12 October 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

Re: Docket No. USCIS-2019-0007, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services; Friday, September 11, 2020, pp.56338 – 56422

Dear Mr. McDermott:

We are writing to address the Notice of Proposed Rulemaking (NPRM) on Collection and Use of Biometrics by U.S. Citizenship and Immigration Services (USCIS). We write on our own behalf, drawing on the credentials and expertise of our group. **Dan Berger** is Partner at the immigration law firm Curran, Berger & Kludt LLC in Massachusetts and an expert on immigration law; **Margaret Hu** is Professor of Law and International Affairs at Penn State Law and School of International Affairs at The Pennsylvania State University, and an expert in immigration policy, national security, cybersurveillance, and civil rights; **Sara Katsanis** is Research Assistant Professor of Pediatrics at Northwestern University Feinberg School of Medicine and an expert in forensic DNA, clinical genetic testing, genetic testing oversight, and genetics policy; and **Jennifer K. Wagner** is Assistant Professor in the Center for Translational Bioethics and Health Care Policy at Geisinger, a licensed attorney, a member of the Pennsylvania Bar Association's Cybersecurity and Data Privacy Committee, and an expert in genetics, bioethics, and anthropology.

HIGHLIGHTS

General considerations

- The proposal expands the definition of biometrics to authorize the collection of personal data for the purposes of vetting and tracking individuals throughout the "immigration lifecycle." The proposed changes are both complex and sweeping and, therefore, should be the subject of Congressional action and rigorous, sustained oversight.
- DHS provided an insufficient comment period of 30 days for complicated topics that involve science, law, and ethics, especially during a pandemic and a presidential election cycle. We join others in calling for an extended comment period.[1]
- The proposed rules outline two separate processes: (1) the expanded definition and uses of biometrics and (2) the systematic implementation of DNA testing for verification of family relationships. These processes are complex and final rules should separately address each since the legal authority and the parameters for testing and oversight of testing are different from that of the collection and storage of information.
- DHS has not adequately identified the problem for which broad expansion of and emphasis on biometrics and reduced reliance on documents and other biographical information is the appropriate

[1] Letter signed by 106 organizations. *Re: Request for 60-day comment period for DHS proposed rule on the expansion of biometrics/ USCIS Docket No.: USCIS-2019-0007*. September 16, 2020. Available at https://www.americanimmigrationcouncil.org/sites/default/files/general_litigation/letter_requesting_60-day_comment_period_on_proposed_rule_expanding_collection_of_biometrics.pdf

solution. Such an explanation is necessary to justify a request for increased appropriations, which would be necessary to fully and evenly implement their proposed rules.
- The technologies specifically proposed (e.g., facial recognition technology) have already been scientifically shown to be discriminatory (e.g., against women and people of color). The proposed rules are highly likely to have disparate and discriminatory effects on certain populations and groups of people.
- The proposal includes a dramatic expansion of the collection and storage of data on children. There is a long history of data from children being recognized as more sensitive than that of adults (e.g., medical and educational contexts). Additionally, removing the presumption of innocence for children is contrary to the growing trend to protect trafficked persons from punishment for acts taken at the demand of their oppressors (traffickers). Such action would subject children to unnecessary and unjustified criminal and terroristic screening. Any proposed change must be pursuant to Congressional action and subject to independent oversight informed by professionals with relevant expertise.

Considerations for DNA testing for family verification
- Increased reliance on DNA for verification of family units, especially with a focus on parent-child relationships, will lead to increased separations of children from accompanying caregivers.
- The proposed rules aim to use DNA testing for detection of child trafficking. Final rules must address two realities: (1) presence of a biological relationship does not eliminate the possibility of a parent trafficking their child and (2) absence of a parentage relationship does not constitute evidence of trafficking.
- The proposed rules outline plans to retain relationship test results as "partial DNA profiles." Instead, any genetic data should be destroyed and only the resulting test outcome (i.e., indication of confirmation of relationship) retained for immigration records only if DHS demonstrates the DNA testing and data retention is consistent with statutory authority.
- The proposed rules specify reliance on relationship testing laboratories accredited by American Association of Blood Banks (AABB). AABB-accreditation is insufficient oversight, as it does not address how test limitations are communicated before testing nor how unusual test results or unexpected findings are handled.
- Relationship DNA testing for family verification should use the most appropriate technology to measure a range of relationships, not just parentage. Rapid DNA tests at this time can only be applied to parent-child and full sibling relationships.

Privacy concerns
- Privacy is a fundamental human right identified in the Universal Declaration of Human Rights. A proposal with international implications must extensively engage with relevant international laws and guidelines on data privacy.
- This proposal marks a major shift toward ongoing dataveillance of immigrants, and even of U.S. citizens and lawful permanent residents. The proposed rules note DHS made the decision to move "beyond only eligibility and admissibility determinations" in order to enable "identity management" and "enhanced vetting." These applications mark major departures from agency privacy practices that recognize the critical importance of nuance, context, and discretion under the Privacy Act of 1974 (5 USC § 552a).
- The proposed rules allow sharing of DNA test results and biometric data "with other agencies where there are national security, public safety, fraud, or other investigative needs." There should be clear guidelines for use or sharing of biometric data, including DNA test results.

COMMENTS

1. The 30-day comment period is insufficient.

The 30-day window for public comments is insufficient to address proposed policy changes of such magnitude and complexity, particularly as the window falls within a presidential election year during a global pandemic. The proposed rules involve a dramatic shift in policy, expanding the types of biometrics collected and broadening the use of biometric data significantly. Despite the complexity and magnitude of the proposed policy changes, DHS has limited the opportunity for public comments to a mere 30 days, requiring comments to be submitted by October 13, 2020. Each section of the proposed rules contains scientific, legal, and ethical aspects that warrant further evaluation by experts in fields including but not limited to genetics; biometrics; forensics; ethics; and distinct areas of law (such as immigration, family, constitutional, administrative, national security, cybersecurity, and data privacy). We are in support of our colleagues who have requested an extension of the comment period.[2]

2. The proposed rules attempt too much, too fast.

The ambitious breadth of the 85-page NPRM conflates processes that should be considered separately: (1) vetting of those seeking immigration benefits; and (2) verification of family relationships. The proposed rules also attempt to make too many changes too quickly. We call into question both DHS's authority to implement the proposed changes and its capacity to implement the policies evenly across populations in a way that is sensitive to the complexities of evolving technologies (e.g., rapid DNA, facial imaging). Each of these topics involves different legal authorities; therefore, Congressional authorization should address each separately.

In addition, we strongly recommend that Congressional authorization set up an interdisciplinary group beyond the AABB to evaluate and oversee the uses of DNA technology in immigration cases (discussed further below, section 4). This is crucial given the continuous advances in technology, the privacy and ethical issues involved, and the legal complexity of incorporating these factors into a regulatory and enforcement structure.

3. The proposed rules conflate DNA testing and DNA collection.

While we appreciate the increased transparency provided by the NPRM's descriptions of expanded DNA testing and collection of biometric data, addressing these distinct challenges in a single executive notice is inappropriate. The proposed rules outline two separate processes: (1) the expanded definition for and uses of biometrics (including DNA as a biometric); and (2) the systematic implementation of DNA testing for verification of family relationships. The general public and media routinely confuse DNA testing and DNA collection. This NPRM undermines efforts to differentiate these processes, which are distinct in terms of outputs (biometric data vs. DNA test results). The proposed rules outline that DNA data will *not* be a biometric tool *except* following DNA relationship testing. DHS acknowledges that DNA samples acquired for these tests will not be retained and yet outlines plans for retention of a "partial DNA profile"[3] resulting from DNA testing. While we, as experts, can recognize the intent of DHS in differentiating samples from data, the conditions for retention of data need to be clear.

Oversight of DNA testing is complicated, with different mechanisms for oversight of clinical genetic testing (i.e., through the Department of Health and Human Services), forensic DNA testing (i.e., through the Department of Justice), and relationship testing. In fact, relationship DNA testing has very weak oversight (discussed below, section 4). Nevertheless, the need for oversight of the testing process belies the difference between DNA testing and DNA data as a biometric. The validity of equipment used in developing DNA data from a biological specimen is certainly important in both circumstances. However, how data are utilized and how resulting data are secured are handled differently. DNA data as a biometric need not be subject to the same level of scrutiny as DNA testing, as long as the analytic validity of the equipment is sufficient.

[2] *Id.*
[3] E.g., 85 FR 56338

Combining these two sets of rules confuses the public into thinking that DNA data collection will be expanded within USCIS; this might indeed be the eventual intention of USCIS, but it is not the stated purpose of this NPRM (excepting the vague "partial DNA profile" retention plans). Each of these processes should be addressed in separate final rules since legal authority and parameters for DNA testing are different from those of the collection and storage of biometric information, including DNA data.

4. The proposed rules deploy DNA technologies with limited capabilities and limited oversight. The proposed rules describe the use of rapid DNA technologies to verify claims of family relationships, in part to detect potential cases of child trafficking. Rapid DNA testing is indeed a valuable emerging technology;[4] however, it is limited. Rapid DNA tests rely on a type of DNA test (STRs, short tandem repeats) that are only able to detect parent-child and full sibling relationships. Since migrating family units often are composed of non-parentage relationships, relying on this limited technology will not be effective. Relationship DNA testing for family verification should use the most appropriate technology to measure a range of relationships, not just parentage. For instance, single nucleotide polymorphism (SNP)-based haplotype DNA tests (similar to what is used in commercial ancestry DNA tests) would detect a broader range of and more distant relationships such as half-siblings and cousins.

Validation of rapid DNA is in its early stages. The FBI has validated two vendors for use in booking stations for known DNA samples.[5] The technology has yet to be validated by the forensic community for relationship testing or evidence processing. The process for validation is not arduous, as rapid DNA has proven to be an effective tool for disaster victim identification[6] and rape kit analysis.[7] Yet the lack of peer-reviewed evidence of its validation in immigration-based relationship testing applications highlights the prematurity of implementation at this time. Before a technology is accepted and written into federal policy, the scientific community should consider and embrace the validity of the tool.

In addition to rapid DNA technology, the proposed rules also suggest reliance on relationship DNA testing laboratories accredited by the AABB. AABB-accreditation is insufficient oversight for this purpose, as it oversees the technical validity of genetic testing for relationships, but not the application validity.[8] AABB is a professional organization. The relationship testing laboratory standards are set by a membership roster comprised of laboratory personnel from the commercial organizations conducting DNA testing. This self-oversight system is insufficient to ensure quality and accuracy of testing processes. We do not have specific concerns for AABB-accredited relationship testing laboratories currently conducting DNA testing. Rather, we advocate that if these laboratories are to be relied upon to

[4] Rapid DNA technology is distinct from traditional identity DNA analysis in a forensic laboratory setting. Its portability and the relatively faster processing time from sample collection to analysis lend themselves to contexts where on-site testing is desirable. The potential for non-expert users to operate rapid DNA instruments (with proper training) also allows the possibility for its use in a variety of contexts. Provided non-expert operators have proper training, the hands-free testing enabled by rapid DNA and the involvement of relatively fewer people in the movement of sample to instrument lower risks of sample contamination or swapping. Rapid DNA also offers potential privacy benefits by exposing DNA samples to fewer people; offering built-in data access controls and the ability to expunge data from the instrument's internal database; and exhausting DNA specimens (providing that the sample is not split). While these qualities provide utility, they also have the potential to ameliorate or amplify social, ethical, and legal challenges in the use of forensic DNA and to create new challenges. Implementation of and policies for the use of rapid DNA must be governed by the suitability of current rapid DNA cost and capabilities to purpose and context-specific ethical and social implications.

[5] The ANDE technology was validated in 2018 (ANDE. *ANDE corporation's rapid DNA identification system first to receive FBI approval under new standards*. June 4, 2018. Available at https://www.ande.com/press/archive/ande-rapid-dna-approved-by-fbi-first/); the Thermo Fisher Scientific technology in 2020 (Thermo Fisher Scientific. *FBI approves Thermo Fisher Scientific's rapid DNA solution for national DNA index system*. September 8, 2020. Available at https://www.prnewswire.com/news-releases/fbi-approves-thermo-fisher-scientifics-rapid-dna-solution-for-national-dna-index-system-301124673.html)

[6] E.g., Gin K, Tovar J, Bartelink EJ, Kendell A, Milligan C, Willey P, et al. The 2018 California wildfires: Integration of rapid DNA to dramatically accelerate victim identification. *J Forensic Sci*. 2020 May;65(3):791-9

[7] E.g., von Ancken E. DNA machine promises to catch killer, identify bodies, assist rape victims. *Clickorlando*. March 25, 2020. Available at https://www.clickorlando.com/news/local/2020/03/25/dna-machine-promises-to-catch-killer-identify-bodies-assist-rape-victims/

[8] American Association of Blood Banks. *Standards for relationship testing laboratories*, 14th edition, effective January 1, 2020. October 8, 2019

fill such an ongoing and important role in the immigration process, then federal oversight is essential to uphold the quality and integrity of the laboratories in the coming decades.

Some AABB-accredited relationship DNA testing laboratories provide SNP-based DNA testing services; however, this technology is rarely applied in typical relationship tests (i.e., paternity cases), so AABB guidelines for SNP testing are limited.

Finally, the costs of rapid DNA testing and/or testing through AABB-accredited relationship DNA testing laboratories must be weighed against the limited applicability of DNA testing to assess only certain types of family relationships.

5. DNA testing for verification of family relationships should not be dispositive.

DNA testing in immigration must be considered as an inclusionary tool to protect the family unit rather than as an exclusionary tool, as is proposed by DHS. Attention must be given to avoid the ignorant application of an ethnocentric and geneticized definition of "family" in immigration contexts that would likely cause structural violence. DNA testing in immigration has had a controversial history; an expansion of DNA testing has occurred over the years[9] whilst underlying statutory language remains unchanged, caught up in broader immigration reform gridlock.[10] The USCIS launched a pilot program in 2008 requiring DNA testing for family reunification of refugees under a Priority 3 (P-3) petition (8 CFR 204.2(d)(2)(vi),10).[11] The 2008 pilot program was aimed at East African refugees applying for entry into the United States.[12] The report seemed to corroborate prior reports of high levels of fraud among East African family refugee applications[13] but failed to differentiate those families who simply failed to appear for DNA testing from those deemed "fraudulent cases."[14] In 2010, the Department of State passed new

[9] The 2000 USCIS Cronin memo (Cronin MD. *Memorandum for all regional directors: Guidance for processing applicants under the north American Free Trade Agreement (NAFTA)*. July 24, 2000) allowed field offers to *suggest* DNA testing when documentation or blood type testing of familial relationships was inconclusive. In 2006, the USCIS Gonzalez Memo (Gonzalez ET. *Recommendation from the CIS Ombudsman to the Director, USCIS. Recommendation to accept DNA test results as secondary evidence of family relationship, to grant authority to directors to require DNA testing and to initiate a DNA testing pilot project to study the impact of requiring DNA testing as evidence of family relationship*. April 12, 2006) and the 2008 USCIS Aytes memo (Aytes ML. *Memorandum: Genetic relationship testing; suggesting DNA tests revisions to the Adjudicators Field Manual (AFM) Chapter 21 (AFM Update AD07-25)*. March 19, 2008) acknowledged that there was no legal authority to require DNA testing. In 2010, came an announcement that the P-3 program would resume with mandatory DNA testing to verify claimed familial relationships (75 FR 54690. *60-day notice of proposed information collection: DS-7656; Affidavit of Relationship (AOR); OMB Control Number 1405-XXXX*. September 9, 2010)

[10] See recent chapter on DNA and immigration: Katsanis SH. Tracing windblown seeds: Genetic information as a biometric for tracing migrants in the U.S. In *Silent Witness: Applying Forensic DNA Analysis in Criminal and Humanitarian Disasters*, Eds. Erlich H, Stover E, and White T. Oxford University Press; 2020

[11] The United States Department of State considers refugees for admission to the United States that are referred by the United Nations High Commissioner for Refugees (UNHCR) under three priorities: Priority 1 - Individual cases referred by designated entities to the program by virtue of their circumstances and apparent need for resettlement; Priority 2 - Groups of special concern designated by the Department of State as having access to the program by virtue of their circumstances and apparent need for resettlement; and Priority 3 - Individual cases from designated nationalities granted access for purposes of reunification with family members already in the United States (U.S. Department of State, Citizenship and Immigration Service. *Visas and DNA*. 9 FAM 601.11. 2017)

[12] Esbenshade J. *Special report: An assessment of DNA testing for African refugees*. Immigration Policy Center, American Immigration Council. October 21, 2010. Available at https://www.americanimmigrationcouncil.org/research/assessment-dna-testing-african-refugees

[13] As outlined by the U.S. Department of State, Bureau of Population, Refugees, and Migration. *Fact sheet: Fraud in the refugee family reunification (Priority Three) program.* Washington, DC. 2008

[14] The Esbenshade 2010 report noted the mis-attribution of the term "fraud" to a wide-number of anomalous cases, "While it was widely reported that over 80% of cases were fraudulent, this figure includes all cases in which one or more family members did not show up to the interview, one or more family members refused the test (which was presented as voluntary),20 or the results indicated that one or more relationships were not what they were claimed to be. For example, if a case was comprised of five family members and DNA tests proved claimed relationships for only four, the whole case was considered fraudulent. A very large number of people either refused to take the test or did not show for it, and in the larger (3,000 person) sample this accounted for the "great majority" of negative cases, according to the State Department. A no-show (even one out of five people on an application) was interpreted as a fraudulent case without deducting even the normal rate of no-shows, which—while much smaller—was not insignificant. The government, however, will not release the underlying statistics"; See also

rules requiring DNA testing for international refugees seeking to reunify with their families in the United States.[15]

Edward S. Dove, a law professor at University of Edinburgh wrote that, "the refugee's body has become a site of evidence where truth lies and fraud lurks. 'Family' has regressed from relational understanding to biological, corporeal understanding."[16] Legal scholar Emily Holland advocated at the time of the P-3 DNA testing rules that the United States adopt a broader definition of "family" to encompass members who might not have biological ties but who otherwise comprise a support system for a refugee.[17] She noted, "Officials tasked with reuniting refugees with those whom they consider to be family members, even when there are no biological ties, should understand that a broader definition will ensure that refugees have a support system and enable them to become self-sustaining residents more quickly."[18] A broader definition of family strengthens migrants' success once re-settled into their communities. This notion of a broader social definition of family is echoed by others criticizing reliance on DNA testing in immigration processes.[19]

Importantly, the real likelihood of detecting non-paternity in cases where a father is unaware of his biological relationship to his child can and will lead to violence against women. Many women are raped, and migrant women in particular are raped during passage. Resulting pregnancies are commonly masked, and revelation of the violence through DNA testing is certain to incite further the violence.[20] No woman should be forced to reveal the paternity of a child under these circumstances or against her will.

A 2008 note by the UN High Commissioner for Refugees (UNHCR)[21] underscored that DNA testing must be "carefully regulated" in order to not infringe upon the international human right of the family to be recognized and protected by the State, including as per Article 23 of the International Covenant on Civil and Political Rights (ICCPR), a treaty which the United States has signed and ratified.[22] Importantly, UNHCR indicated that (1) DNA testing for verification of familial relationships was to be a matter of last resort, reserved for those rare instances "where serious doubts remain after all other types of proof have been examined, or where there are strong indications of fraudulent intent and DNA testing is considered as the only reliable recourse to prove or disprove fraud;" (2) that DNA test results indicating a lack of a genetic relationship are not, in and of themselves, "conclusive of fraudulent intent;" (3) a culturally sensitive definition of "family" must be applied; and (4) pre-test counseling by qualified professionals is imperative.

The proposed rules do acknowledge "DHS recognizes that there are qualifying family members, such as adopted children, who do not have a genetic relationship to the individual who makes an immigration benefit request on their behalf."[23] Still, the rules need to specify how family units are selected for DNA testing in order to assure fair and effective use of the technology among populations. DNA testing should remain one tool among others—such as collection of biographical details to contextualize relationships—to verify claimed relationships and must not be used as the definitive tool for deciding family

Dove ES. Back to blood: The sociopolitics and law of compulsory DNA testing of refugees. *University of Massachusetts Law Review*. 2013;8(466):1-42

[15] 75 FR 54690, see *supra* note 9

[16] See Dove 2013, *supra* note 14

[17] Holland E. Moving the virtual border to the cellular level: Mandatory DNA testing and the U.S. refugee family reunification program. *California Law Review*. 2011;99:1635-1682

[18] *Id*.

[19] Heinemann T, Lemke T. Suspect families: DNA kinship testing in German immigration policy. *Sociology*, 2013;47(4):810-826

[20] *Supra* note 12

[21] UNHCR. *UNHCR note on DNA testing to establish family relationships in the refugee context*. June 2008. Available at: https://www.refworld.org/docid/48620c2d2.html

[22] The United States signed the ICCPR in 1977 and ratified the ICCPR in 1992, attaching "an unprecedented number" of reservations, understandings, and declarations. Pursuant to the Supremacy Clause of Article VI of the U.S. Constitution, ratified treaties are binding "law of the land." See Schabas WA. Invalid reservations to the International Covenant on Civil and Political Rights: Is the United States still a party? *Brooklyn J Int'l L*. 1995;21(2):277-325; see also United Nations. International covenant on civil and political rights. *United Nations Treaty Collection*, Chapter IV: Human Rights. December 16, 1966

[23] 85 FR 56341

membership. Congress should specify whether and under what circumstances DNA testing can be used as an inclusionary tool and, to prevent discrimination, should prohibit DHS and other federal agencies from using DNA testing as an exclusionary tool.

6. DHS has failed to adequately justify the proposed rules.

DHS has failed to adequately justify their increasing reliance on biometric analysis. The NPRM suggests that automated and digitized systems of identity verification will help DHS modernize and move away from paper-based documentation and other biographical evidence for proof of identity. DHS purports to justify the proposed changes, therefore, by referring to the convenience of modernizing identification systems. However, the need for technical updates to our immigration system does not automatically provide a blanket justification for the changes proposed by DHS. Reduced reliance on documents is insufficient cause to justify the measures taken. In fact, a general call for modernization only begs the question of how we should modernize DHS functions and underscores that this modernization should be directed by Congress through express statutory authorization.

DHS also identifies child trafficking as a central justification for the proposal. However, DHS asserts without evidence that biometric identification can effectively reduce the incidence of child trafficking. DHS does not present any evidence to convincingly support the claim that establishing familial relationships through DNA screening reduces child trafficking. As discussed in section 5 above, familial relationships are not necessarily defined by genetic information, and non-traditional families may face discrimination and unfair assumptions of illegal activity.

Congressional action is needed to justify the expanded collection of biometric data for child trafficking purposes, including a congressional finding that biometric data collection and analysis can serve the goals of combatting and preventing this social issue. DHS has not articulated clearly or with any specificity how or why an increased reliance on biometrics will solve the problem of child trafficking, neither do they point to no congressional findings to that end. In fact, current legislators who seem to support expanded use of biometrics—such as Senator Marsha Blackburn (R-TN) and Senator Joni Ernst (R-IA), cosponsors of S.2420, the End Trafficking Now Act, which would amend the Immigration and Nationality Act to allow DNA testing, or Rep. Ken Calvert (R-CA-42), sponsor of H.R. 364, SAFER Act of 2019, which would expand reliance on biometrics for certain refugees)—have not offered any congressional findings as the foundation for their proposals (nor have they marshaled the support of any additional cosponsors for those efforts).

Moreover, a coalition of legislators (16 original cosponsors of S.557, the REUNITE Act) have indicated that use of DNA testing for family reunifications in particular requires, amongst other items, joint guidance outlining with specificity the coordinated efforts of various agencies. Within this bill, these 16 senators have underscored that reliance on DNA testing as part of any family reunification effort must be a technique of last resort (with the potential use limited to only those instances in which reliance upon documents, representations, and observations of interactions between adults and children has not settled the determination of family relationships); must be subject to significant confidentiality protections and constraints on uses of the genetic information; and must enhance protections for families that have been separated.

Notably, comprehensive immigration reform (S.744, 113th Congress) would have expanded the collection and use of biometric screening of *foreign individuals* seeking admission into the United States and would have instructed DHS to create an entry-exit system (limiting such a system to non-citizens). While that bipartisan effort passed in the Senate, the House of Representatives never brought the bill to the floor. The desire to modernize the use of biometrics within immigration contexts is not a sufficient basis for these proposed rules. Congress has had numerous opportunities to delegate authority to modernize the use of biometrics in immigration and has failed to do so. DHS cannot move forward without the prerequisite delegation of authority from Congress, regardless of whether it is a good policy decision or not. These proposed rules attempt to go above and beyond the reforms that had bipartisan support. DHS is acting *ultra vires* and the proposed rules violate the constitutionally mandated separation of powers.

7. DHS has failed to identify their authority to propose these rules.

Congress did not delegate to DHS the authority to update the definition of biometrics nor to modernize its use and collection. Therefore, the proposed changes would constitute an unlawful and arbitrary abuse of power. In the NPRM, DHS cites specific authority in five statutes, which do *not* actually delegate the authority to update the biometrics definition. First, DHS employs 8 USC § 1125(d)(3), which states that it has the "power…to take and consider evidence of or from any person." Second, they cite 8 USC § 1357(b), which gives DHS the authority to "take and consider evidence concerning the privilege of any person to enter, reenter, pass through or reside in the United States, or concerning any matter which is material or relevant to the enforcement of this chapter and the administration of the Service." Neither statute has been interpreted to compel an immigrant to submit to DNA testing. Third, 8 USCS §§ 1444 and 1446 require submission of photographs and a personal investigation before an application for naturalization, citizenship or other similar requests may be approved. In *Mahamoud v. Mueller*, 2007 U.S. Dist. Lexis 81056 at *9 (S.D. Ohio 2007), the court only interpreted "personal investigation" to mean that the Attorney General should consider the "vicinities in which such person maintained his actual place of abode and in the vicinity or vicinities in which such person has been employed or has engaged in business or work for at least five years immediately preceding the filing of his application for naturalization." Fourth, 8 USC §§ 1302(a) and 1304(a) provide direct statutory authority for the collection of fingerprints for the purpose of registering immigrants; however, this statute neither allows for DNA collection nor provides DHS the authority to update the definition of biometrics. Therefore, none of the statutes cited by DHS are demonstrative of authority having been delegated by Congress to update (i.e., redefine) the definition of biometrics.

Further, there are several statutes that preclude the agency from enacting the proposed changes because they specifically provide the biometric data to be collected without mentioning DNA. For example, 8 CFR § 236.5 provides that "[e]very alien 14 years of age or older against whom proceedings based on deportability under section 237 of the Act are commenced under this part by service of a notice to appear shall be fingerprinted and photographed." By proposing to make the submission of DNA test results mandatory for all individuals associated with an application for an immigration benefit, *regardless of age*, DHS is attempting to override statutory law.

DHS also cites the Immigration and Nationality Act, 8 USC § 1103(a), as a general authority to the Secretary of Homeland Security (hereafter referred to as "the Secretary") to update the statutory definition of biometrics. However, this statute delegates to the Secretary only the "*administration and enforcement* of this act and all other laws relating to the immigration and naturalization of" immigrants (85 FR 56339, emphasis added). This statute does not confer on the Secretary the right to legislate; further, the statute does not suggest that the Secretary has the authority to override longstanding precedent and Congressional authority alike by redefining the meaning of the language contained in relevant statutes governing the practices of the agency. If the Secretary did have the authority to unilaterally override or otherwise determine the laws by which DHS is regulated, the agency would face no meaningful oversight or regulation. Therefore, the proposal is in clear violation of the constitutional principles on which our federal government is based.

The proposal also expands the definition of biometrics to authorize the collection of personal data for the purposes of vetting and tracking individuals throughout the "immigration lifecycle."[24] In 34 USC § 12592(b)(3)(D), Congress provided guidelines for the establishment of a federal index of DNA identification records that outlaw the stated ambitions of the DHS proposal in question. The law clearly provides that the index described in subsection (a)[25] of the statute "shall include only information on DNA identification records that are… maintained by Federal, State, and local criminal justice agencies… pursuant to rules that allow disclosure of stored DNA samples and DNA analyses only… if personally

[24] E.g., 85 FR 56338

[25] 34 USC 12592 (a)(1-4) states in (a)(1)(C): "other persons whose DNA samples are collected under applicable legal authorities, provided that DNA samples that are voluntarily submitted solely for elimination purposes shall not be included in the National DNA Index System"

identifiable information is removed, for a population statistics database, for identification research and protocol development purposes, or for quality control purposes." By proposing to create a DNA identification records database for the purposes of enhanced vetting and tracking throughout the "immigration lifecycle," DHS seeks to create a population statistics database without removing personally identifiable information. Not only does DHS lack the authority necessary to institute the proposed changes, but also the changes themselves are unequivocally unlawful.

Finally, congressional and judicial precedents have made it abundantly clear that the federal government has the right to collect, store, and analyze DNA records only in the course of investigating serious crimes of a violent nature.[26] The DHS proposal is also in conflict with these precedents and would be unlikely to receive congressional or judicial approval under scrutiny.

8. DHS does not have the authority to redefine biometrics.

The proposed rules cite several statutes where Congress has defined biometrics; not only did Congress not include DNA in any of these statutes despite detailed consideration of biometrics, they have also never been interpreted to include DNA in court.[27] DHS is acting in conflict with Congress's demonstrated understanding of current limitations. Congress has introduced bills attempting to authorize DNA testing (e.g., S. 2420 or H.R. 3864; S.557 and H.R.1012; H.R. 364) but none have passed. An examination of legislative activity between January 1, 2019 and September 1, 2020 conducted using Congress.gov confirmed that Congress has not used "biometrics"; "biometric information"; or "biometric data" consistently and has not used "biometrics" as a general catchall concept to authorize any and all forms of biometrics that an administrative agency might consider advantageous. Rather, Congress regularly deploys a specific term for a specific policy context or application.[28] These proposed rules are not on solid footing as DHS has assumed that Congress has delegated broad, general authority where Congress, in fact, has demonstrated repeatedly through its legislative actions that it has not.

DHS seeks to establish its own new standard definition of "biometrics" that would apply uniformly. Based on this new definition and deployment of a novel term of art ("authorized biometric modalities"),[29] DHS would determine for itself which kinds of biometrics it collects and uses. This novel agency definition of "biometric modalities" would presumably enable DHS to collect and use palm prints, voice

[26] The DNA Analysis Backlog Elimination Act of 2000 (Public Law 106-546) authorizes DNA record maintenance for criminal justice, with qualifying federal offenses including murder, sexual abuse, peonage and slavery, kidnapping, and robbery. The Patriot Act of 2001 (Public Law 107-56) list of offenses related to terrorist activity is extensive, but nowhere includes any mention of applying for immigration benefits

[27] First, DHS cites 18 USC § 1028(d)(7)(B) and 17 CFR 162.30(b)(8), which both define "unique biometric data" as one "means of identification" consisting of "fingerprint[s], voice print[s], retina or iris image[s], or other unique physical representation[s]." Further, in *United States v. Zheng*, 762 F.3d 605, 609 (7th Cir. 2014), the court defined "means of identification" as a "very broad" term, yet it still did not include DNA. Instead, the court stated that means of identification primarily refer to "intangible identifying information" such as "name[s], date[s] of birth, Social Security number[s]." Second, DHS cites 8 USC § 1732(b)(1), which requires that the Attorney General and the Secretary of State "issue to [immigrants] machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers." In *Santillan v. Gonzales*, 2005 U.S. Dist. Lexis 39118 at *6 (N.D. Cal. 2005), the court only referred to "biometric identifiers" as "data-fingerprints, photographs, and the like," without mention of DNA. Third, 27 CFR 73.3 and 21 CFR 11.3(b)(3) both define biometrics as a "method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable." Courts have never interpreted "physical feature(s)" and "repeatable action(s)" to include DNA

[28] Of 344 bills identified through eight separate search strings, 42 involved facial imaging (mentioning "faceprint" and/or "facial recognition"); 165 involved biometrics (mentioning "biometrics," "biometric information," or "biometric data"); and 137 involved genetics (mentioning "genetic information," "genetic data," or "DNA"). The overlap of bills identified through these eight separate searches revealed 233 unique bills. Only six (less than 3%) of those mentioned "faceprint," and only 84 of the 233 (approximately 36%) mentioned "DNA." If the concept of biometrics were envisioned generically, one would anticipate that bills involving biometrics would be uniformly identifiable using "biometrics," "biometric information," and "biometric data" as search terms; however, this is not the case. Of the 165 bills identified through the three searches, 102 were unique. Of those, the text of only two bills included all three terms. Seven (6.9%) used "biometrics" and "biometric information" but not "biometric data;" 31 (30.4%) used "biometrics" and "biometric data" but not "biometric information;" and 62 (60.7%) used only "biometrics"

[29] E.g., 85 FR 56341

prints, iris scans, facial imaging, and DNA data even in contexts in which the statutory authority only anticipated or referenced signatures, fingerprints, and traditional photographs.

The citations provided within the proposed rules do not support the inclusion of DNA within the definition of biometrics nor the agency's authority to undertake the proposed changes. DHS seeks to update the definition of the term "biometrics," notably by including DNA in order to require the submission of samples "in connection with services provided by the [agency]."[30] Further, the proposed rules state that anyone seeking an immigration benefit is subject to the agency's authority to collect biometrics but does not provide a framework for who will be subject to this biometrics requirement.[31]

Moreover, nearly three years ago (on December 21, 2017), Senators Edward J. Markey (D-MA) and Mike Lee (R-UT) sent a letter to DHS Secretary Kirstjen Nielson noting, "…the use of the program on U.S. citizens remains facially unauthorized."[32] In their letter, the Senators demanded that DHS indicate with specificity what authority it was relying upon for its biometric expansion plans; stated unequivocally, "Congress has pointedly neglected to authorize DHS to use the [biometric scanning] program on U.S. citizens for any purpose;" and underscored, "convenience should not be placed above congressionally mandated requirements."[33] In a follow-up letter on May 11, 2018, the Senators reiterated their concerns and requested details on how data will be safeguarded.[34] Similarly, in July 2019, Rep. Zoe Lofgren (D-CA) reportedly commented that facial recognition scans are "a massive, unwarranted intrusion into the privacy rights of Americans without authorization by law."[35] Local bans, moratoriums, and limitations are spreading across the United States,[36] further underscoring the public's opposition to governmental use or expansion of facial recognition technologies.

9. The proposed rules rely on a controversial executive order that excludes non-resident foreigners from The Privacy Act of 1974.

Biometric identification often anchors the process of immigration-based screening and vetting. As part of recent vetting protocols, DHS also seeks social media identification data and tracks social media activities. In the proposed rules, DHS expressly plans to authorize the collection and use of a wide range of biometrics for a wide range of purposes, including "[i]dentity enrollment, verification, and management in the immigration lifecycle; national security and criminal history background checks; determinations of eligibility for immigration and naturalization benefits; and the production of secure identity documents."[37] The NPRM itself notes DHS made the decision to move "beyond only eligibility

[30] 85 FR 56341
[31] 85 FR 56340
[32] Markey EJ, Lee M. Letter to The Honorable Kirstjen Nielson. December 21, 2017. Available at https://www.lee.senate.gov/public/index.cfm/2018/6/sens-lee-markey-release-statement-on-facial-recognition-technology-uses-at-airports
[33] *Id*.
[34] Markey EJ, Lee M. Letter to The Honorable Kirstjen Nielson. May 11, 2018. Available at https://www.lee.senate.gov/public/index.cfm/2018/6/sens-lee-markey-release-statement-on-facial-recognition-technology-uses-at-airports
[35] Harwell D. Facial-recognition use by federal agencies draws lawmakers' anger. *The Washington Post*. July 9, 2019. Available at https://www.washingtonpost.com/technology/2019/07/09/facial-recognition-use-by-federal-agencies-draws-lawmakers-anger/
[36] E.g., San Francisco, CA; Oakland, CA; Somerville, MA; Brookline, MA; Portland, OR; and Pittsburgh, PA (see e.g., Harwell D. Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use. December 19, 2019. Available at https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/; Davidson T. Mayor Peduto to sign legislation restricting facial recognition in Pittsburgh. *TribLIVE*. September 22, 2020. Available at https://triblive.com/local/mayor-peduto-to-sign-legislation-restricting-facial-recognition-in-pittsburgh/; Bond P, Cloves E, Serafino M. Preparing for the next front in biometric class actions: Portland's facial recognition ban. *JD Supra*. September 22, 2020. Available at https://www.jdsupra.com/legalnews/preparing-for-the-next-front-in-74867/; and Round I. Bill introduced in Council to ban facial recognition technology. *Baltimore Brew*. September 21, 2020. Available at https://baltimorebrew.com/2020/09/21/bill-introduced-in-council-to-ban-facial-recognition-technology/)
[37] 85 FR 56355

and admissibility determinations"[38] in order to enable "identity management and enhanced vetting."[39] This pursuit of "enhanced vetting" from the current administration has involved a blunt approach to the Privacy Act of 1974 and a major departure from agency privacy practices that recognized the critical importance of nuance, context, and discretion in the application of the Privacy Act of 1974 to non-resident foreigners.

In February 2017, following Executive Order (E.O. 13,768) issued on January 25, 2017, the administration mandated agencies to "ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information." Parts of that Executive Order have already been deemed unconstitutional, and privacy experts who analyzed E.O. 13,768 for the World Privacy Forum concluded it could "fatally undermine" the then fragile EU-U.S. Privacy Shield Agreement. On July 16, 2020, that privacy shield was, in fact, invalidated by the Court of Justice of the European Union in its Schrems II decision. The Court of Justice explained (with emphasis in the original):

> In the view of the Court, the **limitations on the protection of personal data arising from the domestic law of the United States on the access and use by U.S. public authorities** of such data transferred from the European Union to that third country, which the Commission assessed in Decision 2016/1250, **are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary.**

The uncertain legality of E.O. 13,768 and Schrems II decision underscore the wide-ranging implications and costs of this proposed rule that have not been adequately evaluated by DHS.

10. The proposed rules adversely impact the privacy rights of U.S. citizens and permanent residents.

Beyond proposing complex and broad changes which should be left to Congressional authority and oversight, the proposed rules have serious implications for privacy. This proposal marks a major shift toward ongoing dataveillance of not only immigrants but also U.S. citizens and lawful permanent residents. We are particularly concerned about what happens to data after an immigrant is sworn in as a U.S. citizen. The biometric data is to be used throughout the "immigration lifecycle," but once an immigrant becomes a U.S. citizen, that data would still exist within DHS, creating a sub-class of U.S. citizens for whom there are significant privacy concerns.

The "enhanced vetting" and discontinuation of privacy protections for those who are not U.S. citizens or lawful permanent residents has major implications for the future of privacy and dataveillance for everyone in the United States, as do DHS's plans for "transitioning to a person-centric model for organizing and managing its records."[40]

Newly developed big data cybersurveillance tools fuse biometric data with biographic data and internet and social media profiling to assess risk. Consequently, the NPRM should be considered within a broader context of cybersurveillance capacities and dataveillance trends in governance norms. Multiple Executive Orders issued by the current administration mandate "Expedited Completion of the Biometric Entry-Exit Tracking System" by DHS. Current refugee vetting procedures include database screening through the U.S. Department of Defense (DOD) Defense Forensics and Biometric Agency's Automated Biometric Identification System. DHS specifies that vetting of refugees includes "[a] biometric record check of the [U.S.] Department of Defense's (DOD) records collected in areas of conflict (predominantly

[38] 85 FR 56350
[39] *Id.*
[40] 85 FR 56351. Interestingly, footnote 30 of the NPRM directs readers to https://www.dhs.gov/privacy for the DHS Privacy Impact Assessment for Continuous Immigration Vetting (February 14, 2019), but no such document is available at that location, and the item is not listed among the "Privacy Reports" or among "Privacy Policy" materials. Rather, those interested in this privacy impact statement must work to find it

Iraq and Afghanistan). DOD screening began in 2007 for Iraqi applicants and has now been expanded to all nationalities."[41]

The new DHS biometric collection and vetting program is mistakenly presented as affecting only noncitizens: immigrants, refugee and asylum applicants, and visitors seeking a travel visa to the United States. More accurately, the proposed rules should be understood as the embrace of a dramatic expansion of mass surveillance that attempts to assess criminal and terroristic risk across entire populations and subpopulations through mass data collection, database screening and data fusion, artificial intelligence, and algorithm-driven predictive analytics. The application of these technologies might eventually extend to the entire U.S. citizenry through a variety of policy proposals, including a biometric national identification system, and various mandatory vetting and database screening programs. The plans presented in the proposed rules appear to be the beginning of extended surveillance in the form of a mandatory national biometric database for "identity management":[42] (1) containing comprehensive dossiers of biographical information as well as DNA, faceprints, and other biometrics; (2) relying upon immigrants and their sponsors as the initial data subjects to develop and test those policies and processes; and (3) providing flexibility for DHS to make future changes to the types of biometrics collected (so-called "biometric modalities"[43]), the scope of individuals to whom the practices might be applied, and purposes for using the biometrics.

The enduring consequences of modern big data surveillance can be better envisioned by anticipating how and why big data vetting protocols may be extended to the entire population through "identity management" systems: systems that control methods enacted for identity verification. Eventually, all residents of the United States, both citizens and noncitizens, might face various stages of technological vetting and algorithmic screening as a part of a post-September 11, 2001 national security policy trajectory that embraces big data surveillance for its presumed efficacy. Importantly, in parallel with the extreme vetting protocols mandated by the administration's Executive Orders, almost every immigration reform effort since 9/11 has called for biometric data collection from the entire citizenry in the United States to enhance border security efforts. At the same time, increasing concern regarding homegrown terrorism has resulted in a call to extend domestic surveillance and counterterrorism efforts to both citizens and noncitizens. The Snowden disclosures, for example, have further revealed how foreign-intelligence- gathering tools, such as bulk metadata collection, can be indiscriminate in scope and impact both citizens and noncitizens.

DHS has not adequately considered the technical and ethical debts or long-term consequences of its proposed rules. Only a generic reference to "concerns germane to privacy, intrusiveness, and security" appears in the NRPM,[44] and nowhere does DHS mention—let alone address—"cybersecurity," "data privacy," "information privacy," "data access," "data misuse," "bias," "data justice," and "dataveillance." It is clear that DHS has not discharged its responsibility to account for and justify the costs (including the potential technological and ethical debts)[45] that such a proposed rule would compound if finalized in its current form. This lack of attention is particularly alarming given the recent report[46] issued by the Department of Homeland Security's Office of the Inspector General on September 21, 2020 (just 10 days

[41] USCIS. Refugee processing and security screening. Available at https://www.uscis.gov/refugees-and-asylum/refugees/refugee-processing-and-security-screening (explaining that refugee vetting procedures include database screening through the U.S. Department of Defense's Defense Forensics and Biometrics Agency's (DFBA) Automated Biometric Identification System (ABIS) and detailing that in addition to ABIS, biometric checks include FBI fingerprint check through Next Generation Identification (NGI) and the DHS Automated Biometric Identification System (IDENT))

[42] E.g., 85 FR 56340

[43] E.g., 85 FR 56338

[44] 85 FR 56388

[45] Fiesler C, Garrett N. Ethical tech starts with addressing ethical debt. *Wired*. September 16, 2020. Available at http://wired.com/story/opinion-ethical-tech-starts-with-addressing-ethical-debt/

[46] DHS Office of the Inspector General. Review of CBP's major cybersecurity incident during a 2019 biometric pilot. OIG-20-71. September 21, 2020. Available at https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf. See also DeChiaro D. Privacy of biometric data in DHS hands in doubt, inspector general says. *Roll Call*. September 29, 2020. Available at https://www.rollcall.com/2020/09/29/privacy-of-biometric-data-in-dhs-hands-in-doubt-inspector-general-says/

after the issuance of this NPRM) detailing how U.S. Customs and Border Protection (CBP) "did not adequately safeguard sensitive data" from the 2019 piloting of its facial recognition technology, which ultimately compromised the biometric data from 184,000 travelers and involved several images being posted to the dark web.

Further, in the criminal context, the United States Supreme Court upheld DNA collection as a reasonable search under the Fourth Amendment only when it is clear that the use was limited to identification and when collection and storage were standardized.[47] The Court noted that the Combined DNA Index System (CODIS, which connects DNA laboratories from the local, state, and national levels) is based on a limited number of genetic loci (currently 20), which are "noncoding DNA parts that do not reveal an arrestee's genetic traits and are unlikely to reveal any private medical information."[48] In this way, collection of DNA from arrestees was found to be acceptable because it only "relate[s] to the identification of individuals."[49] Therefore, based on its limited use and accuracy, the Court found the practice was constitutional.[50] The Court also emphasized that the DNA collection was "authorized by Congress" and that the DNA data analyses are "supervised by the Federal Bureau of Investigation (FBI)" to ensure compliance with the "scientifically rigorous" standards that CODIS employed.[51] The genetic testing outlined in the NPRM is designed to screen for fraud and child trafficking. If this is the goal, then the criminal investigation of human trafficking should be held to the same criminal justice standards, requiring standardization, validation, and oversight for scientific rigor. Based on the Supreme Court's analysis in the criminal context, it is unlikely that the NPRM's collection of DNA data would be constitutional because of the lack of information on standards, use, and storage.

11. Data sharing parameters need to be addressed.

The proposed rules allow sharing of DNA test results and biometric data "with other agencies where there are national security, public safety, fraud, or other investigative needs."[52] There should be clear guidelines for use or sharing of biometric data, including DNA test results. Details regarding data sharing with other agencies are absent from the NPRM; however, the NPRM allows considerable leeway for DHS to share. For instance, the rules suggest the use of DNA testing to verify family relationship claims to detect potential cases of child trafficking and proposes to retain genetic data as "partial DNA profiles" resulting from such tests. Such genetic data should not be used or shared for purposes outside of its intended use. Instead, genetic data should be destroyed and only the resulting test outcome (i.e., indication of confirmation of relationship) should be retained for immigration records. The proposed use of rapid DNA and relationship DNA testing through AABB-accredited laboratories will result in data created by and staying with commercial organizations. The protections of these data by the contracted commercial organizations must be outlined with specificity and scrutinized to prevent inadvertent release of or access to sensitive data by third parties. Interagency data sharing policies are frequently established through memoranda of understanding (MOUs),[53] which have drawn their own criticism.[54] It is a serious concern that law enforcement agencies and other governmental actors could circumvent data-access and use-

[47] *Maryland v. King*, 569 U.S. 435, 445 (2013)
[48] *Id*.
[49] *Id.* at 444
[50] Research since the 2013 *Maryland v. King* case has shown that forensic STR alleles could be connected to corresponding SNP haplotypes and vice versa. SNP haplotypes can reveal physical and health-related information. Edge D, Algee-Hewitt BFB, Pemberton TJ, Li JZ, Rosenberg NA. Linkage disequilibrium matches forensic genetic records to disjoint genomic marker sets. *Proc Natl Acad Sci USA*, 2017;114(22):5671-5676
[51] *King*, 412 U.S. at 445
[52] 85 FR 56354
[53] E.g., Rodriguez J. How does information sharing between DHS and other non-enforcement executive agencies work? *Bipartisan Policy Center*. April 17, 2018. Available at https://bipartisanpolicy.org/blog/how-does-information-sharing-between-dhs-and-other-non-enforcement-executive-agencies-work/
[54] The integrity of data protections established through MOUs might be undermined by high-ranking elected officials reportedly stating "…they don't mean anything." See Mason J. No more MOUs! USTR Lighthizer tweaks trade terminology after dispute with Trump. *Reuters.* February 22, 2019. Available at https://www.reuters.com/article/us-usa-trade-china-trump/no-more-mous-ustr-lighthizer-tweaks-trade-terminology-after-dispute-with-trump-idUSKCN1QB2OR

constraints (established through MOUs) by seeking access directly from the commercial entities. Since commercial entities are not subject to the same sunshine requirements as governmental agencies, these proposed rules need clarity regarding the data privacy and security protocols that will regulate commercial entities involved in this proposed program. Similarly, it is a concern that such data could be accessed by private individuals, given the patchwork of state laws governing genetic privacy and the uncertainty as to whether assurances (such as those offered for research data by Certificates of Confidentiality)[55] could effectively shield data in private entities' possession from disclosures compelled by subpoenas, warrants, and other legal processes. Left unaddressed, these concerns could become a substantial chill factor that frustrates the responsible inclusion of under-served and under-represented immigrant populations in genomic research and hinders precision and public health initiatives for immigrants and non-immigrants alike.[56]

It is unclear how the applicable regulatory limitations on how long and for what reasons federal agencies may keep DNA information in a database affect the expansion of its use into the "immigration lifecycle." The limits on how biometric data from U.S. citizens can be used for the purpose of family-based petitions needs to be delineated in the final rules, including what types of information are kept, what information is shared, and retention periods.

12. The proposed rules purport to provide clarity on how USCIS uses and intends to use biometric data; however, the long-term consequences are unknown.

It appears that the NPRM could advance much-needed transparency by providing the public with (1) data on how USCIS has used DNA testing; and (2) information on how USCIS uses and intends to use biometric data. The NPRM provides a potential road map for biometric collection in varying situations, estimated costs of implementation, and details on the rapid DNA pilot program begun in 2019. We applaud the transparency within the NPRM, for example the provision of data from the recent rapid DNA applications, "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 20*[sic]* percent)."[57] These figures are important in tracking the value of DNA testing for investigating cases of fraud and/or human trafficking. The proposed rules provide an opportunity to systematize the processes to ensure consistency in selection of family units for testing. However, the NPRM fails with this statement to define the "indicators of fraud" that lead to DNA testing for these select families, nor do they define the criteria for verifying the "432 incidents of fraudulent family claims."

The NPRM further fails to provide critically important information on how and whether acquired biometric data will be commingled with data in other biometric databases. It fails to outline the circumstances in which the biometric data might be used for criminal and/or terrorist investigations. It fails to describe whether acquired biometric data will be shared with the private sector pursuant to government contracts. It fails to explain to what extent biometric data will be shared with other federal agencies and the military. These specifics are essential for the American public to weigh the consequences of the proposed rules, which appear to infringe on current liberties.

13. The proposed rules will have detrimental effects on families, women, and racial and ethnic minorities.

DHS proposes to use a number of technologies that could contribute to disparate and discriminatory impacts of policies on different populations including diverse family structures,[58] women, and racial and

[55] See e.g., Wolf LE, Beskow LM. Genomic databases, subpoenas, and Certificates of Confidentiality. *Genetics in Medicine*. 2019;21:2681-2682

[56] E.g., Wagner JK. Ethical and legal considerations for the inclusion of underserved and underrepresented immigrant populations in precision health and genomic research in the U.S. *Ethnicity & Disease*. 2019;29(supp. 3):641-650

[57] 85 FR 56352

[58] Family is a social construct, not a biological one. Families can be made up of a variety of combinations of biological (e.g., parent(s)-child, grandparent-child, aunt or uncle-child, siblings), legal (e.g., adoptive, step), and/or caregiving (e.g., informal adoption) relationships. All of these types of relationships can have a bearing on immigration-related decisions on the part of

ethnic minorities. It is difficult to grasp the full impact of using a web of biometric technologies for "identity management," in part because biometric data can be inclusive of both hard biometrics (fingerprints) and soft biometrics (skin color). Thus, biometric identification can include biometric screening that uses soft biometric indicators (such as digital assessments of skin color and estimated age extracted from a digital photo) and can combine race data proxies with other proxy variables to purportedly predict criminal or terroristic behavior (e.g., aggregating passport number and digital photo with data analysis of web browsing activity and social media presence). In addition, there are multiple components to vetting and biometric identification technologies, including but not limited to record linkage, information extraction, and predictive analytics.

Notably, DHS is expressly advancing its interest in mass collection of facial images to be used for highly controversial facial recognition technologies. These technologies are heavily biased, as demonstrated by the National Institute of Standards and Technology (NIST) study reports.[59] Empirical evidence[60] has shown worrisome ethnicity, age, and gender bias of facial recognition technologies. Moreover, Congress has increasingly criticized the technology[61] because of, among other problems, its persistent bias against people of color.[62]

We note that the proposed rules plan to "accept DNA test results from relevant parties."[63] While we strongly assert that any expanded use of DNA data for immigration applications or petitions requires Congressional approval (with careful study and oversight), we do support the general idea that a future that genetic test results could be provided as part of an initial filing. Our research and experience in immigration law have shown us that streamlining the petitioning process can be beneficial for all parties involved. [64] For families who might lack other forms of documentation or evidence to establish familial relationships, the petition process could be expedited if they were allowed to voluntarily submit DNA testing up front. DHS should, however, specify expressly that it is inappropriate to draw inferences and conclusions from a failure to voluntarily submit a DNA test result. There are many instances when submission of DNA test results might not be practicable or preferential, such as for non-biological families (e.g., adopted children) or when the submission of biometric data would defy a cultural or religious practice of the immigrant petitioner.

14. The proposed DNA testing will have detrimental effects on children.

Increased reliance on DNA for verification of family units, especially with a focus on parent-child relationships, will lead to increased separations of children from accompanying caregivers.[65] A number of

the U.S. government, especially where the well-being of minors is concerned. In an immigration context where officials may encounter individuals with a variety of cultural understandings of and terms for familial relationships, this concept is key for officials to contextualize relationship claims. Given that the appropriate type of DNA testing is used to detect the claimed relationship and results are interpreted by an expert when needed (e.g., in rare cases such as chimerism), DNA testing provides one tool for investigating or proving relationship claims

[59] Reports on demographic effects and accuracy of FRT are ongoing. See NIST. Face recognition vendor test (FVRT) ongoing. Available at https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

[60] E.g., Porter J. Federal study of top facial recognition algorithms finds 'empirical evidence' of bias. *The Verge*. December 20, 2019. Available at https://www.theverge.com/2019/12/20/21031255/facial-recognition-algorithm-bias-gender-race-age-federal-nest-investigation-analysis-amazon

[61] E.g., Harwell D. July 19, 2019, *supra* note 35; and Harwell D. December 19, 2019, *supra* note 36

[62] Wiggers K. NIST benchmarks show facial recognition technology still struggles to identify Black faces. *Venture Beat*. September 9, 2020. Available at https://venturebeat.com/2020/09/09/nist-benchmarks-show-facial-recognition-technology-still-struggles-to-identify-black-faces/

[63] 85 FR 56353

[64] Both USCIS policy (8 CFR 204.2(d)(2)(v)) and Department of State policy (9 FAM 601.11-1(B)(a)(2)) preclude DNA evidence until the adjudicating officer has determined that initial evidence is unavailable or unreliable. That can take months or years, leaving families separated in some cases. Regarding the challenges posed by the inability to proffer DNA evidence without specific request by a government officer, see also Sheets K, Baird M, Berger D. Navigating DNA testing in immigration cases. *Bender's Immigration Bulletin* 2016;21:719-726

[65] Family separation based on inadequate technology has already caused incalculable harm. Shepherd K. The government knew it didn't have the technology to track separated families. It did so anyway. *Immigration Impact*. December 4, 2019. Available at https://immigrationimpact.com/2019/12/04/technology-to-track-separated-families/#.X3i1YXlKiUk

migrating family units are non-nuclear, with children arriving with aunts, uncles, siblings, half-siblings, grandparents, and non-biological family members. By prioritizing rapid DNA testing for only parent-child relationships, the inability to biometrically verify other relationships would necessitate separation of children from their caregivers. Since the 2008 Trafficking Victims Protection Act (TVPA),[66] and before, child advocates have relied on non-biological evidence, for example social clues when interviewing children and families to detect trafficking. Advocates might ask for medical records with caregivers' signatures, education records, or request stories from the children and families, assessing consistency. DNA testing is merely an additional tool for social workers and child advocates to detect human trafficking; it should not be the only tool and certainly should not be used to the exclusion of other approaches in screening for trafficking.

The final rules need to clarify how pre-test counseling will be conducted to communicate the limits of DNA testing for specific family relationships. Definitions of relationships vary among cultures, so counseling in relevant languages and with culturally-sensitive expertise is essential to preventing misunderstandings of the role of DNA data in detecting biological connections. The final rules also need to clarify how post-test counseling will be conducted in order to avoid inadvertent revelation of unexpected findings. Unexpected revelation of misattributed parentage is common in relationship testing, for example in cases where a child was switched at birth (i.e., in a hospital) or where a mother mistakes the identity of a biological father. In the medical community, rates of misattributed paternity are considered to range from 0.8% to 30% (median 3.7%).[67] As mentioned in section 5, in some instances, DNA testing will bring to light a family secret, such as undisclosed rape, secret adoptions, or a grandmother taking on maternal role for a teenage daughter's child. Revelation of these biological truths can bring trauma and/or violence to a family and disrupt a child's social structure. Care must be taken in how such findings are communicated.[68] In some cases, an unusual finding might be a biological anomaly that can be explained; in such instances, reliance on genetics experts to explain the findings to both the officials and the family is important.[69]

15. Data from children should be subject to greater protections than those of adults.

The proposal includes a dramatic expansion of collection and storage of data on children. DHS proposes to eliminate age restrictions for biometrics to allow for their collection and use across the lifespan and to eliminate the presumption of good moral character for people under 14 years of age. There is a long history of data from children being recognized as more sensitive than that of adults. The human subjects research regulations outline special protections for children and fetuses.[70] The Children's Online Privacy Protection Act of 1998 (15 USC 6501-6505), now more than 20 years old, provides requirements to ensure children's online privacy and extends those protections to all individuals under the age of 13. Included in the protected information are images of a child and the voice of a child, both potential biometrics under the NPRM.

Removing the presumption of innocence is contrary to the common law "infancy defense," which remains applicable in criminal proceedings involving individuals under the age of 14 and which has been recognized for hundreds of years.[71] Removing the presumption of innocence for children is also contrary to the growing trend to protect trafficked persons from punishment for acts taken at the demand of their oppressors (traffickers). Such action would subject children to unnecessary and unjustified criminal and

[66] William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008 (Public Law 110-457)

[67] Lowe G, Pugh J, Kahane G, Corben L, Lewis S, Delatycki M, Savulescu J. How should we deal with misattributed paternity? A survey of lay public attitudes. *AJOB Empir Bioeth.* 2017;8(4):234-242

[68] *Id*. And Prero MY, Strenk M, Garrett J, Kessler A, Fanaroff JM, Lantos JD. Disclosure of Misattributed Paternity. *Pediatrics.* 2019;143(6)

[69] Sheets *et al*. *supra* note 64

[70] 28 CFR part 46; and 45 CFR part 46, subpart D (§§ 46.401-46.409)

[71] E.g., *Com. v. Martz*, 2015 Pa. Super. 144, 118 A.3d 1175 (2015) (noting English common law—as well as common law in the United States since its inception—presumed that individuals under age 7 years were too young to be criminally culpable and recognized a rebuttable presumption that those between ages 7 and 14 years are too young to be criminally culpable). See also *Com. v. Green*, 396 Pa. 137, 151 A.2d 241 (1959) and *Com. v. Cavalier*, 284 Pa. 311, 131 A.229 (1925)

terroristic screening, potentially for the entirety of their lives. Detection of child trafficking is a laudable objective in screening arriving migrants and a necessary step under the TVPA[72] to protect children. Any potential victim of trafficking must be protected as they would be in other law enforcement circumstances. Similarly, victims' biological data from sexual assaults are collected and used in investigations of perpetrators; however, the data is not maintained in searchable databases or shared across jurisdictions. This should apply to data from children where they might be collected for investigations of human trafficking.

SUMMARY

With this submission of comments, our intention is to bring to your attention important matters of procedure and substance that DHS has not adequately addressed in the proposed rules for Collection and Use of Biometrics by U.S. Citizenship and Immigration Services. While we have been able to emphasize several distinct aspects that require further attention (and, notably, both congressional and public deliberation to resolve), the extraordinarily short comment period prevented us from providing comprehensive analysis detailing all of our concerns. Nevertheless, we hope that these comments provide a compelling case that prompts DHS to reconsider this proposal and provide future meaningful opportunity for the public and relevant interdisciplinary experts to be engaged in the policymaking process so that we can ensure that any biometric program designed and deployed is on sound technical, ethical, and legal footing.

Sincerely,

Dan Berger, JD
Partner, Curran Berger & Kludt LLC
Honorary Fellow, American Academy of Adoption and Assisted Reproduction Attorneys

Sara H. Katsanis, MS
Research Assistant Professor
Northwestern University Feinberg School of Medicine
Ann & Robert H. Lurie Children's Hospital of Chicago

Margaret Hu, JD
Professor of Law and International Affairs
Penn State Law and School of International Affairs
Institute for Computational and Data Sciences
The Pennsylvania State University

Jennifer K. Wagner, JD, PhD
Assistant Professor
Center for Translational Bioethics & Health Care Policy
Geisinger

The comments herein are our own and not reflections of our professional affiliations.

The authors thank Elliot Caron-Vera, Diana Madden, and Justine Sheehan for their considerable assistance with the preparation of these comments.

[72] *Supra* note 66