AMNESTY INTERNATIONAL

Michael J. McDermott
Security and Public Safety Division, Office of Policy and Strategy
U.S. Citizenship and Immigration Services
Department of Homeland Security
20 Massachusetts Ave. NW, Washington,
DC 20529–2240
(202) 272–8377

USCIS Docket No. USCIS–2019–0007-0001

October 13, 2020

Via electronic submission to eRulemaking Portal

RE: Amnesty International USA Comments on "Collection and Use of Biometrics by U.S. Citizenship and Immigration Services"

Amnesty International USA submits the following comment in response to the September 11 notice of proposed rulemaking which, if implemented, would authorize mass, unwarranted, indefinite surveillance of immigrants and their loved ones. Amnesty International strongly opposes the proposed rule and urges that the Department of Homeland Security (DHS) withdraw it immediately.

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.

This rule, if implemented, makes several alarming, unnecessary, and discriminatory changes that infringe upon the privacy rights of immigrants, asylum-seekers, and their U.S. citizen loved ones. First, it dramatically expands the universe of people who could be subjected to biometrics collection, making such collection the norm, not the exception. The rule also expands the scope of biometric information to be collected, allowing DHS to collect a vast array of data, including facial image data for facial recognition – a technology Amnesty International has criticized as invasive and racially biased.[1] Third, it allows DHS subagencies to require DNA tests from both immigrants and U.S. citizen relatives as "evidence of a claimed genetic relationship," which raises serious privacy concerns. Finally, it subjects immigrants to an ominous and discriminatory regime of "continuous vetting": at any point during the years-long (often decades-long) process of becoming a U.S. citizen, DHS can demand updated information from applicants, and can periodically require their U.S. citizen or lawful permanent resident sponsors to resubmit information as well.

[1] Amnesty International, "Amnesty International Calls for a Ban on the Use of Facial Recognition Technology," June 2020, https://www.amnestyusa.org/wp-content/uploads/2020/06/061120_Public-Statement-Amnesty-International-Calls-for-Ban-on-the-Use-of-Facial-Recognition-Technology-for-Mass-Surveillance.pdf.

Taken together, the provisions of the proposed rule have the potential to power a discriminatory mass surveillance regime – subjecting immigrants and their loved ones to a "digital panopticon." Amnesty International therefore urges that the rule be rescinded in full.

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. At nearly 90 pages in length, the rule dramatically expands who will be subjected to biometrics collection, how long and how frequently the government could demand their information, and what type of information the government can collect about them. If implemented, the rule will impact the lives of millions of immigrants and their U.S. citizen and lawful permanent resident relatives. It will power the mass collection and storage of all manner of biometric information into a new database described by experts as "the largest database of biometric and biographic data on citizens and foreigners in the United States."[2] The ramifications of the rule will be potentially seismic.

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 comment.[3] 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, which, as DHS itself notes, would power biometric data collection for at least six million people annually and will cost taxpayers hundreds of millions of dollars. 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. Yet not only has DHS imposed an abnormally short deadline without any reasonable justification for doing so, it has also, to date, failed to respond to a request for extension of the deadline signed by over 100 organizations.[4]

Furthermore, the proposed rule is incomplete: it lacks information essential to affording the public a meaningful opportunity to comment. It fails to provide concrete data about the biometric information DHS currently collects and - other than conclusory statements about the reliability of documentary versus biometric information – does not explain why that information is insufficient to meet DHS's stated objectives of identity verification and criminal and national security checks. It also fails to describe how the massive amounts of new data it plans to collect will be stored and shared, even though this is critical to understanding the rule's ramifications.

As described below, the proposed rule mentions in a cursory footnote that DHS's IDENT database will be replaced by the Homeland Advanced Recognition Technology (HART) database and says that "DHS will use the term 'IDENT' in this rule to refer to both the current and

---

[2] Jennifer Lynch, "HART: Homeland Security's Massive New Database Will Include Face Recognition, DNA, and Peoples' 'Non-Obvious Relationships'," https://www.eff.org/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and.

[3] *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").

[4] *See* Letter from Catholic Legal Immigration Network (CLINIC) et al. to DHS, Sept. 17, 2020, https://cliniclegal.org/resources/federal-administrative-advocacy/more-100-organizations-join-urge-dhs-provide-60-day.

successor systems."[5] Yet these two databases are hardly interchangeable: HART is cloud-based and will reportedly include a vast array of capabilities that IDENT does not have, including broadened-out data sharing agreements.[6] By failing to provide even the barest amount of transparency about where the massive amounts of data collected under this rule will be stored, let alone how it will be shared, the rule fails to provide necessary transparency about its potential ramifications. For this reason alone, the rule should be rescinded, as DHS has failed to provide the public a meaningful opportunity to comment on its far-reaching impacts.

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

The Rule Is Based on Harmful, Xenophobic, and Discriminatory Motivations

As an initial matter, Amnesty International is alarmed by this rule's xenophobic motivations. The rule repeatedly cites to President Trump's second Muslim ban, one of a series of measures designed to implement "extreme vetting" – an initiative which disproportionately impacts Black and brown immigrants and their families, making their status and their belonging constantly suspect.[7]

From its earliest days, the Trump administration has pursued a discriminatory vision of extreme vetting, which it has justified through inflammatory and false portrayals of the threat immigrants pose to the United States.[8] Extreme vetting has led to the targeting of Muslim refugees – already the most vetted population of any to enter the United States[9] – as well as reprisals against activists and outspoken critics of the Trump administration, a practice experts have described as "censorship masquerading as immigration enforcement."[10]

Expansive biometrics collection has always been a centerpiece of the administration's extreme vetting regime.[11] Scholars have termed the "increasingly fervent data collection" on migrants and

[5] 85 Fed. Reg. 56388, 56349.
[6] See *infra* page 18-20.
[7] *See, e.g.*, Letter from 57 Organizations to Acting DHS Secretary Elaine C. Duke, Nov. 16, 2017, available at https://www.documentcloud.org/documents/4243212-Coalition-Letter-to-DHS-Opposing-the-Extreme.html (noting that ICE's Extreme Vetting Initiative is "tailor-made for discrimination"); Harsha Panduranga & Faiza Patel, "Extreme Vetting and the Muslim Ban," Brennan Center for Justice, Oct. 2, 2017, https://www.brennancenter.org/our-work/research-reports/extreme-vetting-and-muslim-ban (noting that the "burden" of new vetting procedures "are likely to fall most heavily" on Muslims).
[8] *See, e.g.*, Lauren Said-Woodhouse & Ryan Browne, "Donald Trump wants 'extreme vetting' of immigrants. What is the US doing now?," CNN, Aug. 16, 2016, https://www.cnn.com/2016/08/16/politics/how-us-vets-immigrants-donald-trump-extreme-vetting/index.html.
[9] International Refugee Assistance Project, "Debunking 'Extreme Vetting': Recommendations to Build Back the U.S. Refugee Admissions Program," Oct. 2020, https://refugeerights.org/wp-content/uploads/2020/10/Vetting-Report-2020.pdf/.
[10] Carrie DeCell, "Trump's 'extreme vetting' is muzzling activists and shutting them out," The Guardian, April 20, 2018, https://www.theguardian.com/commentisfree/2018/apr/20/trump-extreme-vetting-activists-censorship-immigration.
[11] Blair Guild, "What Is Extreme Vetting? White House Outlines Proposed Policy," CBS News, Nov. 1, 2017, https://www.cbsnews.com/news/what-is-extreme-vetting/ (describing "[e]nhanced collection and review of biometric and biographical data" as a centerpiece of the new extreme vetting regime).

asylum-seekers "data colonialism," reproducing inequalities and infringing upon the population's rights to privacy and nondiscrimination.[12]

Together, the changes proposed in the rule would create a regime in which immigrants and their U.S. citizen relatives - disproportionately people of color - are continuously surveilled, and the government is entitled to collect all manner of sensitive, identifying information about them, regardless of whether that information is actually necessary to establish identity or eligibility for immigration status. That information would be stored in a massive database whose information is shared across law enforcement agencies and even with foreign governments, meaning that communities already more likely to be policed and scapegoated could now be easily surveilled and even falsely identified in connection with crimes.

The Rule Seriously Infringes Upon Privacy Rights and Empowers Mass and Unprecedented Surveillance of Immigrants and U.S. Citizens

The proposed rule, if implemented, would seriously infringe upon the privacy rights of immigrant communities and their U.S. citizen family members, subjecting them to unlawful and unnecessary surveillance.

The rule makes four key changes to DHS's collection of biometric data:

- First, it dramatically expands the universe of people who could be subjected to biometrics collection, authorizing the collection of biometrics from a broad array of immigrants and U.S. citizens: "*any applicant, petitioner, sponsor, beneficiary, or individual* filing or associated with an immigration benefit or request," and any person placed into removal proceedings, could be required to submit biometrics unless the agency specifically waives the requirement.[13] The rule could even require survivors of domestic violence and trafficking to submit to invasive biometrics collection. The purpose of biometric collection, under the new rule, will include not just verification of identity, familial relationships, and criminal/national security concerns but will broadly encompass "identity management" and "vetting" - in other words, a digital panopticon for immigrants and their family members. (Proposed 8 C.F.R. 103.16; various other provisions.)
- Second, it expands the scope of biometric information to be collected, allowing DHS to collect iris scans, facial images, palm prints, and, in some cases, DNA test results, including partial DNA samples. (Proposed 8 C.F.R. 103.16.)
- Third, it allows DHS subagencies to require DNA tests from both immigrants and U.S. citizen relatives "as evidence of a claimed genetic relationship to determine eligibility for immigration or naturalization benefits or to perform any other functions necessary for administering and enforcing immigration and naturalization laws." (Proposed 8 C.F.R. 103.16(d)(2).)
- Finally, it subjects immigrants to an ominous regime of "continuous vetting": at any point during the years-long process of becoming a U.S. citizen, DHS can demand updated biometric information from them, and can periodically require their U.S. citizen or lawful

[12] Petra Molnar, "New technologies in migration: human rights impacts," Forced Migration Review, June 2019, https://www.fmreview.org/sites/fmr/files/FMRdownloads/en/ethics/molnar.pdf.
[13] Proposed rule 8 C.F.R. sec. 103.16(a); *id.* sec. 236.5.

permanent resident relatives to resubmit information as well. (Proposed 8 C.F.R. 103.16(d)(2).)

- **Guiding Principles**

Both domestic and international law limit the government's ability to interfere with individuals' right of privacy, including through intrusive data collection. Under domestic law, data collection, such as the forced collection of DNA, implicates constitutional rights, including the Fourth Amendment's prohibition against unlawful government intrusions upon privacy rights.

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."[14] 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.[15]

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 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 fails to (1) serve a legitimate purpose, is (2) necessary and proportionate to achieve that purpose, and (3) the least intrusive option available.

As a preliminary matter, the broad and indefinite data collection contemplated by the rule falls outside the scope of legislative authority cited by DHS as the basis for the rule and thus fails to meet the criterion of legality.

While the Immigration and Nationality Act provides authority to "take and consider evidence of or from any person touching the privilege of any alien or person he believes or suspects to be an alien to enter, reenter, transit through, or reside in the United States or concerning any matter which is material and relevant to the enforcement of this chapter," it does not silently authorize the mass collection of a broad array of biometric data for an undefined purpose.[16] Furthermore,

[14] 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.
[15] *Id.*
[16] INA section 235(d)(3), 8 U.S.C. 1225(d)(3).

at the time this statutory provision was written, the types of technologies this rule would implement on a widespread basis – including DNA collection and face recognition technology – were not contemplated, and are significantly more invasive than photograph, signature, and fingerprint collection, particularly when multiple biometric modalities are collected and combined at once.

Finally, specific statutes explicitly prohibit the massive expansion of biometric data proposed by the rule. For example, one statute prohibits Customs and Border Protection (CBP), a DHS subagency, from "facilitat[ing] or expand[ing] the deployment of biometric technologies, or otherwise collect[ing], usi[ing], or retain[ing] biometrics" unless specifically authorized by statute.[17] Therefore, the rule exceeds – and in some respects, even contravenes – legislative authority and on that basis alone, should be rescinded.

Furthermore, even if the biometrics collection contemplated by the rule were authorized by law, it still constitutes an impermissible infringement upon the right to privacy. Analyzing each of the changes proposed by the rule in turn, the invasive biometrics collection contemplated is simply neither necessary nor proportionate to DHS's stated objectives.

- **Default collection of biometrics**

Currently, submission of biometrics is mandatory only in conjunction with certain benefits requests; otherwise, to collect biometrics, DHS must justify the request and notify the individual that biometrics are required. DHS proposes flipping this presumption so that biometrics collection is generally always authorized, including upon apprehension or arrest by DHS, unless the agency waives the requirement.

Per the proposed rule, "[b]iometrics collection upon apprehension or arrest by DHS will accurately identify the individuals encountered, and verify any claimed genetic relationship," which will allow DHS to "make better informed decisions as to the processing, transporting, and managing custody of aliens subject to DHS's law enforcement authorities," and somehow even "increase the safety of DHS detention facilities" by "increasing the reliability of data."[18] DHS also claims that requiring biometrics collection "would eliminate an incentive that currently exists for unscrupulous individuals to jeopardize the health and safety of minors to whom they are unrelated, transporting the minors on a dangerous journey across the United States border, and claiming to be the parents of unrelated minors in order to claim to be a 'family unit' and thus obtain a relatively quick release from DHS custody."[19]

DHS essentially justifies this expansive new data collection by arguing that it will help (1) establish identity and (2) deter fraud. To the first concern, DHS fails to explain why potential collection of a vast number of different biometric identifiers is *necessary* to establish identity when other, less intrusive alternatives exist (such as provision of fingerprints and photographs and eliciting of information through interviews, as is currently required in many cases). While it suggests that providing this array of biometric data will lead to the capture of more "reliable" information, it fails to explain why less invasive data collection doesn't produce sufficiently reliable results. If by "reliable," DHS means that it can glean more information about immigrants

[17] 6 U.S.C. 1118.
[18] 85 Fed. Reg. at 56350.
[19] 85 Fed. Reg. at 56350.

and their family members by collecting a broader array of biometric information, this is exactly what makes collecting that information so troubling: it potentially gives DHS far more information than it needs for the limited purposes of establishing identity, familial relationships, and conducting background checks.

Furthermore, DHS fails to acknowledge that biometrics are 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, and the rule suggests that "using biometrics for identity management in the immigration lifecycle will help ensure that an individual's immigration records pertain only to that individual," research shows that biometrics are not a certain method of identification and can change over time.[20]

Given flaws and uncertainties in existing DHS databases,[21] this method of identification risks negatively impacting immigrants and U.S. citizens subject to the new rule. Matching new biometrics against compromised and flawed data will yield inconclusive results, leading to misidentifications or a lack of verification that will prevent people from accessing services to which they would be otherwise entitled.

As to fraud prevention, DHS repeatedly asserts that biometric collection is necessary to prevent fraud without attempting to quantify how widespread or frequent this phenomenon is. At one point in the proposed rule, it cherry-picks and misleadingly presents statistics from a rapid DNA test pilot program at the border (which itself presents serious ethical and civil liberties concerns)[22], suggesting that a large percentage of family units were fraudulent, when the family units tested had already presented indicia of fraud and when the supposed "fraud" in question could actually be a non-blood-relative guardian or a non-parent caretaker traveling with a child.[23] Notoriously, DHS used allegations that adults were fraudulently posing with children as family units as partial justification to separate families, even though such instances of family fraud are statistically exceedingly rare.[24] Similarly, allegations of fraud in the citizenship application process are not borne out by fact.[25] Now, DHS is using these unsubstantiated allegations to enable it to needlessly collect massive amounts of biometric data that can then be used to track, surveil, and target immigrants and their family members - potentially in perpetuity. DHS has

---

[20] 85 Fed. Reg. at 56340.

[21] In *Gonzales v. Immigration and Customs Enforcement* (ICE), the Court found current government immigration databases to be "largely erroneous" and of "dubious reliability," and held that "the collection of datapoints ICE gathers from the various databases does not provide affirmative indicia of removability to satisfy probable cause determination because the aggregation of information ICE receives from the databases is largely erroneous and fails to capture certain complexities and nuances of immigration law." *See Gerardo Gonzales et al v. Immigration and Customs Enforcement et al,* 126, (C.D. Cal 2019) available at: https://www.immigrantjustice.org/sites/default/files/content-type/press-release/documents/2019-09/gonzalez-v-ice_20190927_decision.pdf.

[22] 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.

[23] Nomaan Merchant, "Border Patrol Expands Fingerprinting of Migrant Children," Associated Press, April 26, 2019, https://apnews.com/article/8aec21ef9cc34638a9e54a19466dc867.

[24] Linda Qiu, "Kirstjen Nielsen Justifies Family Separation by Pointing to Increase in Fraud. But the Data Is Very Limited," New York Times, June 18, 2018, https://www.nytimes.com/2018/06/18/us/politics/nielsen-family-separation-factcheck.html.

[25] Randy Capps & Carlos Echevarria-Estrada, "A Rockier Road to U.S. Citizenship? Findings of a Survey on Changing Naturalization Procedures," Migration Policy Institute, https://www.migrationpolicy.org/research/changing-uscis-naturalization-procedures.

therefore utterly failed to justify why such collection is necessary or proportionate to its stated objectives.

Furthermore, the suggestion that such massive data collection will make DHS detention facilities safer is laughable. On the contrary, the database in which this massive amount of personal information will be stored can be easily accessed by other law enforcement agencies, meaning that immigrants who have any level of interaction with any law enforcement agency in the country could be easily funneled into these historically deadly and overcrowded facilities.[26] Far from making detention facilities safer, this data will supercharge racially biased policing, arrests, and detentions.

- **Removing age restrictions**

The proposed rule would allow collection of biometric data regardless of age when issuing Notices to Appear (NTAs). The proposed rule estimates this would lead to the collection of the data of 63,000 additional children in the NTA issuance process. This is a dramatic expansion of the collection and storage of children's data.[27]

DHS articulates two reasons to collect immigrants' biometrics regardless of age: first, "to ensure that the immigration records created for children can more assuredly be related to their subsequent adult records despite changes to their biographic information," and second, "to help combat human trafficking, specifically human trafficking of children, including the trafficking and exploitation of children forced to accompany adults traveling to the United States with the goal of avoiding detention and exploit immigration laws."[28]

Personal data about children is particularly sensitive and subject to additional protections, especially given children's inability to understand and consent to such data collection. Here, DHS's primary stated objective appears to be that it wants as many data points as possible about children, so that it can link a child's records with later adult records. But DHS's wish to track children across their lifespans is hardly a justification to subject them to biometrics collection. Alarmingly, there is no mention of how child welfare experts and professionals would be involved in this process - let alone whether they were consulted in the formulation of the rule - increasing the risk that children's privacy rights will be violated.

Furthermore, children's biometrics are still in development and therefore unreliable, only becoming more stable only at age 15.[29] An upcoming guide by UNICEF, "Biometrics and Children," suggests that "while biometric technologies have *some* application in children above 5

[26] *See, e.g.*, Amnesty International, "We Are Adrift, About to Sink," April 2020, https://www.amnesty.org/en/documents/amr51/2095/2020/en/ (describing historically deadly conditions in ICE facilities).
[27] In a 2017 memo, then-DHS Secretary John Kelly announced via memorandum a change of policy in which age would no longer be a basis for determining when to collect biometrics. That policy memorandum additionally encouraged DHS to amend existing regulations to allow for expansive collection of biometrics regardless of age. "DHS Biometrics Expansion for Improved Identification and Encounter Management," May 24, 2017, https://www.dhs.gov/sites/default/files/publications/dhs_biometrics_expansion.pdf.
[28] 85 Fed. Reg. at 56352.
[29] "Modeling the Growth of Fingerprints Improves Matching for Adolescents," http://www.stochastik.math.uni-goettingen.de/preprints/ModelingTheGrowthOfFingerprintsImprovesMatching.pdf.

years of age, solutions at younger ages are largely experimental and require more research."[30] UNICEF states that "this technology was largely designed to work with adults and may not perform as well when used with children. Errors in biometric recognition can result in potential exclusion from important services and create additional barriers for marginalized and vulnerable groups." By proposing to remove all age limitations on restrictions on biometric collection, the rule places children at a heightened risk of being locked out of the biometric system or misidentified.

The lack of both a right to refuse in the proposed rule and any special provisions regarding the processing of children's data are particularly concerning from a child safety and child welfare perspective. In comparative contexts, a child's refusal to the processing of biometric data may even override parental consent.[31] The European General Data Protection Regulations provide that children merit special protection with respect to their personal data.[32] No such protections are outlined, let alone acknowledged, in the proposed rule.

Similarly, while concerns about human trafficking and child safety must be addressed, requiring the mass collection of children's biometrics to assess is not proportionate - and indeed, could work at cross-purposes[33] - 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[34] - a serious breach of the right to family unity. Instead, the administration should rely on the expertise of child welfare professionals in making decisions related to the verification of family relationships - a suggestion the administration has repeatedly refused to implement. If the administration were serious about child trafficking concerns, it would not have suspended protections wholesale for children under the Trafficking Victims Protection Reauthorization Act (TVPRA), as it has done during the COVID-19 pandemic.[35]

- **Expanding collection of biometrics of U.S. citizens and lawful permanent residents**

Currently, to comply with statutes requiring that family-based visa petitioners not be convicted of a specific subset of crimes under federal law,[36] DHS runs criminal background checks on U.S. citizen and lawful permanent resident (LPR) family members petitioning on behalf of their

[30] UNICEF, "Biometrics and Children," available at https://data.unicef.org/resources/biometrics/
[31] 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.
[32] *Id.*
[33] 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.
[34] "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.
[35] "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/.
[36] Specifically, the Adam Walsh Child Protection and Safety Act of 2006 prohibits U.S. Citizenship and Immigration Services (USCIS) convicted of a "specified offense against a minor" from petitioning for a family-based or fiancé visa, while the International Marriage Broker Act requires petitioners for fiancé or spousal visas convicted of a specified list of offenses to provide certified copies of the dispositions during the visa approval process.

relatives. Although the number of such individuals is likely exceedingly small, the proposed rule would subject all family-based visa petitioners to expansive biometrics collection, and to demand collection of such biometrics at multiple points in the application process.

The rule claims that "name-based checks do not identify all offenders with visa petitions who have been convicted of qualifying crimes" under the relevant statutes, and such checks "reveal only petitioners who are currently required to register as a sex offender or who have a current order of protection in place," while the relevant statutes apply to all family-based petitioners with qualifying convictions regardless of when the criminality occurred. The rule argues that "[r]equiring biometrics collection for all family-based petitioners will result in production of an official Federal Bureau of Investigation criminal history result which provides greater accuracy and detail relating to the petitioner's criminal history."[37]

This justification ignores that petitioners must self-report, under penalty of perjury, any disqualifying criminal history in the process of petitioning for visas for immigrant relatives.[38] It also fails to provide the number of people annually who are convicted of disqualifying crimes as well as any explanation of why the existing background check measures are not sufficient to capture this population. Rather than limiting biometrics collection for just the small fraction of people who report disqualifying criminal history or whose name-based background checks reveal past convictions, the rule instead treats every family-based visa petitioner as a potential criminal suspect, subjecting them to invasive biometrics collection even where there are no indicia of criminal history.

Even more chillingly, the rule requires *subsequent* collection of biometrics if a petition is reopened - potentially subjecting every U.S. citizen and LPR to multiple rounds of invasive biometric collection just in the process of petitioning for a relative. In short, this rule forces U.S. citizens who wish to reunify with their families to potentially subject themselves to intrusive data collection and ongoing surveillance. In addition to likely having a chilling effect on citizens' and permanent residents' willingness to sponsor relatives, such broad, invasive, unjustified data collection impermissibly infringes upon their privacy rights.

- **Expanding scope of biometric data collected**

The rule articulates a set of "authorized biometric modalities" that DHS may "request, require, or accept from individuals in connection to services provided by DHS and to perform other functions related to administering and enforcing the immigration and naturalization laws."[39] Its general justification in doing so is that "DHS needs to keep up with technological developments that will be used by the FBI and agencies with which we will be sharing and comparing biometrics in this area and adjust collection and retention practices for both convenience and security, and to ensure the maximum level of service for all stakeholders."[40]

While privacy concerns with each of the different new "modalities" are addressed below, an overarching issue is that, through this rule, DHS is giving itself wide latitude to choose from an array of modalities, all of which infringe upon privacy and civil liberties and can be weaponized

[37] 85 Fed. Reg. at 56359.
[38] U.S. Citizenship and Immigration Services, "Chapter 2- Signatures," https://www.uscis.gov/policy-manual/volume-1-part-b-chapter-2 (last accessed Oct. 11, 2020).
[39] 85 Fed. Reg. at 56341.
[40] 85 Fed. Reg. at 56355.

for surveillance and intrusion. As experts have noted, the "privacy risks that accompany biometrics databases are extreme," particularly when databases are "multimodal," or store several different biometric identifiers; unlike an ID number or a pin code, biometrics are unique to each person and cannot generally be changed.[41] Here, DHS paves the way for a regime of mass biometrics collection without explicitly justifying why its current practice of collecting photographs, fingerprints, and signatures has proven insufficient to verify identities and criminal history and national security concerns – thus violating the principle that infringements upon privacy rights be necessary and proportionate.

Below, privacy concerns with each of the new proposed authorized biometric modalities is discussed in turn.

- Iris image

DHS justifies its plans to collect iris images by noting that "[i]ris as a biometric modality is a valuable identifier especially for individuals whose fingerprints are unclassifiable or unattainable through loss of fingers, hand amputation, normal wear in the ridges and patterns over time (i.e., due to age, types of employment, etc.), or deliberate eradication/distortion of fingerprint ridges to avoid identification and detection. . . . Biometric iris recognition is fast, accurate, and offers a form of identification verification that requires no physical contact to collect an iris image."

The privacy implications of a massive database of iris scans are chilling. Iris scanners capture 240 different biometric features, which are unique to every eye.[42] While iris recognition is fast and does not require physical contact, as the Electronic Frontier Foundation has noted, a database of iris scans "raises serious civil liberties and privacy concerns" as it can "track people without their knowledge or consent" and enable long-range identification.[43] In addition, iris scans are not foolproof, and can yield false negative error rates of 2.5-20%.[44]

- Palm prints

DHS justifies its plans to collect palm prints by noting that "capturing and scanning latent palm prints is becoming an area of increasing interest among the law enforcement community," and describing how the "National Palm Print Service is being developed to improve law enforcement's ability to exchange a more complete set of biometric information, make additional identifications, and improve the overall accuracy of identification through criminal history records."[45] DHS explains that "[c]ollecting palm prints would permit DHS to align [its] background checks capability with the total available records at the FBI Criminal Justice Information Services (CJIS), keep current with the changing records of law enforcement, and make sure immigration benefit background checks are as accurate and complete as possible."[46]

Here, DHS all but explicitly states that it is collecting information for law enforcement purposes, using biometrics collection as a dragnet and to better "align" its data collection with FBI

[41] Electronic Frontier Foundation, "Biometrics," https://www.eff.org/issues/biometrics (last accessed Oct. 11, 2020).
[42] Electronic Frontier Foundation, "Iris Recognition," https://www.eff.org/pages/iris-recognition.
[43] *Id.*
[44] *Id.*
[45] 85 Fed. Reg. at 56356.
[46] 85 Fed. Reg. at 56356.

databases. There is not even an attempt at a justification as to why palm prints, on top of the biometrics DHS already collects, are necessary to verify identity, eligibility, or conduct background checks. This data collection is thus neither necessary nor proportionate to any permissible objective.

- Facial image

Under the proposed rule, DHS would use "facial images and facial recognition technology for fraud, public safety or criminal history background checks, and national security screening and vetting," and would include the use of a facial recognition technology system on these images.

While DHS currently collects photographs of applicants to produce immigration documents, this rule would enable it to expand its use of facial images to build out a facial recognition system. The mass use of facial recognition technology is deeply concerning: not only do such systems frequently misidentify Black people and other people of color, they also pave the way for mass, pervasive, continuous surveillance without cause, particularly if information-sharing across multiple databases is enabled.[47]

Facial recognition software is among the most invasive digital surveillance technologies. It enables governments to identify and track individuals in public spaces or single them out based on their physiological or behavioral characteristics, and it poses a clear threat to the rights to privacy, freedom of assembly, speech, religion and non-discrimination.[48]

Here, a database with facial recognition capabilities of primarily brown and Black immigrants and their family members - who are already likely to be over-policed compared to the rest of the population - could easily lead to their false identification through information-sharing with criminal databases, which are accessed by state, local, and federal law enforcement agencies. It could also easily enable them to be continuously monitored and surveilled.

To offer one chilling example of possible misuse of facial recognition technology, this summer, during historic civil rights protests in support of the Black Lives Matter movement, DHS agents were deployed to protests across the country. With access to a far-reaching biometric database of certain immigrant and U.S. citizen profiles with facial recognition capabilities, DHS could easily identify, track, and arrest immigrants and their U.S. citizen family members in the database who participate in protests.

There is simply no justification provided for this far-reaching use of facial recognition technology when identification via less invasive means is possible. Nor has DHS even attempted to justify through this rule why mass facial recognition is necessary when other means of identification are available. While 1:1 identity verification processes that do not store or collect information could be permissible, the proposed rule does not articulate or explain what limitations will be placed to address serious privacy and discrimination concerns raised by facial recognition technology.[49]

---

[47] Amnesty International, "Amnesty International Calls for a Ban on the Use of Facial Recognition Technology," June 2020, https://www.amnestyusa.org/wp-content/uploads/2020/06/061120_Public-Statement-Amnesty-International-Calls-for-Ban-on-the-Use-of-Facial-Recognition-Technology-for-Mass-Surveillance.pdf.
[48] Amnesty International, "EU companies selling surveillance tools to China's human rights abusers," Sept. 21, 2020, https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers/.
[49] 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.

- Voice print

DHS proposes collecting voice prints to improve identity verification for (1) verification when immigration benefits requests are submitted electronically and (2) for integration in the call center process to establish faster verification.[50]

Like other biometric identifiers, the storage and use of voice prints implicate privacy concerns. Speech recognition "pierces the veil of anonymity" by linking a disembodied voice to a particular identity;[51] collecting voice prints and later using those for identification purposes can create many of the same concerns related to intrusion of privacy as facial recognition technology. The possibility of both false positive and false negative identifications is particularly worrisome in the use of voice prints, as is the presence of both race and gender bias, which could adversely impact people who speak non-American accented English and people who are transgender, among others.[52] DHS fails to explain why a less intrusive mechanism - such as entry of an A-number or a code - could not be used for telephonic and electronic verification.

In sum, each of the new authorized biometric modalities contemplated by the proposed rule are seriously intrusive upon privacy rights, and the creation of a multimodal biometrics database raises grave concerns given the amount of additional information generated by connecting different identifiers. Because the proposed rule fails to justify why collection of this vast amount of biometric data is necessary or proportionate to its stated objectives, and because it additionally fails to explain how this information will be used and safeguarded, it must be rescinded.

- **DNA testing to establish family relationships**

Currently, familial relationships are established primarily through provision of documentary evidence; where that evidence is unavailable, individuals may submit blood tests. Under the proposed rule, DHS proposes *requiring* the collection of DNA to establish a claimed genetic relationship. While it claims it will not share or store raw DNA or biological samples "unless required to share by law," DHS "may store or share DNA test results, which include a partial DNA profile, with other law enforcement agencies to the extent permitted by and necessary to enforce and administer the immigration laws."[53] DHS claims DNA testing is necessary to establish family relationships because "DNA is the only biometric that can verify a claimed genetic relationship."[54]

Unlike fingerprints, which can only be used for identification, DNA provides a "massive amount of unique, private information about a person that goes beyond identification of that person."[55] A DNA sample "contains [a person's] entire genetic code - information that has the capacity to reveal the individual's race, biological sex, ethnic background, familial relationships, behavioral

[50] 85 Fed. Reg. at 56356.
[51] Oleksandr Pastukhov and Els Kindt, "Voice Recognition: Risks to Our Privacy," Forbes, Oct. 6, 2016, https://www.forbes.com/sites/realspin/2016/10/06/voice-recognition-every-single-day-every-word-you-say/#732a0fd2786d.
[52] Joan Palmiter Bajorek, "Voice Recognition Still Has Significant Race and Gender Biases," Harvard Business Review, May 2019, https://hbr.org/2019/05/voice-recognition-still-has-significant-race-and-gender-biases.
[53] Proposed 8 C.F.R. 103.16(e).
[54] 85 Fed. Reg. at 56353.
[55] *State v. Medina*, 102 A.3d 661, 682 (Vt. 2014) (citations omitted).

characteristics, health status, genetic diseases, predisposition to certain traits."[56] DNA "contains an extensive amount of sensitive personal information beyond mere identifying information and has the potential to reveal intensely private details about a person's life and future."[57] DHS fails to justify why it should have unfettered discretion to require invasive DNA collection and testing to prove family relationships when less invasive means - such as the provision of documentary evidence like birth certificates - could suffice to prove familial relationships in most instances.

DHS briefly acknowledges the heightened privacy concerns with DNA collection and attempts to address those by stating that it will "not handle or share any raw DNA for any reason beyond the original purpose of submission (e.g., to establish or verify a claimed genetic relationship), unless DHS is required to share by law," and store only "DNA test results, which include a partial DNA profile," including 16-24 genetic markers of the "over two million contained in human DNA."[58] This is less than reassuring: DHS leaves open the possibility that raw DNA could be shared "as required by law" and contemplates sharing test results, which still contain a significant number of genetic markers, "with other agencies when there are national security, public safety, fraud, or other investigative needs."[59] Simply put, both highly sensitive raw DNA and DNA test results could be shared for a potentially broad and indeterminate set of reasons unknown to the public at this time.

Requiring DNA collection is a marked departure from existing policy that is not acknowledged or justified in the proposed rule. Although USCIS and consular posts have long accepted DNA analysis as evidence of biological familial relationship, they have never formally required it. Rather, DNA evidence is one of several forms of secondary evidence to be considered in determining the veracity of a familial claim.[60] A 2008 USCIS policy memorandum incorporated into the USCIS Policy Manual explicitly states that DNA testing is *not required* to establish a claimed relationship. If submitted, however, the agency requires that DNA analysis be conducted by a laboratory certified by the American Association of Blood Banks (AABB).[61] USCIS currently does not accept DNA test results using alternative technologies such as Rapid DNA analysis.

DNA collection raises particular privacy and Fourth Amendment concerns. The proposed rule relies in part the DNA Fingerprint Act of 2005, which authorizes the Attorney General to collect DNA samples from individuals who are arrested, facing charges, or convicted and from "non-United States persons who are detained under the authority of the United States." Until recently, however, that law was not applied to non-citizens who were not detained by ICE, or from whom DNA was not collected in the course of a criminal investigation.[62]

Since 2013, the Supreme Court's decision in *Maryland v. King* has permitted law enforcement to collect DNA samples based on their arrests or convictions for certain criminal offenses. Efforts of

---

[56] *People v. Buza*, 4 Cal. 5th 658, 720 (2018) (Cuellar, J., dissenting) (citations omitted).
[57] Electronic Frontier Foundation, "DNA Collection," https://www.eff.org/cases/dna-collection.
[58] 85 Fed. Reg. at 56353.
[59] 85 Fed. Reg. at 56354.
[60] *Matter of Rehman*, 27 I&N Dec. 124 (BIA 2017).
[61] Memo, Aytes, Assoc. Dir. Domestic Operations, USCIS (Mar. 19, 2008), https://www.uscis.gov/sites/default/files/document/news/genetic_testing.pdf.
[62] *See* Sarah B. Berson, *Debating DNA Collection*, National Institute of Justice Journal 264 (Nov. 2009), https://www.ncjrs.gov/pdffiles1/nij/228383.pdf (discussing the DNA Fingerprint Act of 2005 and state court decisions grappling with the collection of DNA from persons not yet convicted of any crime, prior to *Maryland v. King*).

some states to expand the collection of DNA to persons arrested for lower level offenses have been met with great concern.[63] No subsequent law, however, has permitted authorities to collect DNA samples from U.S. citizens and non-citizens who have not been arrested by law enforcement authorities or detained by ICE.

The agency does not address these serious matters in its proposed rule. It believes that the rule does not create new privacy concerns but merely expands the population affected by privacy concerns.[64] Even if that were so, the agency makes no effort to allay concerns related to privacy and overreach. It does not propose any measures that would lessen the impact of the rule where less invasive measures of identity verification are available and sufficient, such as supervisory review of DNA requests, any threshold of evidence short of DNA collection that would satisfy requirements, a provision requiring informed consent, or any protocol for the evaluation of test results reported by the government. Instead, it extends to DHS broad, unreviewable discretion to determine when DNA collection should be required and analyzed.

Similar expansions of DNA collection in other countries have been recognized as disproportionate and a violation of rights, and courts across Europe, the Middle East,[65] and Africa,[66] have struck down such systems, leading to a waste of public resources in the creation of these systems. In 2018, for example, the European Court of Human Rights reached a unanimous judgment in a case against the UK on DNA collection, holding that "the retention [of DNA, biological samples and fingerprints] constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society."[67] In response to the judgment and debate around the issue of DNA collection, the Protection of Freedoms Act 2012 came into force in England and Wales, which saw the removal of over 1.7 million DNA profiles of innocent people and children and the destruction of close to 8 million DNA samples.[68]

- Concerns regarding rapid DNA

The proposed rule contemplates use of Rapid DNA analysis, approvingly citing a pilot program to collect family units' DNA at the border, an initiative which constitutes an alarming intrusion

---

[63] *See e.g.*, Bill Farrar, *Proposal to Expand Mandatory DNA Collection in Virginia Raises Serious Privacy and Due Process Concerns*, ACLU Free Future Blog (Jan. 8, 2018), https://www.aclu.org/blog/privacy-technology/medical- and-genetic-privacy/proposal-expand-mandatory-dna-collection (noting that a proposal in Virginia would have added "obstruction of justice" and "shoplifting" to the list of misdemeanor offenses that authorized DNA collection).

[64] 85 Fed. Reg. at 56343. ("There could be some unquantified impacts related to privacy concerns for risks associated with the collection and retention of biometric information, as discussed in DHS's Privacy Act compliance documentation. However, this rule would not create new impacts in this regard but would expand the population that could have privacy concerns.")

[65] In 2017, a court in Kuwait found that the collection of DNA samples of citizens and visitors of Kuwait by the government violated constitutional provisions on personal liberty and privacy, *see* Human Rights Watch, *Kuwait court strikes down draconian DNA law*, (Oct. 2017), available at: https://www.hrw.org/news/2017/10/17/kuwait-court-strikes-down-draconian-dna-law.

[66] A High Court in Kenya struck down the collection of DNA in the context of a biometric digital ID system earlier this year, High Court of Kenya at Nairobi, *Nubian Rights Forum & 2 others v Attorney General & 6 others; child Welfare Society & 9 others (interested parties)* [2020] eKLR, (Jan 2020) available at: http://kenyalaw.org/caselaw/cases/view/189189/

[67] *Marper v The United Kingdom*, Eur Ct H. R., (2008), available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]}

[68] National DNA Database Annual Report 2012/13. The Home Office, London available at:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/252885/NDNAD_Annual_Report_2012-13.pdf.

upon the right to privacy and could facilitate erroneous family separations. The continued use of Rapid DNA analysis raises additional privacy, accuracy, and quality control concerns.

The proposed rule would authorize DHS to use Rapid DNA testing, when available, to verify biological parent-child relationships in the course of evaluating eligibility for immigration benefits. It asserts that "Rapid DNA testing technolog[y] [is] a precise and focused investigative tool to identify suspected fraudulent families and vulnerable children who may be potentially exploited."[69]

Experts do not agree, however, that Rapid DNA testing provides results of biological relationships that are accurate enough to support allegations of fraud and the separation of families that would result. In 2017, the Swedish National Forensic Centre reported serious errors with a similar Rapid DNA testing system.[70] In contrast, USCIS policy currently is that DNA analysis may only be submitted as evidence of a familial relationship if it occurred at an AABB-certified laboratory.[71] The proposed rule contemplates the use of Rapid DNA analysis by "non-technical" officers, in marked departure from existing policy.

DHS cites the results of its own pilot program as evidence of the success of Rapid DNA testing technology, but the data it reports in the proposed rule is incomplete and achieved using flawed methods. The agency asserts that Rapid DNA testing technologies are a "precise and focused investigative tool to identify suspected fraudulent families and vulnerable children who may be potentially exploited. Between July 1, 2019, and November 7, 2019, DHS encountered 1,747 self-identified family units with indicators of fraud who were referred for additional screening. Of this number, DHS identified 432 incidents of fraudulent family claims (over 2020 [*sic*] percent)."[72]

First, although DHS claims to have received consent from participants in the pilot program, it is likely that many of them experienced the program in coercive conditions and lacked sufficient understanding in their best language to provide informed consent. The program and others like it were undertaken without public review and were the subject of a letter of inquiry from members of Congress only after they began.[73] DHS's own Privacy Impact Assessment, published shortly before embarking on the 2019 pilot program, notes that declining to participate in the Rapid DNA testing is to be considered a factor in determining whether to allow the family unit to proceed together, a condition of participation that is inherently coercive.[74] It identifies several other privacy concerns, but disposes of most of them as "partially mitigated" by the small sample size. DHS did not update their assessment prior to publishing this notice of proposed rulemaking.

---

[69] 85 Fed. Reg. at 56352

[70] Saira Hussain, *Rapid DNA Testing on Migrants at the Border is Yet Another Iteration of Family Separation*, EFF Deeplinks Blog (Aug. 2, 2019) (quoting report from the Swedish National Forensic Centre)(emphasis in original), https://www.eff.org/deeplinks/2019/08/ices-rapid-dna-testing-migrants-border-yet-another-iteration- family-separation.

[71] Memo, Aytes, Assoc. Dir. Domestic Operations, USCIS (Mar. 19, 2008), https://www.uscis.gov/sites/default/files/document/news/genetic_testing.pdf.

[72] 85 Fed. Reg. at 56352. *See also id.* At 56341 n. 7, where DHS notes that 20% of those tested were found to not match.

[73] Letter to Acting DHS Secretary Chad Wolf from Reps. Rashida Tlaib, Joaquin Castro, and Veronica Escobar dated Jan. 21, 2020, https://tlaib.house.gov/sites/tlaib.house.gov/files/DHS%20DNA%20Collection%20Letter_Signed.pdf.

[74] DHS Privacy Impact Assessment for the Rapid DNA Operational Use, June 2019, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-rapiddna-june2019_3.pdf

Second, based on the "severe errors" and "low success rate" reported in the Swedish study, it is likely that some of the 432 "fraudulent family" claims reported by DHS were the result of failures in testing. DHS's own results fail to show that fraudulent family claims are a large enough problem to justify invasive DNA collection. In fiscal year 2019, CBP encountered 473,682 persons classified as belonging to family units.[75] During the period from July through October 2019, CBP encountered over 83,000 noncitizens that were classified as members of family units.[76] The 1,747 family units that were selected for testing during that period were referred because they showed certain unspecified "indicators of fraud." As the testing group was small and not random, and results based on flawed technology, the tiny number of purportedly fraudulent findings cited by the agency is an insufficient data point from which to conclude that expanded DNA collection using Rapid DNA testing is warranted.

- **Continuous biometrics collection**

Ominously, the rule would allow DHS to demand biometrics of immigrants at any time as part of a regime of "continuous immigration vetting," which experts have described as a "a moment-by-moment monitoring of immigrant activities during the lifecycle of their interactions with the United States" motivated by directives in President Trump's explicitly discriminatory series of Muslim bans.[77] The rule would also allow DHS to demand repeated biometrics collection of U.S. citizens and lawful permanent residents at any time an application for a relative for whom they are petitioning is reopened.

DHS states that it needs a "strong system for the collection and use of biometrics from foreign nationals who enter or wish to enter the United States in order to, as directed by the President, 'identify individuals who seek to enter the United States on a fraudulent basis, who support terrorism, violent extremism, acts of violence toward any group or class of people within the United States, or who present a risk of causing harm subsequent to their entry.'"[78]

As described above, continuous vetting raises serious human rights concerns and paves the way for discriminatory surveillance of predominantly people of color.[79] Demanding that immigrants and U.S. citizens submit to needlessly invasive biometrics collection is, as described above, a serious and unnecessary infringement upon privacy rights. Potentially requiring them to submit to this invasive collection *repeatedly* is entirely unjustifiable - and indeed, DHS does not really even attempt to justify why the rule is necessary, other than citing to Trump's explicitly discriminatory vision of "extreme vetting" for immigrants and their family members. Far from keeping the United States safe, this rule, if implemented, will allow DHS to demand sensitive information of immigrants at any time in the years-long (sometimes decades-long) process of naturalization.

---

[75] U.S. Customs and Border Protection, News Release, Statistics of Southwest Border Migration FY 2019, https://www.cbp.gov/newsroom/stats/sw-border-migration/fy-2019.
[76] *Id.*
[77] Chinmayi Sharma, "The National Vetting Enterprise: Artificial Intelligence and Immigration Enforcement," Lawfare, https://www.lawfareblog.com/national-vetting-enterprise-artificial-intelligence-and-immigration-enforcement.
[78] 85 Fed. Reg. at 56352.
[79] Harsha Panduranga & Faiza Patel, "Extreme Vetting and the Muslim Ban," Brennan Center for Justice, Oct. 2, 2017, https://www.brennancenter.org/our-work/research-reports/extreme-vetting-and-muslim-ban.

The Rule Raises Serious Concerns Related to Storage and Information-Sharing

In addition to raising serious privacy concerns related to biometric data collection, the rule also invites serious questions related to data protection, storage, and information sharing.

The rule does not explicitly state where DHS plans to store the vast amounts of biometric data it will collect. Currently, DHS biometric data is stored in IDENT (Automated Biometric Identification System) under the auspices of the Office of Biometric Identity Management (OBIM). Going forward, this data will be stored in DHS's new Homeland Advanced Recognition Technology (HART) database, which raises serious concerns regarding its information-sharing and use.[80]

HART, the world's second largest biometric system,[81] will be hosted by Amazon Web Services' GovCloud (AWS), and it "stores and processes biometric data."[82] The database will contain "centralized DHS-wide biometric" data, as well as more limited contextualizing biographic and encounter history data. A HART record may include biometric data, biometric-associated biographic data, derogatory information, officer comments, encounter data, and machine-generated identifiers.

This proposed rule allows biometrics to be fed into HART on a large scale without the necessary privacy impact assessments having been conducted - making the lack of any reference to HART in the text of the proposed rule particularly concerning. DHS has only conducted a privacy impact assessment (PIA) for the first increment of HART (which is rolling out in four increments).[83] The Increment 1 PIA indicates that "Increment 2 will provide additional biometric capabilities to HART to meet customer needs"; a PIA has therefore not yet been conducted for functionalities within the overall design of HART that implicate the data that is the subject of this rule. Through this rule, then, a vast array of data will be slipped into a system without a prior privacy impact assessment concerning its processing and use. By the time any kind of assessment or challenge could be brought, it could be too late.

HART will also make it possible to share this information at a large scale, circumventing traditional points of oversight or limitation. For example, Customs and Border Protection's (CBP) Analytic Framework for Intelligence (AFI) collects information from Internet and social media sources, and HART shares personally identifying information with a feeder database for AFI.[84] CBP also operates as a data provider to HART. It has stated that it plans to expand database capabilities to include access to commercially available license plate reader information.[85]

---

[80] 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.

[81] 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

[82] U.S. Department of Homeland Security, Privacy Threshold Analysis (PTA) for Homeland Advanced Recognition Technology (HART) Development Testing Environment (DTE) (Apr 2015), produced as part of EPIC-18-06-18-DHS-FOIA-20190422-Production, available at https://epic.org/foia/dhs/hart/EPIC-2018-06-18-DHS-FOIA-20190422-Production.pdf [hereinafter *DHS HART DTE PTA]* at 6

[83] *See supra* note 78 at 3.

[84] *DHS HART DTE PTA* Replacement Biometric System Increment 1, at 6-8

[85] U.S. Department of Homeland Security Customs and Border Protection, Privacy Impact Assessment Update for the Automated Targeting System, DHS/CBP/PIA-006(e), 77, (Jan. 13, 2017), at

Commercial aggregators collect license plate information from private businesses, local governments, law enforcement agencies, and financial institutions (typically via repossession companies) and then these aggregators "store, index, and sell access to the images and time and location of collection."[86] CBP has itself noted the potentially negative effects of the use of LPR data, which can potentially provide information about constitutionally protected activities such as "travel over time … [or] an individual's private life, such as frequenting a place of worship or participating in protests and meetings."[87] CBP claims its structure mitigates civil liberties and privacy concerns, but still, for example, allows users to query historical license plate reader data up to five years old.[88]

HART also allows for more interoperability and information-sharing between US databases and even foreign databases. For example, the FBI, DHS, and Department of Defense (DOD) have announced that they are introducing new standards that allow their major biometric databases to "communicate natively, 'in their own language.'"[89] The Electronic Biometric Transmission Specification (EBTS) version 4.1 will, or does, allow the Automated Biometric Information System (DOD), Next Generation Identification (FBI), and IDENT/HART (DHS) greater transactional interoperability. EBTS also "enabl[es] information sharing with foreign partners."[90]

Information-sharing both among various government agencies and among governments raises serious privacy concerns. The U.N. Office for the High Commissioner of Human Rights has explained that information-sharing can constitute a serious threat to human rights, given that it frequently circumvents legal constraints on the obtaining of such information – thereby eroding the "essence of the right to privacy."[91] These human rights risks are "heightened by the current lack of transparency, accountability and oversight of intelligence-sharing arrangements."[92]

In practice, the disastrous effects of information-sharing between inaccurate, biased, and unreliable law enforcement databases and immigration databases has been extensively documented.[93] Information stored in unreliable and secretive gang databases has been used to deny asylum claims and separate families.[94] For example, CBP has relied on data via a transnational intelligence-sharing program, involving Mexico, El Salvador, Guatemala, and

---

https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp006-ats-may2020.pdf (hereinafter CBP ATS PIA Update).

[86] *CBP ATS PIA Update* at 77

[87] *CBP ATS PIA Update* at 84.

[88] *CBP ATS PIA Update* at 82.

[89] Chris Burt, *U.S. agencies working on standard for seamless communication between biometric databases*, Biometric Update (Sept. 26, 2018), at https://www.biometricupdate.com/201809/u-s-agencies-working-on-standard-for-seamless-communication-between-biometric-databases.

[90] *Id.*

[91] 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.

[92] *Id.*

[93] In *Gonzalez v. ICE*, for example, the Ninth Circuit has held that, in their enforcement actions, ICE has relied on databases with large gaps in necessary data that have significant error rates in the data they contain. *See* "Explaining the Gonzalez v. ICE Injunctions," Immigrant Legal Resource Center, October 2019, https://www.ilrc.org/sites/default/files/resources/2019.11_ilrc_gonzalez_v_ice-11.07.pdf. See also Joan Friedland et al., Untangling The Immigration Enforcement Web, National Immigration Law Center, (September 2017), https://www.nilc.org/wp-content/uploads/2017/09/Untangling-Immigration-Enforcement-Web-2017-09.pdf .

[94] Melissa del Bosque, *Immigration Officials Use Secretive Gang Databases to Deny Migrant Asylum Claims*, ProPublica, July 8, 2019, https://www.propublica.org/article/immigration-officials-use-secretive-gang-databases-to-deny-migrant-asylum-claims

Honduras to make determinations to tear families apart.[95] With the vast expansion of information collection contemplated by this rule, these problems could exponentially increase.

Not only is there no way to ensure that information fed into the databases "communicating" with HART is accurate, the implications of biometrics being stored in HART, and that data shared with foreign governments, is particularly alarming for immigrants who have a fear of persecution in their home countries or who were subject to trafficking. The rule contains no information on how information-sharing will be limited to protect against data falling in the wrong hands.

The Rule Adversely Impacts Survivors of Violence and Trafficking

Finally, the rule would require self-petitioners under the Violence Against Women Act (VAWA) and applicants for trafficking visas, regardless of age, to submit to invasive biometrics collection to establish "good moral character." Most cruelly, the rule would remove the presumption of good moral character for T visa applicants under the age of 14. DHS fails to justify why existing methods to establish good moral character, including police certifications, are insufficient.

As the Tahirih Justice Center has noted, given the potential for information-sharing between state/federal law enforcement and immigration agencies, as well as the frequency with which abusers may falsely report survivors for crimes or otherwise entangle them in the criminal enforcement apparatus, biometrics collection may reveal criminal charges survivors incurred in conjunction with past abuse, leading to wrongful denials of their applications.[96] Similarly, trafficking survivors frequently also incur criminal records in conjunction with coerced activity.[97]

Furthermore, survivors of violence and trafficking may be particularly subject to harm if their data falls into the wrong hands. This risk is exacerbated by data-sharing agreements, including foreign data-sharing agreements, governing the HART database in which the data will be stored. Unlike a name or an ID, people's biometric information is immutable and unique to them, and they may be rightly terrified of the ramifications of sharing multiple biometric identifiers with the government in the context of applying for protection. Requiring invasive data collection for survivors will likely create a chilling effect, preventing them from coming forward and applying for protections they desperately need. Furthermore, as discussed above, subjecting children under 14 to an invasive biometrics requirement raises serious concerns regarding their privacy and confidentiality rights, as well as their ability and capacity to consent.

For all these reasons, Amnesty International USA urges DHS to immediately rescind this rule and demands that the administration cease its discriminatory efforts to create a mass surveillance regime for immigrants and communities of color.

---

[95] *See* Jesse Franzblau, "Family Separation Policy Continues, New Documents Show," National Immigrant Justice Center, June 22, 2019, https://immigrantjustice.org/staff/blog/family-separation-policy-continues-new-documents-show. DHS officials have separated families on the basis of unsubstantiated information shared from foreign governments. *See* U.S. House Judiciary Committee Hearing Oversight of Family Separation and U.S. Customs and Border Protection Short-Term Custody under the Trump Administration, Statement of the National Immigrant Justice Center (NIJC), July 25, 2019, https://www.congress.gov/116/meeting/house/109852/documents/HHRG-116-JU00-20190725-SD014.pdf.

[96] Tahirih Justice Center, "Tahirih Statement on Sweeping Proposal to Expand Biometrics Collection," Sept. 10, 2020, https://www.tahirih.org/news/tahirih-statement-on-sweeping-proposal-to-expand-biometrics-collection/.

[97] Polaris Project, "The Importance of Criminal Record Relief for Human Trafficking Survivors," March 20, 2019, https://polarisproject.org/blog/2019/03/the-importance-of-criminal-record-relief-for-human-trafficking-survivors/.

Sincerely,

Charanya Krishnaswami
Americas Advocacy Director
Amnesty International USA