometimes decades. Using the faceprints it acquires from CBP's collection, ICE could significantly expand its ability to track and apprehend undocumented individuals going about their daily lives—as they drop their kids at school, pay parking tickets, or visit family in the hospital—as well as through mass raids that have inspired deep fear in immigrant communities and torn families apart.

Indeed, DHS's proposed regulations are part of a larger pattern of heightened surveillance and scrutiny of immigrants. In September 2020, DHS proposed dramatically expanding biometric collection in other contexts "to perform any other functions necessary for . . . enforcing immigration and naturalization laws."[31] That rule describes a process of "continuous vetting" of immigrants,[32] which would lead to biometrics collection throughout individuals' years-long immigration processes, in excess of current practice and without justification.

The use of face surveillance for persistent, mass tracking of people is not theoretical. In other countries, face recognition is already being used as part of comprehensive surveillance systems that monitor people's movements, with dramatic negative consequences for human rights. For example, China has 200 million surveillance cameras and is working to develop the

---

[27] Evan Selinger & Albert Fox Cahn, *Did You Protest Recently? Your Face Might Be in a Database*, Guardian (July 17, 2020), https://www.theguardian.com/commentisfree/2020/jul/17/protest-black-lives-matter-database.

[28] Justin Jouvenal & Spencer S. Hsu, *Facial Recognition Used to Identify Lafayette Square Protestor Accused of Assault*, Wash. Post (Nov. 2, 2020), https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html; Kate Cox, *Cops in Miami, NYC Arrest Protestors From Facial Recognition Matches*, ArsTechnica (Aug. 19, 2020), https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches.

[29] Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, Wash. Post (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches.

[30] Kim Lyons, *ICE Just Signed a Contract with Facial Recognition Company Clearview AI*, The Verge (Aug. 14, 2020), https://www.theverge.com/2020/8/14/21368930/clearview-ai-ice-contract-privacy-immigration.

[31] Collection and Use of Biometrics by U.S. Citizenship and Immigration Servs., 85 Fed. Reg. 56338 (Sept. 11, 2020).

[32] *Id.*

capability to identify any citizen within seconds.[33] The Chinese government is amassing facial recognition databases of individuals who have mental illnesses, used drugs, or petitioned the government with grievances. It is also using the technology as a tool to track and oppress ethnic minorities, including the Uighur population. China reportedly keeps a facial recognition database of all Uighurs who leave the province of Xinjiang, and is developing systems that can alert police when a Uighur person moves into a new neighborhood.[34]

In the United States, law enforcement uses of faceprints collected through the proposed regulations would raise serious constitutional concerns, and could render the initial collection of faceprints unreasonable under the Fourth Amendment.[35] These concerns are compounded by the government's failure to comply with constitutional obligations to provide notice to criminal defendants about its reliance on face surveillance.[36] Government use of face recognition also poses a grave threat to First Amendment rights, as it may chill individuals from participating in protests, attending a religious service, or engaging in other constitutionally protected activity.

In addition to chilling avenues for constitutionally protected freedom of speech, CBP's proposed collection of faceprints also poses an inherent security risk, as this sensitive information may be subject to hacking and data breaches.[37] And once information is shared with other government agencies or foreign governments, DHS no longer retains control over how that information is maintained or secured. Breaches of biometric data are particularly harmful since, as noted above, biometrics cannot readily be changed. Once someone's biometric information has been compromised, there may be no redress.

In fact, CBP has already demonstrated its failure to adequately protect faceprints. According to a DHS Inspector General Report, a recent data breach compromised approximately 184,000 traveler images from a CBP face recognition pilot program, and at least 19 of the images

---

[33] Jon Russell, *China's CCTV Surveillance Network Took Just 7 minutes to Identify a Reporter*, Tech Crunch (Dec. 14, 2017), https://techcrunch.com/2017/12/13/china-cctv-bbc-reporter.

[34] 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; Drew Harwell & Eva Dou, *Huawei Tested AI Software That Could Recognize Uighur Minorities and Alert Police, Report Says*, Wash. Post (Dec. 8, 2020), https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says.

[35] As the Supreme Court has recognized in a variety of contexts—including digital searches—a search or seizure that relies on an exception to the warrant requirement is strictly limited by its original justification. *Terry v. Ohio*, 392 U.S. 1, 19 (1968); *Rodriguez v. United States*, 575 U.S. 348, 353-57 (2015); *Riley v. California*, 573 U.S. 373, 400-01 (2014).

[36] *See, e.g.*, Amici Curiae Br. of ACLU, et al., *Lynch v. Florida*, Case No. 1D16-3290 (Fla. Mar. 11, 2019), https://www.aclu.org/lynch-v-state-amici-brief; Georgetown Law Center on Privacy & Technology, *The Perpetual Line-Up* (Oct. 2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf.

[37] *See, e.g.*, Devlin Barrett, et al., U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say, Wall St. J. (June 5, 2015), http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breachsources-say-1433451888.

were posted to the dark web.[38] DHS's current systems are also proving to be insecure, as demonstrated by the hacking campaign against DHS and other agencies that was discovered in December 2020.[39] According to the Government Accountability Office (GAO), CBP has not yet fulfilled all of its cybersecurity requirements, and has not yet conducted necessary "cyber resiliency" testing.[40]

Separately, there are serious concerns about the nature of the public-private partnerships envisioned by the NPRM, and whether airlines and other private entities will comply with CBP's privacy requirements. Since 2017, several airlines have volunteered to use their own camera operators and cameras in partnership with CBP's face-matching program to test a facial recognition-based boarding process for international flights.[41] CBP's widespread deployment of face recognition under the proposed regulations would likewise rely on airlines' cameras and camera operators to capture faceprints at departure. Although the NPRM states that CBP's private partners will be prohibited from retaining, "for their own business purposes," the photos they collect,[42] the line between an airline's purposes and CBP's purposes is unclear. For example, the NPRM notes that airlines may choose to use their facial-recognition camera hardware "for their own purposes," such as "simplifying the baggage drop and claim process or for access into elite traveler lounge areas."[43] But this observation elides the fact that CBP has already permitted airlines to use its face-matching *software* at baggage drops.[44] If identity-verification at baggage drops is an airline objective, not a CBP objective, the line between "government purposes" and "business purposes" has already been blurred.

Moreover, CBP has failed to audit compliance with its rules concerning airlines' retention of faceprints. A recent GAO report found that CBP had "audited only one of its more than 20 airline partners" to assess whether airlines complied with CBP's privacy requirements, and that CBP "did not have a plan to ensure all partners are audited."[45] According to the same

---

[38] DHS, Off. of Inspector Gen., *Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot*, OIG-20-71 (Sept. 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

[39] 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.

[40] GAO Report 38, 84, 86.

[41] 85 Fed. Reg. 74173.

[42] *Id.* at 74178.

[43] *Id.* at 74185.

[44] TSA Biometrics Overview, House Committee on Oversight and Reform Staff (Jul. 23, 2018), *available at* https://www.aclu.org/sites/default/files/field_document/2020-tsfo-00198_00562-00572.pdf#page=9; Emergency Amendment Alternative Procedures, AP 1546-12-07, *available at* https://www.aclu.org/sites/default/files/field_document/2020-tsfo-00198_00650-00662.pdf; TSA-Approved Security Program Amendment, DALA-18-04 (Dec. 1, 2018), *available at* https://www.aclu.org/sites/default/files/field_document/2020-tsfo-00198_00715-00717.pdf ("This amendment allows the aircraft operator to use a bag drop system utilizing the Customs and Border Protection's (CBP) Traveler Verification Service (TVS) for passenger identification via facial recognition.").

[45] GAO Report (i), 46.

report, "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."[46]

In sum, the NPRM fails to account for how CBP's proposed faceprint collection threatens travelers' privacy and enables systematic surveillance by both our government and foreign governments, leading to further surveillance and scrutiny of immigrants and people of color. By deploying this technology at airports, sea ports, and the land border, CBP would take a significant step toward normalizing the government's collection of faceprints—and radically altering the nature of freedom and privacy in this country.

III. The proposed collection and use of faceprints is prone to error and will disproportionately harm people of color and vulnerable populations.

In addition to creating the harms to privacy, expression, and association discussed above, the proposed faceprint collection would also fail to accomplish DHS's central stated goal: ensuring the valid identification of individuals entering and exiting the country. This function can only be accomplished if faceprints accurately and reliably identify individuals. However, as a general matter, facial recognition technologies are not reliably accurate. These systems "vary in their ability to identify people, and no system is 100 percent accurate under all conditions."[47] Scientific studies show that existing technologies for gathering and analyzing faceprints are flawed, error-prone, and far more complicated than fingerprinting. Importantly, the misidentification rates are generally higher for people of color, young people, and the elderly, and many facial recognition algorithms misgender transgender and gender-nonconforming people.

The risks and consequences of faceprint-matching errors in this context are serious. Database matching errors can result in delays or the wrongful detention of people lawfully in the United States. When there is a faceprint-matching error, CBP may not have a traveler's fingerprints on file as an alternative means of identity-verification. For these travelers in particular, faceprint-matching errors could lead to wrongful deportation or even false arrest for criminal charges. Indeed, at least two Black men have already been falsely identified by face recognition in Detroit, leading to their wrongful arrests for crimes they did not commit.[48]

Even if a faceprint-matching error is not dispositive because individuals are offered an opportunity to submit fingerprints or provide additional information, it may prove troublingly influential. Research conducted by NIST and others has shown that people are likely to believe computer-generated results, and that those who are not specially trained in face recognition are

---

[46] GAO Report 48.

[47] Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, Electronic Frontier Foundation 6 (May 2019) https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf.

[48] Elisha Anderson, *Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit*, Detroit Free Press (July 11, 2020), https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002.

poor at identifying people they do not know,[49] even if they perform face identifications as part of their daily work.[50] It is also unclear how an individual can correct an error once it is introduced into the system—not just in terms of the particular incident where the error was identified, but for their "person-centric" record more broadly, where the error may persist.

Given these risks, DHS should not proceed with this rulemaking at least until NIST completes its study of the accuracy of a face-matching algorithm similar to the one used by CBP. In December 2018, NIST entered into an agreement with CBP to specifically assess the accuracy of this algorithm, including the impacts of gender, ethnicity, and age on matching accuracy.[51] According to a GAO report, NIST's work was delayed by the coronavirus pandemic, and the new completion date for its study is unknown.[52] CBP has represented that its internal analysis of data collected through certain face-matching pilot programs "showed a negligible effect in matching accuracy based on demographic variables."[53] However, CBP also acknowledged that this analysis "was limited," because CBP lacked "data on race or ethnicity" of travelers entering and leaving the country.[54]

The NPRM touts the accuracy of CBP's facial matching system, but significant questions remain, particularly with respect to its operation in the field. For example, in 2019, as part of a long-term analysis of CBP's facial recognition technology, GAO auditors 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."[55] Similarly, in September 2018, the DHS Office of Inspector General reported that CBP was unable to biometrically match 15 percent of all passengers in one of its pilot programs.[56] Although an August 2019 test of one of CBP's face surveillance programs concluded that the agency was able to correctly match 98 percent of travelers' photos

[49] 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; P. Jonathon Phillips et al., *Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms*, 115 PNAS 6171 (June 2018), https://www.pnas.org/content/115/24/6171; David White, et al., *Error Rates in Users of Automatic Face Recognition Software*, PLoS One (Oct. 2015), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0139827 (noting participants made over fifty percent errors for adult target faces).

[50] White, *supra* note 49 (finding equivalent performance between untrained examiners and passport officers).

[51] GAO Report 52.

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] *Id.* at 53.

[56] DHS Office of Inspector General, *Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide*, OIG-18-80 (Sept. 2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf.

with photo galleries built from passenger manifests,[57] even a 2 percent error rate could result in additional processing, delays, or worse for enormous numbers of travelers each day.

Facial recognition technologies are particularly unreliable when used for people of color. According to a comprehensive study by NIST, African American and Asian people are up to 100 more times likely to be misidentified by a facial recognition system than white men, depending on the algorithm.[58] As explained by a 2018 MIT study, facial recognition algorithms are trained on datasets "overwhelmingly composed of lighter-skinned subjects," making them far less effective at identifying those with darker skin pigmentation.[59] Studies on products marketed by private companies, including Amazon, Microsoft, and IBM, also found higher rates of inaccuracy on people with darker skin pigmentations—especially women.[60] Additional bias is introduced when facial recognition systems rely on digital camera images because, when taking photos of faces with darker skin pigmentation, the cameras may fail to provide the degree of color contrast that the algorithms need to produce and match faceprints.[61]

Facial recognition algorithms are also less reliable when applied to young people and the elderly, raising serious concerns about CBP's proposed collection of faceprints from children under the age of 14 and adults older than 79. According to the comprehensive NIST study described above, the majority of more than 100 facial recognition algorithms had a higher rate of mistaken matches among children and the elderly.[62] Other studies have likewise found that facial recognition technologies are less accurate in matching children's faceprints.[63]

In addition, many facial recognition algorithms misgender transgender and gender-nonconforming people. In a 2019 study, researchers from the University of Colorado tested several facial recognition products, including from Amazon, Microsoft, and IBM, to assess their

---

[57] GAO Report 51.

[58] *See* Patrick Grother, et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTR 8280 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, Wash. Post (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-manyfacial-recognitionsystems-casts-doubt-their-expanding-use.

[59] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[60] Tom Simonite, *Photo Algorithms ID White Men Fine—Black Women, Not So Much*, Wired (Feb. 6, 2018), https://www.wired.com/story/photo-algorithms-id-white-men-fineblack-women-not-so-much.

[61] Georgetown Law Center, *supra* note 36, at 54.

[62] Grother, et al., *supra* note 58, at 8; *see also* Joseph Goldstein & Ali Watkins, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database*, N.Y. Times (Aug. 1, 2019), https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.

[63] Nisha Srinivas, et al., *Face Recognition Algorithm Bias: Performance Differences on Images of Children and Adults*, United States: N.p. (June 2019), https://www.osti.gov/biblio/1559665.

application of gender labels to images.[64] These products were consistently less accurate in identifying the gender of transgender people as compared to cisgender people.[65]

It is simply not appropriate for the government to use a novel technology that has significant differences in accuracy depending on people's race, ethnicity, age, or gender. These risks of error will have grave consequences. Because misidentification can lead to interrogations, delays, and even denial of entry into the United States, reliance on facial recognition is especially dangerous.

IV. The proposed collection and use of faceprints is not justified by the government's stated goals.

Given the privacy and security interests implicated by the government's use of facial recognition technology, the undersigned commenters believe its use by CBP or other law enforcement agencies is categorically inappropriate. At a minimum, however, any use of the technology must be justified and necessary for a particular government purpose. The proposed regulations fail even this test.

DHS's justification for collecting faceprints—that they can aid DHS in identifying imposters, criminals, suspected terrorists, and visa overstays—is undercut both by the inaccuracies of facial recognition technology, discussed above, and the fact that such purposes can be accomplished by fingerprint collection. DHS has not provided any evidence that its current collection of fingerprints has led to misidentification problems at points of entry into the United States. At exit, DHS says that fingerprint scans are "more time consuming" and that the equipment needed is "more expensive than facial recognition," but it fails to quantify these costs.[66] DHS also contends that fingerprint scanning is "more intrusive than taking a picture," and for that reason, presents "additional privacy concerns."[67] Not so. While a fingerprint scan may involve more direct physical interaction with a device, fingerprint collection (unlike faceprint collection) does not pose the same risk of future persistent and secretive surveillance on a large scale. It is true that fingerprints are a biometric, can be used to invade privacy, and must be collected judiciously and handled with care. However, it is not possible to collect thousands of fingerprints an hour from subjects walking down a public sidewalk without their knowledge—as facial recognition technology can do. Moreover, fingerprinting has more established standards for accuracy than facial recognition technology. In these circumstances, the collection of faceprints is disproportionate and unnecessary.

---

[64] Morgan Klaus Scheuerman, et al., *How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis and Image Labeling Services*, Proceedings of ACM Human-Computer Interaction (Nov. 2019), https://www.morgan-klaus.com/pdfs/pubs/Scheuerman-CSCW2019-HowComputersSeeGender.pdf.

[65] *Id.*; Vanessa Taylor, *Facial recognition misclassifies transgender and non-binary people, study finds*, Mic (Oct. 30, 2019), https://www.mic.com/p/facial-recognition-misclassifies-transgender-non-binary-people-study-finds-19281490.

[66] 85 Fed. Reg. 74191.

[67] *Id.*

Notably, in December 2019, the Director of the Office of Test and Evaluation for DHS reviewed the results of CBP's facial recognition tests for departing flights, and concluded that the program "did not provide clear, measurable benefits to CBP's existing operations at airports," and "did not change or enhance the day-to-day capabilities of CBP officers."[68] As the September 2020 GAO report explains, "CBP officers generally are not present during facial recognition identity verification at airline gates and, while they can be notified of no-matches, operational testing found notifications did not contain actionable information."[69] As CBP eventually acknowledged, the use of face surveillance on departing travelers "does not change or improve CBP officers' abilities to enforce customs and immigration laws or execute other assigned responsibilities at airports."[70] Instead, according to CBP, the system's "primary purpose is to confirm the identity of travelers and fulfill CBP's statutory mandate to create a biometric entry-exit record system."[71] But as discussed in Section I, *supra*, Congress never intended to authorize the collection of faceprints as part of this system. In any event, the demonstrated costs to travelers' privacy, and the risk of normalizing face surveillance, plainly outweigh the unproven benefits of this surveillance to CBP's existing operations at airports.

In addition, the NPRM fails to explain how the expansion of face recognition will meaningfully enhance CBP's ability to detect identity fraud, which is one of the stated objectives. As the NPRM acknowledges, the use of e-Passports with security features makes it "prohibitively expensive in most cases" to alter or fraudulently manufacture passports.[72] It is instead more common for imposters to use a non-altered travel document legitimately issued to another person.[73] But DHS recognizes that even this type of fraud is "mitigated" because airlines and other carriers are themselves required to ensure that the person presenting a travel document is the person to whom it was issued.[74] Although CBP says that its use of facial recognition technology contributed to the identification of seven imposters in the air environment and more than 100 at land border ports,[75] the NPRM does not even attempt to explain whether these individuals would have likely been identified through the collection of fingerprints, questioning by border officers, or other standard means of verification.

The NPRM also fails to accurately assess the time-related costs of CBP's deployment of facial recognition technology. Although one airline concluded that it saved time in boarding its largest aircraft by using CBP's face-surveillance boarding process (in lieu of scanning boarding

[68] GAO Report 55.

[69] *Id.*

[70] *Id.* at 56.

[71] *Id.*

[72] 85 Fed. Reg. 74167.

[73] *Id.*

[74] *Id.*

[75] *Id.*

passes),[76] other findings suggest that the assessment of time-savings is far more complicated—and that CBP's deployment of facial recognition technology may well increase administrative burden and delay.

First, the NPRM fails to account for the costs of delay associated with incorrect matches. Although the NPRM points to a "time in motion study" concluding that the face surveillance process upon departure takes "9 seconds of each traveler's time," the study expressly failed to account for delays resulting from no-match scenarios or erroneous matches.[77] As a result, DHS's entire analysis of the opportunity-cost-per-traveler rests on the erroneous assumption that face recognition will operate with perfect accuracy.

Second, in 2019, an independent analysis concluded that CBP's "air exit" program captured photographs of only 80 percent of in-scope travelers on participating flights, short of the 97 percent requirement that CBP had set. According to the operational testing report, CBP's program did not meet the photo-capture rate for several reasons, including "camera outages, incorrectly configured systems at boarding gates, and airline agents' decisions to exclude certain categories of people out of convenience (to speed up the boarding process), such as families or individuals using wheelchairs."[78] The fact that airline agents *excluded* categories of individuals from CBP face surveillance in order to speed up the boarding process suggests that the time-savings from facial-recognition-based boarding procedures is not nearly as clear as DHS claims. Moreover, the independent testers witnessed camera malfunctions during boarding at all three of the airports they visited.[79]

Finally, the NPRM assumes that U.S. citizens (who are not supposed to be mandatorily subjected to this technology) will be able to voluntarily opt-out of CBP's faceprint collection, and that individuals will choose to opt out at an extraordinarily low rate.[80] But in practice, to date, many U.S. citizens have had extreme difficulty opting out of supposedly voluntary face-recognition pilot programs, calling into question CBP's estimated opt-out rate.[81] Moreover, the GAO has found that CBP's privacy signage, which is supposed to inform the traveling public about how to opt out of facial recognition pilots, was not consistently posted, and the notices were not always current or complete.[82] The correction of these issues, and the installation of proper signage, may also alter the opt-out rate for U.S. citizens.

---

[76] *Id.* at 74181.

[77] *Id.*

[78] GAO Report 53.

[79] *Id.*

[80] 85 Fed. Reg. 74183.

[81] *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.

[82] GAO Report 39, 41-46.

V. The proposed regulations' open-ended authority to collect any other biometrics in the future raises serious privacy and civil liberties concerns.

DHS also proposes to amend 8 C.F.R. §§ 215.8(a) and 235.1(f) to grant it open-ended authority to collect *any other form* of biometrics from foreign nationals entering and exiting the United States.[83] Currently, DHS's regulations provide that any foreign national may be required "to provide fingerprints, photograph(s) or other *specified* biometric identifiers" upon arrival into or departure from the United States.[84] Through the proposed regulations, DHS seeks to strike the reference to "specified" biometric identifiers, in an effort to broaden its authorization to collect *any* biometric identifiers from foreign nationals—potentially even encompassing DNA. DHS states that the reason for the proposed change is "to allow the flexibility for DHS to employ different methods of biometric collection," because "biometric technology continues to advance and there may be other biometric options that may have potential for implementation in the future."[85]

Given the profound privacy and civil liberties concerns associated with biometric collection, particularly collection by DHS,[86] any future form of biometric collection at the border must be specifically authorized by Congress and subject to the notice-and-comment rulemaking process.

* * *

We therefore urge the Department to rescind the proposed regulations. If you have any questions, please contact Ashley Gorski, ACLU Senior Staff Attorney, at agorski@aclu.org.

Sincerely,

American Civil Liberties Union

American Civil Liberties Union of Illinois

American Civil Liberties Union of Massachusetts

American Civil Liberties Union of New York

American Civil Liberties Union of Northern California

---

[83] 85 Fed. Reg. 74179.

[84] 8 C.F.R. §§ 215.8(a) & 235.1(f) (emphasis added).

[85] 85 Fed. Reg. 74179.

[86] Comment of the ACLU, ACLU of Ill., ACLU of Mass., ACLU of San Diego & Imperial Counties, and ACLU of Wash. in Opposition to 85 Fed. Reg. 56338 (Oct. 13, 2020), https://www.aclu.org/aclu-biometric-collection-nprm-comment.

American Civil Liberties Union of San Diego & Imperial Counties

American Civil Liberties Union of Texas

American Civil Liberties Union of Washington

Advocacy for Principled Action in Government

Defending Rights & Dissent

Electronic Frontier Foundation

Fight for the Future

The Freedom to Read Foundation

Immigrant Legal Resource Center

National Immigration Law Center

Open MIC (Open Media & Information Companies Initiative)