AMNESTY INTERNATIONAL

Michael Hardin, Director
Entry/Exit Policy and Planning
Office of Field Operations, U.S. Customs and Border Protection
Department of Homeland Security
20 Massachusetts Ave. NW,
Washington, DC 20529–2240
(202) 325-1053
michael.hardin@cbp.dhs.gov

CBP Docket No. USCBP–2020–0062

December 18, 2020

Via electronic submission to eRulemaking Portal

RE: Amnesty International USA Comments on "Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States"

Amnesty International USA submits the following comment in response to the November 19 notice of proposed rulemaking (NPRM) which would drastically expand facial recognition technology use at ports of entry. Amnesty International opposes the proposed rule and urges that the Department of Homeland Security (DHS) withdraw it.

Amnesty International is the world's largest grassroots human rights organization, comprising a global support base of millions of individual members, supporters, and activists in more than 150 countries and territories. A top priority for the U.S. section of Amnesty International is protecting the rights of asylum-seekers and migrants, and our organization has also advocated against government overreach and unwarranted intrusions upon the right to privacy. Amnesty International has joined leading civil rights and human rights organizations in calling for a ban on the use of facial recognition technology by law enforcement, recognizing that such technology infringes upon human rights and discriminatorily impacts Black and brown people.[1]

The Proposed Rulemaking Fails to Offer a Meaningful Opportunity to Comment

As a preliminary matter, DHS has not allowed the public sufficient opportunity to comment on this rule. The rule dramatically expands who will be subjected to biometrics collection and what type of information the government can collect about them. If implemented, the rule will impact the lives of millions of travelers to the United States, including U.S. citizens and lawful permanent residents.

Typically, the administration should allow a comment period of at least 60 days following publication of the proposed rulemaking to provide the public a meaningful opportunity to

[1] "Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance," June 11, 2020, https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/.

comment.[2] Here, despite the sweep and complexity of this new rule, DHS has afforded the public only 30 days to comment. There is simply no justification for rushing through a rule of this scope and magnitude. Artificially limiting the time period for comment is particularly unfair at this moment, given that members of the public are grappling with the myriad challenges of managing work and life during a global pandemic.

Furthermore, the proposed rule is incomplete: it lacks information essential to affording the public a meaningful opportunity to comment. It fails to provide information about precisely how the vast array of new facial recognition data Customs and Border Protection (CBP) intends to collect will be stored, and with whom it can be shared, even though this is critical to understanding the rule's ramifications. Nor does it justify why existing methods of identity verification, including fingerprinting, are insufficient to meet the rule's stated objectives of identity verification and criminal and national security checks.

Notwithstanding our organization's objections to the limited time and information provided, we submit this comment to share our concerns about the potentially grave consequences of the proposed rule.

Guiding Principles Regarding the Right to Privacy and Deployment of New Technologies

Both domestic and international law limit the government's ability to interfere with individuals' right of privacy, including through intrusive data collection such as facial recognition technology.

Under international law, the collection of data relating to a person's identity, family, or life implicate the right to privacy, and infringements upon that right are permissible only where they are lawful, necessary, and proportionate. The right to privacy is a fundamental human right: it is recognized in article 12 of the Universal Declaration of Human Rights and in article 17 of the International Covenant on Civil and Political Rights (ICCPR), which the United States has ratified.

The U.N. Office of the High Commissioner for Human Rights (OHCHR) has explained that "[e]ven the mere generation and collection of data relating to a person's identity, family, or life already affects the right to privacy, as through those steps an individual loses some control over information that could put his or her privacy at risk."[3] Both immigrants and citizens are entitled to this right: OHCHR has clarified that the right to privacy "applies equally to everyone," and that "[a]ny differences in its protection on the basis of nationality or any other grounds are inconsistent with the right to equality and non-discrimination" contained in the ICCPR.[4]

Any interference with the right to privacy is permissible only if it is neither arbitrary nor unlawful, meaning it satisfies the principles of legality, necessity, and proportionality. OHCHR has clarified that this means that States "may only interfere with the right to privacy to the extent envisaged by the law," and "the relevant legislation must specify in detail the precise circumstances in which such interference may be permitted." To meet the criterion of legality, the relevant

---

[2] *See, e.g.*, Executive Order 12866 (Oct. 4, 1993) (requiring that the public generally be given 60 days to comment on a proposed rule); Executive Order 13563 (Jan. 18, 2011) ("To provide the public an opportunity to participate in the regulatory process, comment period shall be at least 60 days").
[3] Office of the High Commissioner of Human Rights, "Privacy in the Digital Age," https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.docx.
[4] *Id.*

legislation "must specify in detail the precise circumstances in which such interference may be permitted." Even where legislation may permit such interference, it is nevertheless arbitrary and unlawful if it (1) fails to serve a legitimate purpose, (2) is not necessary and proportionate to achieve that purpose, and (3) is not the least intrusive option available.

While the NPRM notes that the creation of an automated biometric entry/exit registry system is required by statute, and this proposed rule is DHS's attempt to comply with that requirement, the statute in question does not specify or require that DHS comply by rolling out facial recognition technology capabilities at all ports of entry. Rather, the statute mandates the "full implementation of an automated biometric entry and exit data system."[5] Yet, as the American Civil Liberties Union (ACLU) has noted, by predicating its biometric entry/exit system on facial recognition, CBP's system "utilizes the most dangerous biometric," one which can be easily expanded or misused for purposes far beyond the rule's stated objectives of identity verification.[6] For this reason, lawmakers have proposed instating a moratorium on the use of facial recognition technology by *all* law enforcement agencies – including CBP's use of the technology at ports of entry.[7] Because the significant intrusion on privacy presented by mass expansion of facial recognition technology is not specifically authorized in the statute CBP cites as its authority for this rulemaking, the proposed rule arguably does not satisfy the principle of legality.

Furthermore, even if the expansion of facial recognition technology at ports of entry was specifically authorized by law, its use is not necessary or proportionate to CBP's stated objectives. For example, the proposed rulemaking does not describe which other biometric technologies were considered and rejected in favor of face recognition, nor does it describe why existing automated biometrics technologies, such as fingerprint scans, are insufficient for the stated objective of identification of travelers.

Even the contemplated process for opting out of facial recognition is not much of a safety valve. While the proposed rule notes that U.S. citizens can opt out or request an alternative inspection process, non-U.S. citizen travelers have no recourse other than to be subjected to facial recognition: the NPRM notes that "[a]lternative procedures would only be available to U.S. citizen travelers."[8] As the ACLU has noted, even systems that are optional at first can soon become mandatory, through pressure by border agents, negative repercussions, and normalization of intrusive technologies – just as happened with body scanners at airport security checks, which were initially optional and soon became mandatory.[9]

Specific Concerns with Use of Facial Recognition Technology at Ports of Entry

Not only is the use of facial recognition technology not justified by the given circumstances, its rollout and widespread use by CBP also poses several serious concerns.

---

[5] 8 U.S.C. 1365(b).
[6] Jay Stanley, "What's Wrong With Airport Face Recognition?," ACLU, August 4, 2017, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/whats-wrong-airport-face-recognition.
[7] "Facial Recognition and Biometric Technology Moratorium Act of 2020," S. 4084 (June 25, 2020), available at https://www.congress.gov/bill/116th-congress/senate-bill/4084/text.
[8] 85 Fed. Reg. at 74177.
[9] Jay Stanley, "U.S. Customs and Border Protection's Airport Face Recognition Program," ACLU, Feb. 2020, https://www.aclu.org/other/aclu-white-paper-cbps-airport-face-recognition-program.

- **Inaccuracy**

In its NPRM, CBP cites the accuracy of facial recognition as a key factor in favor of deploying it at ports of entry nationwide, and notes that the Traveler Verification Service (TVS) system it plans to use currently reports a 97% accuracy rate.[10] However, just like other technologies, face recognition is fallible, and even at 97% accuracy, one out of every 33 people could be subject to misidentification and additional and potentially time-consuming alternative inspections – an error rate that will be especially burdensome when the technology is deployed at scale.

Like all biometric technologies, facial recognition is fallible, and biometric governance and administration systems are prone to hacking and other data protection violations. This is evidenced and compounded by the number of errors in existing databases. Although they are sometimes described as being a "deterministic" tool of identification, research shows that facial recognition is not a definitive method of identification. Facial recognition technology can frequently fail to identify a face based on age or changes in facial characteristics – a particularly salient concern when considering that the proposed rule would also allow for the mass collection of facial image data for children, as described further below.

- **Discriminatory impact on Black and brown travelers**

Furthermore, research suggests that facial recognition technology misidentifies faces in racially discriminatory ways, meaning Black and brown travelers will be adversely impacted by the widespread rollout of facial recognition technology. Amnesty International has noted how facial recognition programs undermine the human right to equality and nondiscrimination by enabling profiling and targeted discrimination, as well as by frequently misidentifying women and people of color.

Research has consistently found that facial recognition systems process some faces more accurately than others, depending on key characteristics including skin color, ethnicity and gender. For example, researchers at the Massachusetts Institute of Technology Media Lab have documented how commercially available facial recognition technology from leading U.S. tech companies repeatedly misgenders women, particularly women with darker skin tones. Similarly, the National Institute of Standards and Technology measured the effects of race, age and sex on leading facial recognition systems used in the United States and found that "the majority of face recognition algorithms exhibit demographic differentials."[11] The agency "found empirical evidence for the existence of demographic differentials in face recognition algorithms that [it] evaluated and measured higher false positives rates in women, Black people, and particularly in Black women.[12]

While the NPRM notes the potentially discriminatory impacts of facial recognition along race and gender lines, it states that "[b]y expanding the scope of individuals subject to facial image

[10] 85 Fed. Reg. at 74174.
[11] US National Institute of Standards and Technology: 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects', Patrick Grother, Mei Ngan and Kayee Hanaoka, NISTIR 8280 (2019): https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf
[12] Testimony from Dr. Charles H. Romine, Director of the National Institute of Standards and Technology, before the House Committee on Oversight and Reform, Jan. 15, 2020, available at https://www.nist.gov/speech-testimony/facial-recognition-technology-part-iii-ensuring-commercial-transparency-accuracy

collection, the accuracy of the facial matching system will improve for all segments of the population, including children and the elderly."[13] However, this would only be true if CBP were sharing its database of facial images with companies that develop recognition algorithms, which raises serious privacy concerns. Furthermore, this fails to address how, in the interim, CBP will address the certain disproportionate impact of face recognition inaccuracy on Black and brown travelers. Rather than unrolling a flawed and racially biased technology to airports around the nation and trusting these serious errors will somehow resolve themselves, CBP should instead address these serious concerns *before* subjecting travelers to the technology.

- **Impact on children**

The proposed rule seeks to expand who would be subject to the collection of facial images for facial recognition: whereas currently biometrics collection is permitted only for children over the age of 14, this new rule would subject all travelers of all ages to such collection. Yet, as experts have noted, children's biometrics are still in development and therefore unreliable, only becoming more stable at age 15.[14] An upcoming guide by UNICEF, "Biometrics and Children," suggests that "while biometric technologies have *some* application in children above 5 years of age, solutions at younger ages are largely experimental and require more research."[15] By proposing to remove all age limitations on restrictions on biometric collection, the rule places children at a heightened risk of being misidentified.

Furthermore, from a child rights, safety and welfare perspective, children's inability to consent to the collection and storage of their facial images is particularly concerning. In comparative contexts, a child's refusal to the processing of biometric data may even override parental consent.[16] For example, the European General Data Protection Regulations provide that children merit special protection with respect to their personal data.[17] No such protections are outlined, let alone acknowledged, in the proposed rule.

Similarly, though the NPRM claims that collecting children's facial images could help combat human trafficking, requiring the mass collection of children's biometrics to assess the veracity of familial relationships is not proportionate - and indeed, could work at cross-purposes[18] - to achieving this goal. Relying on biometrics to prove relationships could lead children to be erroneously separated from guardians or caretakers who are not their biological parents, as advocates have previously explained[19] - a serious breach of the right to family unity. If the administration were serious about child trafficking concerns, it would not have suspended

[13] 85 Fed. Reg. 74175.
[14] "Modeling the Growth of Fingerprints Improves Matching for Adolescents," http://www.stochastik.math.uni-goettingen.de/preprints/ModelingTheGrowthOfFingerprintsImprovesMatching.pdf.
[15] UNICEF, "Biometrics and Children," available at https://data.unicef.org/resources/biometrics/
[16] UK Home Office, "Protection of biometric information of children in schools and colleges," https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692116/Protection_of_Biometric_Information.pdf.
[17] *Id.*
[18] *See, e.g.*, Electronic Frontier Foundation, "Rapid DNA Testing of Migrants at the Border Is Yet Another Iteration of Family Separation," Aug. 2019, https://www.eff.org/deeplinks/2019/08/ices-rapid-dna-testing-migrants-border-yet-another-iteration-family-separation.
[19] "Trump Administration Expands Collecting Biometric Data of Migrants, Raising Concerns," NBC News, https://www.nbcnews.com/news/us-news/trump-admin-expands-collecting-biometric-data-migrants-raising-concerns-advocates-n1000886.

protections wholesale for children under the Trafficking Victims Protection Reauthorization Act (TVPRA), as it has done during the COVID-19 pandemic.[20]

- **Storage, sharing, and (mis)use**

Notably, the rule is almost entirely silent on how the vast new array of face images it plans to collect will be stored, shared, and protected – other than noting that various facial recognition pilot programs retain facial images from anywhere from 12 hours to 75 *years*.[21]

A face recognition system that conducts 1:1 identity verification and does not store or collect information could be permissible as a minimal infringement upon the right to privacy. However, the proposed rule does not clearly address collection or storage of facial image data collected through CBP's new nationwide facial recognition program, meaning that millions of facial images could be stored on a database ripe for potential misuse and expansion beyond its stated purpose of identifying travelers at ports of entry.[22]

The rule does not specify where the new facial image data will be stored, but most DHS data is currently stored in the IDENT database; going forward, data will be stored in DHS's sweeping new Homeland Advanced Recognition Technology (HART) database, the world's second largest biometric system,[23] whose breadth and scope raises serious concerns regarding information-sharing and use.[24] HART makes widespread sharing and storage possible, circumventing traditional points of oversight or limitation. A privacy impact assessment for HART explicitly notes that TVS – the program which will collect travelers' facial images for face recognition – is an "authorized user" for HART, meaning that the data collected through widespread facial recognition at ports of entry can potentially be used, stored, and shared within HART.[25]

While the NPRM states that facial images are to be used for the purpose of identification, as the ACLU has noted, the presence of a database with millions of facial images is easily susceptible to mission creep: "once CBP begins collecting biometrics for every person traveling across the border . . . there is a significant likelihood that that practice will expand not only to new places

---

[20] "Amnesty International USA Opposes New Rule Empowering Unlawful Expulsions of Asylum-Seekers," April 23, 2020, https://www.amnestyusa.org/our-work/government-relations/advocacy/amnesty-international-usa-opposes-new-rule-empowering-unlawful-expulsions-of-asylum-seekers-at-border/.

[21] 85 Fed. Reg. at 74191 (noting that "under CBP's facial recognition based entry-exit program, CBP's biographic data retention policies remain the same. CBP temporarily retains facial images of non-immigrant aliens and lawful permanent residents for no more than 14 days within ATS–UPAX for confirmation of travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits. However, if the TVS matching service determines that a particular traveler is a U.S. citizen, CBP holds the photo in secure CBP systems for no more than 12 hours after identity verification . . . Photos of all travelers are purged from the TVS cloud matching service within a number of hours, depending on the mode of travel. Photos of in-scope travelers are retained in IDENT for up to 75 years.")

[22] ACLU, "ACLU White Paper: CBP's Airport Face Recognition Program," Feb. 2020, https://www.aclu.org/other/aclu-white-paper-cbps-airport-face-recognition-program.

[23] C Burt, "Inside the HART of the DHS Office of Biometric Identity Management", *Biometric Update* (Sep 2018), available: https://www.biometricupdate.com/201809/inside-the-hart-of-the-dhs-office-of-biometric-identity-management

[24] DHS Homeland Advanced Recognition Technology System (HART) Increment 1 Privacy Impact Statement (PIA), 2, DHS/OBIM/PIA-004 (February 24, 2020), available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf.

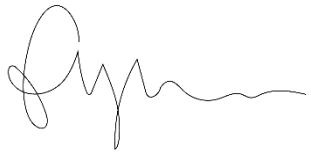
[25] Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART) Increment 1 PIA, DHS/OBIM/PIA-004, Feb. 24, 2020, available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf.

but also for new purposes,"[26] given the "enormous pressure" the agency will face to turn face recognition checkpoints into "broader law enforcement checkpoints where people are subject to watchlist, criminal, and immigration checks."[27] Given TVS's potential interoperability with HART, this vast new collection of facial images could be used for a breathtakingly broad set of purposes beyond identity verification: everything from checks against flawed and racially biased "watchlists" to criminal databases could be fair game. The consequences for Black and brown travelers – who are already likely to be over-policed compared to the rest of the population – could be devastating, given that they are likelier to be falsely identified by facial recognition programs.

Finally, given its history of discrimination and other abuses, allowing CBP access to this trove of new facial image data is particularly concerning. The agency has a long history of racially profiling Black and brown travelers and border residents, including one Black U.S. diplomat stationed in northern Mexico who described facing discrimination and harassment by CBP agents when crossing the border.[28] Amnesty International has extensively documented how lawyers, journalists, and cross-border advocates have been subjected to targeting, surveillance, and retaliation, including being placed on discriminatory and unlawful "watchlists."[29] In recent years, the agency has carried out some of the Trump administration's most grievous human rights abuses, including forcibly separating asylum-seeking families at the border and unlawfully cracking down on racial justice protesters. Empowering an agency with such a troubling track record of human rights violations to implement and roll out a massive, intrusive facial recognition program is precisely the opposite of the increased oversight, accountability, and reform the agency desperately needs.

For these reasons, Amnesty International USA urges CBP to withdraw this proposed rule and calls on the federal government to place a moratorium on the rollout of government facial recognition programs in light of the serious threats they pose to human rights.

Sincerely,



Charanya Krishnaswami
Americas Advocacy Director
Amnesty International USA

---

[26] Jay Stanley, "What's Wrong With Airport Face Recognition?," ACLU, August 4, 2017, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/whats-wrong-airport-face-recognition.
[27] Jay Stanley, "U.S. Customs and Border Protection's Airport Face Recognition Program," ACLU, Feb. 2020, https://www.aclu.org/other/aclu-white-paper-cbps-airport-face-recognition-program.
[28] Katy Murdza, "Institutional Racism is Rampant in Immigration Enforcement at the U.S.-Mexico Border," Immigration Impact, Sept. 2, 2020, https://immigrationimpact.com/2020/09/02/mexico-border-racism/#.X9t6NNhKiUk.
[29] Amnesty International, "Saving Lives is Not a Crime," July 2019, https://www.amnesty.org/en/documents/amr51/0583/2019/en/.