CLASP
Policy solutions that work for low-income people

October 13, 2020

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

Electronically Submitted via ww.regulations.gov

USCIS Docket No. USCIS–2019–0007-0001

RE: 85 FR 56338; EOIR Docket No. 19-0007, CIS No. 2644-19; RIN 1615-AC14; Comments in Opposition to Proposed Rulemaking: Collection and Use of Biometrics by U.S. Citizenship and Immigration Services

The Center for Law and Social Policy (CLASP) respectfully submits this comment urging the Department of Homeland Security (DHS) to withdraw these proposed rules in their entirety.

Established in 1969, CLASP is a national, non-partisan, non-profit, anti-poverty organization that advances policy solutions for people with low incomes. Our comments draw upon the work of CLASP experts in the areas of immigration, child development, and anti-poverty policies. As a national anti-poverty organization, we bring a deep commitment to children, youth, and families living with low incomes and knowledge of the challenges that they experience as a result.

This proposed rule would establish a gross infringement of privacy for both immigrants and their U.S. citizen family members, including children. The collection of additional biometric data will not make our immigration system more secure or efficient, but it will lead to further discrimination towards immigrants. CLASP opposes these regulations in their entirety and calls upon DHS to withdraw them.

DHS Has Not Afforded the Public a Meaningful Opportunity to Comment

As a preliminary matter, DHS has not allowed the public sufficient opportunity to comment on this rule. The rule, nearly 90 pages in length, 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 have a seismic impact on 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."

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. 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 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.

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 - doesn't 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 successor systems." Yet these two databases are hardly interchangeable: HART is cloud-based and will reportedly include a vast array of capabilities that IDENT doesn't have, including broadened-out data sharing agreements, without all the new aspects of HART having undergone a full privacy impact assessment (for more on HART, see "Storage, Information-Sharing, and Use" below). 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.

DHS Failed to Engage in Proper Consultations on the Rule

Given the practical consequences of the proposed change for government at all levels, as well as individuals and their families, the proposed rule should have undergone a risk assessment and consultation process commensurate to the complexities associated with its implementation, including a federalism assessment.

Critically, the rule justification states that the regulation "will not have substantial effect on the States, on the relationship between the national Government and the States, or on the distribution of power and responsibilities among the various levels of government" and therefore does not warrant a federalism assessment. Yet, the HART database in which the information will be stored allows international, federal, state and local data sharing. The use of data at the state level is governed by state law and some functions, such as familial searching, are conducted and regulated only at the state level. Thus, legislation around the protection and sharing of data at the state level is highly relevant to this rule.

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.[1] 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 (oftentimes decades-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 permanent resident relatives to resubmit information as well. (Proposed 8 C.F.R. 103.16(d)(2)).

The proposed rule impinges upon protected civil liberties by encouraging sweeping, unnecessary data collection and potentially empowering mass surveillance.

Guiding principles: Under international law, the collection of data relating to a person's identity, family, or life implicates the right to privacy. Infringements on that right are permissible only where they are lawful, necessary, and proportionate.

- From the UN High Commissioner for Human Rights' report on the right of privacy in the digital age:
    - The right to privacy is a fundamental human right, recognized in article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights and in many other international and regional human rights instruments. In the digital environment, informational privacy, covering information that exists or can be derived about a person and her or his life and the decisions based on that information, is of particular importance.
    - Even 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.
    - The right to privacy applies equally to everyone. Any 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 article 26 of the International Covenant on Civil and Political Rights, which the United States has ratified.
    - Any interference with the right to privacy is only permissible if it is neither arbitrary nor unlawful. Human rights mechanisms have consistently interpreted those words as pointing to the overarching principles of **legality, necessity and proportionality**. In keeping with those principles, 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. Interference is unlawful and arbitrary not only when it is not provided for by law but also when a law or the particular interference is in conflict with the provisions, aims and objectives of the Covenant. A limitation can only be lawful and non-arbitrary if it serves a **legitimate**

[1] Proposed rule 8 C.F.R. sec. 103.16(a); *id.* sec. 236.5.

purpose. The limitation must be **necessary** for reaching that legitimate aim and in **proportion** to that aim and must be the **least intrusive option available**.

- Under domestic law, data collection, such as the forced collection of DNA, implicates constitutional concerns, including concerns under the Fourth Amendment (discussed below in the DNA collection section), which guard against unlawful government intrusions upon privacy rights.

Here, analyzing each of the changes to biometrics information collection in turn, it's clear that the invasive biometrics collection contemplated is simply neither necessary nor proportionate to DHS's stated objectives, and thus the proposed rule constitutes an impermissible infringement upon privacy rights.

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.

- Objective of rule: 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."[2] 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."[3]
- Analysis: DHS 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 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, 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.
        - Biometrics 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

[2] 85 Fed. Reg. at 56350.
[3] 85 Fed. Reg. at 56350.

individual."[4] Yet, research shows that biometrics are not a certain method of identification and can change over time. Changes to fingerprint and palm biometrics will be particularly problematic for certain groups, such as manual laborers, but other biometric modalities, such as facial images and voice prints, are also affected by age.[5]

- The rule proposes running newly collected biometric information against existing databases. Given flaws and uncertainties in existing DHS databases,[6] this method of identification risks negatively impacting anyone subject to the new biometric 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 they would be entitled to.
- The risk posed by matching biometrics with flawed existing data is exacerbated when the system is considered to be an exact form of identification and therefore provides little room for challenging results. The proposed rule states that USCIS "has internal procedural safeguards to ensure technology used to collect, assess, and store the different modalities is accurate, reliable and valid."[7] Yet it fails to expand upon this, and problems in existing DHS databases indicate that they are not sufficient to protect against misidentification or data protection violations.
- Further, there are no concrete provisions on the process around the opportunity to rebut information collected, stored and processed through this rule.[8] With the data collected being stored in the HART database going forward, looking to the rules on correction of information in that context is even more concerning.

- 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, overcrowded facilities. Far from making detention facilities safer, this data will supercharge racially biased policing, arrests, and detentions.
- 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), 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. 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

[4] 85 Fed. Reg. at 56340.
[5] For studies on the changing nature of fingerprint biometrics *see e.g.* J Galbally, R Haraksim & L Beslay, "A Study of Age and Ageing in Fingerprint Biometrics", *IEE Transactions on Information Forensics and Security* (Oct 2018), available at: https://www.researchgate.net/publication/328526153_A_Study_of_Age_and_Ageing_in_Fingerprint_Biometrics; for a study on the implications of facial aging on biometrics showing that negative effects may be reduced but not eliminated *see* A Lantitis, "a survey of the effects of aging on biometric identity verification" *International Journal of Biometrics* 2(1) (Jan 2020), available at: https://www.researchgate.net/publication/247836107_A_survey_of_the_effects_of_aging_on_biometric_identity_verification.
[6] 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.
[7] 85 Fed. Reg. at 56355.
[8] 85 Fed. Reg. at 56355.

exceedingly rare. Similarly, allegations of fraud in the citizenship application process are not borne out by fact. 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.

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.[9]

- Objective of rule: DHS articulates two reasons to collect biometrics at any 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."[10]
- Analysis:
    - 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 policy that children's privacy rights will be violated.
        - Children's biometrics are still in development and therefore unreliable, only becoming more stable only at age 15. An upcoming guide by UNICEF on "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." 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 a right to refuse in the proposed rule and the fact that there are no 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. The European General Data Protection Regulations (GDPR) provide that children merit special protection with respect to their personal data. No such protections are outlined, or even recognized, in the proposed rule.

[9] 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.
[10] 85 Fed. Reg. at 56352.

- 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 - 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 - 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.

Collecting biometrics of LPRs/USCs: Currently, to comply with statutes requiring that family-based visa petitioners not be convicted of certain crimes under federal law, DHS runs name-based criminal background checks on U.S. citizen and lawful permanent resident (LPR) family members petitioning for immigrant relatives. The proposed rule would allow DHS to collect a potentially broad swath of biometrics to assess criminal history of U.S. citizen and LPR petitioners, and to demand collection of such biometrics at multiple points in the application process.

- Objective of rule: 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 current reliance on name-based checks means that certain family-based visa petitioners are not currently identified and vetted. . . . Requiring biometrics collection for all family-based petitioners will result in production of an official FBI criminal history result which provides greater accuracy and detail relating to the petitioner's criminal history."[11]
- Analysis: The rule allows disproportionately broad data collection. It ignores that petitioners must self-report, under penalty of perjury, any disqualifying criminal history in the process of petitioning for visas for immigrant relatives. Rather than limiting biometrics collection for just those individuals 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, it 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. This rule will undoubtedly have a chilling effect on citizens' and permanent residents' willingness to sponsor relatives.

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."[12] 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

[11] 85 Fed. Reg. at 56359.
[12] 85 Fed. Reg. at 56341.

retention practices for both convenience and security, and to ensure the maximum level of service for all stakeholders."[13]

- 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 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. 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.
- 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."
    - Analysis: Iris scanners capture 240 different biometric features, which are unique to every eye. While iris recognition is fast and does not require physical contact, the implications of a database with tens of millions of iris scans is chilling; 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. In addition, iris scans are not foolproof, and can yield false negative error rates of 2.5-20%.
- 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. 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. Collecting palm prints would permit DHS to align our 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."[14]
    - Analysis: 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 databases. There is no explicit justification as to why palm prints, on top of the biometrics DHS already collects, are necessary to verify identity, eligibility, or conduct background checks.
- Facial image: While DHS currently collects and stores photographs for document production, under the proposed rule, it would use "facial images and 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.
    - Analysis: 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

[13] 85 Fed. Reg. at 56355.
[14] 85 Fed. Reg. at 56356.

across multiple databases is enabled. 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. One nightmare scenario involves DHS agents' recent deployments to Black Lives Matter protests - 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 photograph or fingerprint is available.

- 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.[15]
    - Analysis: 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; 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. 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.

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." Proposed 8 C.F.R. 103.16(e).

- Objective: DHS claims DNA testing is necessary to establish family relationships because "DNA is the only biometric that can verify a claimed genetic relationship. . . . DNA testing provides the most reliable scientific test available to resolve a genetic relationship and replaced older serological testing."[16]
- Analysis:
    - 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."[17] 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 characteristics, health status, genetic diseases, predisposition to certain traits."[18] DNA "contains an extensive amount of sensitive personal information beyond mere identifying information and has

[15] 85 Fed. Reg. at 56356.
[16] 85 Fed. Reg. at 56353.
[17] *State v. Medina*, 102 A.3d 661, 682 (Vt. 2014) (citations omitted).
[18] *People v. Buza*, 4 Cal. 5th 658, 720 (2018) (Cuellar, J., dissenting) (citations omitted).

the potential to reveal intensely private details about a person's life and future."[19] 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."[20] 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."[21] 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.[22]
  - 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).[23] The 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 for its legitimacy on the DNA Fingerprint Act of 2005, title X of Public Law 109-162, 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, 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.[24]
  - 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 some states to expand the collection of DNA to persons arrested for lower level offenses have been met with great concern.[25] No subsequent law,

[19] Electronic Frontier Foundation, *DNA Collection*, https://www.eff.org/cases/dna-collection#:~:text=EFF%20has%20long%20been%20concerned,and%20sharing%20of%20genetic%20data.&text=DNA%20analysis%20is%20also%20not,or%20she%20didn't%20commit.
[20] 85 Fed. Reg. at 56353.
[21] 85 Fed. Reg. at 56354.
[22] *Matter of Rehman*, 27 I&N Dec. 124 (BIA 2017).
[23] Memo, Aytes, Assoc. Dir. Domestic Operations, USCIS (Mar. 19, 2008), https://www.uscis.gov/sites/default/files/document/news/genetic_testing.pdf.
[24] *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*).
[25] *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

however, permits 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. The agency believes that the rule does not create new privacy concerns but merely expands the population affected by privacy concerns.[26] 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. By extending to DHS broad, unreviewable discretion to determine when DNA collection should be required and analyzed, the proposed rule fails utterly to respond to these important and relevant policy concerns.
- 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,[27] and Africa,[28] 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."[29] 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.[30]

- 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."[31] 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,

(noting that a proposal in Virginia would have added "obstruction of justice" and "shoplifting" to the list of misdemeanor offenses that authorized DNA collection.)

[26] 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.")

[27] 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.

[28] 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/

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

[30] 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.

[31] 85 Fed. Reg. at 56352

including "the **retrieval of an incorrect DNA profile**, PCR product or **sample leakage** and the **low success rate**."[32]

- 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.[33] 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 NPRM is incomplete and achieved using flawed methods. The agency asserts that:
    - "Beginning in July 2019 DHS has been conducting a small-scale pilot program where, with consent from individuals presenting themselves as family units, officers use Rapid DNA testing technologies as 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 1747 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)."[34]
- 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.[35] 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 explicitly coercive.[36] 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.
- 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.[37] During the period from July through October 2019, CBP encountered over 83,000 noncitizens that were classified as members of family units.[38] The 1,747 family units that were selected for testing during that period were referred because they showed certain unspecified

[32] 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.
[33] Memo, Aytes, Assoc. Dir. Domestic Operations, USCIS (Mar. 19, 2008), https://www.uscis.gov/sites/default/files/document/news/genetic_testing.pdf.
[34] 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.
[35] 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.
[36] 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
[37] 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.
[38] *Id.*

"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.

- Finally, the proposed rule fails to recognize the distinction between Rapid DNA technology and the AABB-certified testing model, noted above. Rather, it states that "[a]fter DNA samples are collected, an individual's raw DNA material would then be either tested locally by an automated machine (*i.e.*, Rapid DNA) *or* mailed to a traditional AABB- accredited laboratory for testing."[39] Moreover, as it proposes that Rapid DNA testing may be performed by "non-technical users," the potential negative outcomes of the proposed rule, including increased family separation and criminal prosecution, are clear and unconscionable.[40] Given the serious misgivings revealed in even a cursory review of relevant materials and the lack of transparency by DHS regarding the metrics used to evaluate the pilot program, the failure of DHS to account for the concerns raised by the use of Rapid DNA testing technology is arbitrary and capricious.

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 the Trump administration's explicitly discriminatory series of Muslim bans. 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.

- Objective: 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.'"[41]
- Analysis: Continuous vetting raises serious human rights concerns and paves the way for discriminatory surveillance of predominantly people of color. 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 doesn't really even attempt to justify why the rule is necessary, other than citing to the Trump administration'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.

The Rule Is Rooted in - and Will Fuel - Discrimination

- The impetus for portions of this rule is the Trump administration's series of Muslim bans, which were explicitly based on discriminatory intent. The portion of the proposed rule permitting continuous data collection cites the second Muslim ban as justification and is a realization of the "extreme vetting" the Trump administration has long sought, which disproportionately impacts Black and brown immigrants and

[39] 85 Fed. Reg. at 56353.
[40] *Id.* n. 37 ("The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has been working in conjunction with DoD and DOJ to fund the development of cost-effective Rapid DNA equipment to allow non-technical users with appropriate training to analyze the DNA of individuals in a field setting and receive reliable results in about one hour.")
[41] 85 Fed. Reg. at 56352.

their families, making their status and their belonging constantly suspect. Scholars have termed this impulse to engage in "increasingly fervent data collection" about migrants and asylum-seekers "data colonialism."

- 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.
- Furthermore, the technologies contemplated for use in the rule - including widespread use of facial recognition technology - replicate and supercharge existing biases in criminal justice and immigration enforcement systems.

Conclusion

These proposed rules represent radical changes to the privacy of immigrants and their U.S. citizen family members and merit a full 60-day comment period for the public to adequately prepare comments. Taken together, these proposed rules would change what personal and private information immigrants and their family members, including children, would be required to provide the U.S. government, and how often. These methods of surveillance and data collection, such as facial recognition, are rooted with algorithmic bias which disproportionately harms people of color. In fact, the rule in its entirety is based in discriminatory intent and will only exacerbate the surveillance of immigrants and their families.

As an anti-poverty organization committed to the dignity of all those who call or seek to call the United States home CLASP calls upon the administration to withdraw these proposed rules in their entirety.

Thank you for the opportunity to submit these comments. Should you have any questions, please contact Hannah Matthews, Executive Director for Policy, at hmatthews@clasp.org.