ELECTRONIC FRONTIER FOUNDATION

COMMENTS OF THE

ELECTRONIC FRONTIER FOUNDATION

REGARDING NOTICE OF PROPOSED RULEMAKING ON THE

COLLECTION AND USE OF BIOMETRICS BY

U.S. CITIZENSHIP AND IMMIGRATION SERVICES

USCIS Docket No. USCIS–2019–0007

85 Fed. Reg. 56338

Submitted on October 13, 2020 to the Department of Homeland Security

INTRODUCTION

The Electronic Frontier Foundation ("EFF") submits the following comments to urge the U.S. Department of Homeland Security ("DHS") to withdraw its Notice of Proposed Rulemaking ("NPRM" or "Proposed Rule"), published at Docket Number USCIS-2019-0007. This proposal, which would drastically expand U.S. Citizenship and Immigration Service's ("USCIS") collection of biometric information in routine immigration applications, threatens the privacy and security of U.S. citizens and non-citizens and should not be implemented.[1]

EFF is a non-profit organization that has worked for 30 years to protect civil liberties, privacy, consumer interests, and innovation in new technologies. EFF actively encourages and challenges the executive and judiciary to support privacy and safeguard individual rights as emerging technologies become more prevalent in society. With more than 30,000 contributing members, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment.

[1] EFF strongly objects to the manner in which DHS rolled out this NPRM. Despite the NPRM's sweeping changes to dozens of federal regulations that implicate the privacy interests of millions of U.S. citizens and non-citizens, DHS only provided the public 30 days to comment on it. Under ordinary circumstances, 30 days would still be well short of the standard 60-day comment period federal agencies generally provide. *See* Exec. Order No. 13563, 3 C.F.R. 215 (2011). But in light of the COVID-19 pandemic that has forced EFF and many others to work remotely under challenging conditions and has restricted the public's ability to engage with the government, the allotted comment period is inadequate. Moreover, given that DHS has been contemplating an expansion of its biometrics collection practices for over a decade, and that this NPRM constitutes 85 pages in the Federal Register, the public deserved more than 30 days to respond. *See, e.g.*, U.S. Citizenship and Immigr. Servs., *Senior Policy Counsel Paper: Expanding DNA Testing in the Immigration Process*, *available at* https://www.eff.org/document/uscis-senior-policy-council%E2%80%94dna-collection-options-paper (records obtained through FOIA discussing USCIS plans in 2009 to update federal regulations to expand DNA collection). Finally, DHS's rollout of the comment period has been marked by errors and confusion. On October 12, the Federal Register's portal to submit comments stated that the comment period would end on that same day at 11:59 pm ET, despite the NPRM providing a deadline of October 13. Later that evening, the portal provided a new deadline of November 12, signaling a 30-day extension. After EFF and other organizations' repeated attempts to reach out to DHS, a DHS official ultimately stated that the new deadline was in error and that comments were in fact due on October 13. These ever-changing deadlines constructively deny many members of the public from providing meaningful input.

EFF is joined in these comments by the following organizations:

- The Center on Privacy & Technology at Georgetown Law
- Immigrant Legal Resource Center
- National Hispanic Media Coalition
- National Immigration Law Center
- New America's Open Technology Institute
- Open Society Justice Initiative
- Open The Government
- Restore The Fourth

TABLE OF CONTENTS

I. USCIS's Proposed Rule Would Drastically Expand DHS's Biometric Surveillance of U.S. Citizens and Non-Citizens

DHS's existing biometrics database is the largest in the federal government, the second largest in the world,[2] and already contains biometric data from more than 260 million people.[3] The Proposed Rule would increase the number of people required to submit biometrics by, at minimum, 2.17 million people per year,[4] adding millions of new biometric submissions on top of the more than 20 million biometric submissions DHS currently adds each year.[5]

Under the current regime, for certain but not all routine immigration applications, DHS requires applicants to submit fingerprints, photographs, or signatures.[6] The NPRM would drastically alter this model. The NPRM would considerably expand the populations that are required to submit biometrics, most notably by including children under the age of 14 for the first time and by sweeping in large pools of U.S. citizens and lawful permanent residents ("LPRs"). It would significantly expand the types of biometric information that immigration applicants are required to submit. In addition, for the first time, it would mandate the submission of DNA samples for immigration benefits from both U.S. citizens and non-citizens. And perhaps most significantly, the NPRM would expand how biometrics are used, implementing a system of persistent and frequent biometric surveillance of U.S. citizens and immigrants.

A. The Proposed Rule Would Expand the Population Required to Submit Biometrics

Under the current governing regime, DHS treats biometrics as "only mandatory for certain benefit requests and enforcement actions."[7] Accordingly, "there are substantial populations associated with immigration benefit requests that do not routinely submit biometrics."[8] The NPRM, by contrast, would create "a system under which biometrics are required for *any* immigration benefit request unless DHS determines that biometrics are unnecessary,"[9] expanding the number of people required to submit biometrics to

[2] Chris Burt, *Inside the HART of the DHS Office of Biometric Identity Management*, Biometric Update (Sept. 4, 2018), https://www.biometricupdate.com/201809/inside-the-hart-of-the-dhs-office-of-biometric-identity-management.

[3] Dep't of Homeland Sec., Biometrics, https://www.dhs.gov/biometrics (last visited Oct. 12, 2020).

[4] *Collection and Use of Biometrics by U.S. Citizenship and Immigration Services*, 85 Fed. Reg. 56338, 56364 (proposed Sept. 11, 2020).

[5] Dep't of Homeland Sec., *supra* n.3.

[6] 85 Fed. Reg. at 56350.

[7] *Id.* at 56340.

[8] *Id.* at 56368.

[9] *Id.* at 56350–51 (emphasis added).

USCIS each year to at least 6.07 million.[10] The number of people that could be required to submit a DNA sample would rise from zero to an estimated 805,493 each year.[11] Of those, approximately 336,650 would be U.S. citizens.[12]

This means that mandatory biometrics collection from U.S. citizens and LPRs will expand significantly. Presently, DHS only requires biometrics from U.S. citizens and LPRs for applications involving adoptions.[13] The NPRM would require the biometric collection from any U.S. citizen or LPR who sponsors a family member for an immigration application, such as a family-based visa petition.[14]

Additionally, the NPRM would amend existing regulations to require biometrics collection from children under the age of 14. The current regime does not allow DHS to collect biometrics from children.[15] The NPRM would "remov[e] the age restrictions for biometric collection writ large."[16]

B. The Proposed Rule Would Expand the Types of Biometrics DHS Routinely Collects

As noted above, for routine immigration applications, DHS currently requires only photographs, fingerprints and signatures.[17] The NPRM would significantly expand the types of biometrics DHS collects.[18] The NPRM would make this change by formally defining biometrics as "the measurable biological (anatomical and physiological) or behavioral characteristics used for identification of an individual."[19] Specifically, the proposal would add palm prints, photographs "including facial images specifically for facial recognition, as well as photographs of physical or anatomical features such as scars, skin marks, and tattoos," voice prints, iris images, and DNA to the types of biometrics that DHS may require.[20] Additionally, while not mentioned explicitly, the use of the term "behavioral characteristics" in the proposed definition clearly contemplates the future inclusion of so-called behavioral biometrics which can identify a person

[10] *Id.* at 56343.
[11] *Id.* at 56380. DHS notes that it "currently accepts DNA test results for 11,383 beneficiaries" each year. *Id.* at 56373. However, none of these submissions are mandatory.
[12] *Id.* at 56380.
[13] *Id.* at 56358.
[14] *Id.* at 56342.
[15] *Id.* at 56356.
[16] *Id.* at 56357.
[17] *Id.* at 56350.
[18] *Id.* at 56355.
[19] *Id.* (citing proposed 8 C.F.R. pt. 1.2).
[20] *Id.*

through the analysis of their movements.[21]

As discussed in depth below, the required submission of DNA evidence is an especially significant change because of the serious privacy risks inherent in collecting DNA. Under the current regime, for certain family-based applications, DHS gives petitioners the option of voluntarily submitting DNA in order to verify a claimed genetic relationship if documentary evidence, such as birth and marriage certificates, cannot do so.[22] Under the NPRM, DHS may *require* petitioners to submit DNA in order to prove a genetic relationship. This DNA sample would be used to produce a partial DNA profile, which DHS may store or share, along with DNA test results, with other law enforcement agencies.[23]

C. The Proposed Rule Would Fundamentally Alter the Way in Which DHS Uses Biometrics

For immigration-related applications, DHS currently is required to confirm an individual's identity and then determine if a person's past record makes them ineligible for certain benefits. To make those determinations, DHS has a wide range of resources available to it. DHS can review an applicant's immigration history, which consists of their "current immigration status, current immigration filings, past immigration filings, and whether previous benefits were granted or denied."[24] In addition, DHS capabilities include, but are not limited to, name-based checks, checks that match fingerprints with the FBI's databases, and "biometrics checks" that match petitioner's biometrics with databases maintained by DHS,[25] the FBI, the Department of Defense, and foreign governments.[26] Under the current regime, DHS claims the authority to store biometrics and use them to "verify an individual's identity in subsequent encounters with DHS," including with "law enforcement components" such as U.S. Immigration and Customs

[21] *See* Jennifer Lynch, Immigration Policy Center & Electronic Frontier Foundation, From Fingerprints to DNA, 4 (2012), https://www.eff.org/document/fingerprints-dna-biometric-data-collection-us-immigrant-communities-and-beyond.
[22] 85 Fed. Reg at 56350, 56353.
[23] *Id.* at 56353.
[24] *Id.* at 56352.
[25] The NPRM states that its expanded biometrics collection will ultimately populate its HART database. *Id.* at 56352. EFF has previously objected to DHS's failure to include important privacy protections in the development of that system. *See* Jennifer Lynch, *HART: Homeland Security's Massive New Database Will Include Face Recognition, DNA, and Peoples' "Non-Obvious Relationships,"* EFF Deeplinks Blog (June 7, 2018), https://www.eff.org/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and.
[26] 85 Fed. Reg. at 56349.

Enforcement ("ICE").[27]

The NPRM would again mark a major shift from past practice. The NPRM makes clear that a core goal of DHS's expansion of biometrics collection would be to implement "enhanced and continuous vetting," which would require immigrants "be subjected to continued and subsequent evaluation to ensure they continue to present no risk of causing harm subsequent to their entry."[28] While the NPRM offers few details about what such a program would entail, it appears that DHS would collect biometric data as part of routine immigration applications in order to share that data with law enforcement and monitor individuals indefinitely. Additionally, the NPRM would require that U.S. citizens and LPRs submit biometrics if DHS decides to re-open their past applications, or if "the previous approval is relevant to an application, petition, or benefit request currently pending with USCIS." [29] The Proposed Rule claims authority for such "enhanced and continuous vetting" through Executive Order 13780, which also banned nationals of Iran, Libya, Somalia, Sudan, Syria, and Yemen from entering the United States.[30]

This, in essence, creates two classes of U.S. citizens: those born on U.S. soil and those who are naturalized and therefore subject to the threat of ongoing biometrics collection and continued re-evaluation of their citizenship status. This is especially alarming amid the increased number of denaturalizations under this administration:[31] out of the 228 denaturalization cases filed since 2008, over 40 percent have been filed since 2017.[32] Earlier this year, the Trump administration signaled its intent to ramp up such cases by establishing an official section within the Department of Justice's immigration office tasked with denaturalization efforts.[33]

[27] *Id.* at 56349.

[28] *Id.* at 56350, 56340.

[29] *Id.* at 56352 (citing proposed 8 C.F.R. pt. 103.16).

[30] Executive Order Protecting the Nation from Foreign Terrorist Entry into the United States, E.O. 13780 (Mar. 6, 2017).

[31] *See generally* Laura Bingham, Open Society Justice Initiative, Unmaking Americans: Insecure Citizenship in the United States 42–108 (2019), https://www.justiceinitiative.org/uploads/e05c542e-0db4-40cc-a3ed-2d73abcfd37f/unmaking-americans-insecure-citizenship-in-the-united-states-report-20190916.pdf.

[32] Katie Benner, *Justice Dept. Establishes Office to Denaturalize Immigrants*, N.Y. Times (Feb. 26, 2020), https://www.nytimes.com/2020/02/26/us/politics/denaturalization-immigrants-justice-department.html.

[33] *Id.*

II. The Proposed Rule's Expansion of Biometric Collection Poses Grave Threats to Privacy and Security

DHS fails to recognize—let alone address—the severe privacy and security implications of the NPRM's proposed massive expansion of biometrics collection. It has not demonstrated that this expansion is necessary or proportionate to the problems it claims it is trying to address or the goals it is trying to achieve.[34] Nor, in putting forward this NPRM, has it complied with Fair Information Practice Principles, which DHS has described as the "foundational principles for privacy policy and implementation" and necessary for "assuring that the use of technologies sustains and does not erode, privacy protections relating to the use, collection, and disclosure of personal information."[35] This Proposed Rule appears to be the first step in DHS's plan to drastically increase the biometric modalities it will collect from each person in the future—a plan that has serious ramifications for immigrants and U.S. persons alike.

A. The Proposed Rule Fails to Take Account of the Reality That Collection of Biometric Information Can Reveal Deeply Private Information Beyond Mere Identity

DHS fails to acknowledge that its Proposed Rule not only expands the population of people whose privacy is threatened, but also, contrary to DHS's assertions, creates unique new threats to privacy as well.[36]

1. <u>DHS's Proposed Definition of "Biometrics" Would Allow for Unlimited Data Collection Going Forward</u>

The NPRM proposes an extremely broad definition of "biometrics." *See supra* Part I.B. This definition allows for virtually unbounded biometrics collection in the future, creating untold threats to privacy and personal autonomy.

[34] *See* Access et. al, Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance (2014), https://necessaryandproportionate.org/files/en_principles_2014.pdf.

[35] Memorandum from Hugo Teufel III, Chief Privacy Officer, Dep't of Homeland Sec., The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (Dec. 29, 2008), https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

[36] 85 Fed. Reg. at 56414.

Not only will the Proposed Rule allow DHS to collect already controversial biometrics like facial images and tattoos,[37] it would explicitly allow DHS to collect "behavioral" biometrics, including voice prints. Unlike traditional biometrics, which are static physical characteristics that are unique to each person, behavioral biometrics are based on dynamic patterns in a person's behavior, such as how a person moves or types. By explicitly referencing behavioral characteristics in its definition of biometrics, DHS leaves the door open for the agency to collect information on how a person walks, their keystrokes when typing, their heartbeat,[38] their geolocation and navigational patterns, and other patterns of behavior.[39] Like face recognition, these biometrics are much more invasive to privacy because they can be collected and used without a person's knowledge. That means individuals may not even know what data has been collected on them, who has access to it, and how and when it may be used in the future.

Behavioral biometrics expose highly personal and sensitive information about a person beyond mere identity and allow for tracking on a mass scale. China recently began using gait recognition to track people in circumstances when face recognition is not available, such as when a person's face is covered or when they are walking away from a camera.[40] When gait recognition is used in combination with face recognition, it allows governments to track people throughout their lives, revealing not only a person's "particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (citing *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). As the U.S. Supreme Court recognized in *Carpenter*, information like this "hold[s] for many Americans the privacies of life." *Id.* (internal quotations omitted).

Notably, the Proposed Rule would allow DHS components to change their own biometric rules without further public engagement in a notice-and-comment rulemaking process. The NPRM contemplates DHS components "may expand or contract their biometric submission requirements" in the future simply by updating their forms.[41]

[37] *See* Electronic Frontier Foundation, *Face Recognition*, https://www.eff.org/pages/face-recognition (last visited Oct. 13, 2020); Electronic Frontier Foundation, *Tattoo Recognition*, https://www.eff.org/pages/tattoo-recognition (last visited Oct. 13, 2020).

[38] *See People can now be identified at a distance by their heartbeat*, The Economist (Jan. 23, 2020), https://www.economist.com/science-and-technology/2020/01/23/people-can-now-be-identified-at-a-distance-by-their-heartbeat.

[39] *See generally* South by Southwest, *I Know Where You're Going*, https://schedule.sxsw.com/2013/events/event_IAP3353.

[40] *See* Michael Grothaus, *China is now using gait recognition to identify people*, Fast Company (Nov. 7, 2018), https://www.fastcompany.com/90263855/china-is-now-using-gait-recognition-to-identify-people.

[41] 85 Fed. Reg. at 56343.

Should the agency finalize the Proposed Rule and allow for this vast expansion of biometrics collection, the United States will have started on a path to state surveillance of minority populations, similar to programs in other countries that many U.S. government officials have harshly criticized. For example, in July 2020, the U.S. House of Representatives passed a bipartisan amendment to the National Defense Authorization Act that would explicitly restrict exports of face recognition and other biometric technologies to China because of the country's use of these surveillance technologies on the Uyghur Muslim minority population.[42] This was prompted by news of U.S. companies such as Amazon, Microsoft, IBM, Intel, Thermo Fisher Scientific, and Hewlett Packard exporting such goods and services to Chinese security agencies and Chinese companies involved in domestic surveillance.[43] In 2018, Senator Marco Rubio wrote a letter to Thermo Fisher Scientific's CEO raising concerns about the company supplying Xinjiang police with DNA sequencers.[44] Citing to a Human Rights Watch report about the Chinese government subjecting the Uyghur population to "DNA samples, fingerprints, iris scans and blood types," Senator Rubio stated that such retention of sensitive biometrics "has understandably raised alarm bells among rights advocates."[45] Later in 2018, Senator Rubio led a bipartisan group of Senate and House members to urge Secretary of State Mike Pompeo and Treasury Secretary Steven Mnuchin to impose sanctions on China and its government officials for "creating a high-tech police state in the [Xinjiang region] that is both a gross violation of privacy and international human rights."[46] The letter also urged sanctions against Chinese companies assisting with "surveillance of ethnic minorities."[47] As noted, the biometrics China currently collects from Uyghurs include fingerprints, voice, face, iris, palm, and DNA, including DNA to track familial relationships[48]—many of the same biometrics DHS

[42] Office of Congressman Tom Malinowski, *House Passes Rep Malinowski's Provision Barring Exports to China That Can Be Used to Violate Human Rights* (July 21, 2020), https://malinowski.house.gov/media/press-releases/house-passes-rep-malinowski-s-provision-barring-exports-china-can-be-used.

[43] *Id.*

[44] Letter from Sen. Marco Rubio to Marc Casper, CEO of Thermo Fisher Scientific (Feb. 8, 2018), https://www.rubio.senate.gov/public/_cache/files/ebde2746-ee3b-4263-8a7a-3e2eb50e67c8/0A83328093F8842D707C67D035C6C0B2.2-8-18-letter-to-ceo-casper-re-thermo-fisher-scientific.pdf.

[45] *Id.*

[46] Letter from Sen. Marco Rubio, et al., to Mike Pompeo, Secretary of State, and Steven T. Mnuchin, Secretary of the Treasury (Aug. 28, 2018), https://www.rubio.senate.gov/public/_cache/files/80388428-6d33-402a-880f-f9bd15a91f85/3E2543611C2CF8754F4257AB6A2913ED.pompeo-mnuchin-xinjiangletter.pdf.

[47] *Id.*

[48] *See* Dylan Byler, *China's hi-tech war on its Muslim minority*, The Guardian (Apr. 11, 2019),

proposes to collect from immigrants and U.S. persons with this Proposed Rule.

2. The Biometrics DHS Plans to Collect Will Be Combined with Other Sensitive Information about Individuals and Shared Broadly

Although the NPRM focuses solely on the collection of biometric data, that collection does not occur in a vacuum. DHS combines biometric data in its Homeland Advanced Recognition Technology ("HART") database[49] with other data that creates a detailed picture of a person's life. This includes biographic data—like name, date of birth, physical descriptors, country of origin, and government ID numbers—and also less defined information such as "miscellaneous officer comment information" and "encounter data, including location and circumstance of each instance resulting in biometric collection."[50] The system will also include data that tracks relationships among individuals and data from "publicly available sources,"[51] which likely will include social media sites, given that DHS now collects social media data from "all refugee and asylum seekers, as well as individuals who are already in the country and working to adjust their status."[52] Other data collected by DHS components, which may be combined with or at

https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition; Sui-Lee Wee, *China is Collecting DNA From Tens of Millions of Men and Boys, Using U.S. Equipment*, N.Y. Times (June 17, 2020), https://www.nytimes.com/2020/06/17/world/asia/China-DNA-surveillance.html.

[49] *See* 85 Fed. Reg. at 56349 n.21. DHS's new HART database will store all of the data covered by the NPRM.

[50] Dep't of Homeland Sec, Homeland Advanced Recognition Technology System (HART) Increment 1 PIA DHS/OBIM/PIA-004 16 (Feb. 24, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf. This PIA was not uploaded to website until May 2020 despite being dated Feb. 24, 2020.

[51] *Id.* at 18.

[52] *See* Brandi Vincent, *DHS Plans to Expand Social Media Collection on Refugees and Immigrants*, Nextgov (Sept. 5, 2020), https://www.nextgov.com/emerging-tech/2019/09/dhs-plans-expand-social-media-collection-refugees-and-immigrants/159669/; *see also* Dep't of Homeland Sec., Privacy Impact Assessment for the Publicly Available Social Media Monitoring and Situational Awareness Initiative DHS/CBP/PIA-058 (Mar. 25, 2019), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp58-socialmedia-march2019.pdf. Over two dozen civil liberties, privacy, and immigrant rights organizations, signed onto comments drafted by the Brennan Center for Justice, ACLU, Center for Democracy and Technology, and Electronic Privacy Information Center opposing DHS's proposed rule on the collection of social media identifiers. Letter from ACLU et al., to Dep't of Homeland Sec. (Nov. 4, 2019),

least linked to biometric data, includes "information gathered at every crossing: the time, date and port of the crossing, the information taken from their travel documents, photos and data collected on their belongings and vehicles, [] determinations made by customs officers throughout the process," and the license plate of any vehicle driven across the border.[53] ICE has also indicated its interest in accessing geolocation data that could "pinpoint the exact locations of cellphones, laptops and other connected devices—even going back in time" up to two years.[54]

Some of this biometric and biographic data will come from the world's most vulnerable populations—refugees and asylum seekers—many of whom will never set foot in the United States.[55] According to data from the United Nations High Commissioner for Refugees, "less than a quarter of the nearly 85,000 cases reviewed by USCIS in 2018 resulted in the refugee being approved for admission to the U.S."[56] Nevertheless, the federal government retains the biometric data collected from all resettlement applicants.

DHS shares data like this broadly with other federal, state, local, and tribal agencies as well as with foreign governments and contractors. DHS recognizes that "[t]here is a potential risk that sensitive data may be shared with groups not authorized to receive the data" and that that risk can only be partially mitigated.[57] Records from people in special protected classes, including "T, U, and VAWA nonimmigrants, Asylee and Refuges, and Temporary Protected Status" are entitled to "special confidentiality through statute, regulation, or DHS policy"[58] but there is nothing in the structure of the HART database to prevent unauthorized access to their data. And in fact, even if DHS wanted to make only certain biometrics available to other agencies accessing HART, the database

https://www.brennancenter.org/sites/default/files/2019-11/DHS%20SMM%20comments%20-%20FINAL.pdf.

[53] Aaron Boyd, *An Inside Look at All the Data CBP Collects About Everyone Crossing U.S. Borders*, Nextgov (Sept. 18, 2019), https://www.nextgov.com/emerging-tech/2019/09/inside-look-all-data-cbp-collects-about-everyone-crossing-us-borders/159946/.

[54] Aaron Boyd, *ICE Seeks Tech To Track Electronic Devices—Even Through Time*, Nextgov (May 21, 2019), https://www.nextgov.com/emerging-tech/2019/05/ice-seeks-tech-track-electronic-deviceseven-through-time/157172/.

[55] Jack Corrigan, *DHS is Collecting Biometrics on Thousands of Refugees Who Will Never Enter the U.S.*, Nextgov (Aug. 20, 2019), https://www.nextgov.com/emerging-tech/2019/08/dhs-collecting-biometrics-thousands-refugees-who-will-never-enter-us/159310/.

[56] *Id.*

[57] Dep't of Homeland Sec., *supra* n.50, at 31.

[58] *Id.* at 31–32 n.57.

cannot filter by individual biometric modality.[59] This means that database users will be able to access *all* biometrics linked to any individual within HART. There is also a recognized risk that this data could be shared with the very countries that people are trying to escape. As DHS acknowledges, it shares much of its data with foreign partners, and "it is more difficult for DHS to externally impose the same controls that govern the data internally."[60] This threat to privacy increases exponentially as more data, and especially biometric data, is collected on each individual.

Given the biographic and other data DHS currently collects, the data it ingests from outside partners, and the additional biometrics DHS proposes to collect by this rulemaking,[61] the scope of DHS's data collection appears unlimited. Aggregating this data and making it broadly accessible only increases the threats to individuals' privacy.

3. DNA Collection Presents Unique Threats to Privacy

With the NPRM, DHS seeks to extend its regulatory authority to mandate DNA collection "for any benefit request where [a genetic] relationship must be established."[62] DHS would apply this rule to prospective immigrants and U.S. persons (both citizens and LPRs) alike and may, at its own discretion, share "DNA test results" and DNA profiles with other agencies, including law enforcement agencies.[63]

Along with other programs that the Trump administration has implemented—such as Rapid DNA testing of family units at the border[64] and collection of fingerprints from all adults in households seeking to care for unaccompanied minors[65]—the proposed rule demonstrates a push toward normalizing biometric collection from immigrants based on unsubstantiated accounts of widespread "family unit fraud" and specious notions of public safety.[66] By vastly expanding the amount of DNA collected and added to national

[59] *See id.* at 33.

[60] *Id.* at 32.

[61] *Id.* at 28.

[62] 85 Fed. Reg. at 56343.

[63] *Id.* at 56353; *see also* proposed 8 C.F.R. pt. 103.16(e).

[64] Priscilla Alvarez & Geneva Sands, *Exclusive: DHS to start DNA testing to establish family relationships on the border*, CNN (May 1, 2019), https://www.cnn.com/2019/04/30/politics/homeland-security-dna-testing-immigration/index.html.

[65] Joshua Barajas, *What changes to this fingerprinting rule could mean for migrant children in U.S. custody*, PBS (Dec. 19. 2018), https://www.pbs.org/newshour/nation/what-changes-to-this-fingerprinting-rule-could-mean-for-migrant-children-in-u-s-custody.

[66] Studies have repeatedly demonstrated no correlation between immigrants and criminality. *See, e.g.*, Anna Flagg, *Is There a Connection Between Undocumented Immigrants and Crime?*, Marshall Project (May 13, 2019),

DNA databases based on status rather than conduct, the proposed rule brings us closer to a regime of DNA collection from the entire population. Further, by allowing the agency to collect and retain DNA profiles that identify genetic familial relationships, the Proposed Rule violates not just individuals' privacy interests, but the privacy interests of whole communities and potentially whole generations of current and former immigrants within and outside the United States.

(a) *DNA Can Reveal More Sensitive and Private Information Than Other Biometrics*

DNA contains our most private and personal information. 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."[67] 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, and even, allegedly, the propensity to engage in violent or criminal behavior."[68] Although DHS states that it does not plan to retain DNA samples,[69] it must take custody of each person's DNA sample to extract a DNA profile. DHS also leaves open the possibility it *will* retain and share "raw DNA" if it is "required to share by law."[70] For these reasons, DHS must take account of the privacy issues and security risks inherent in mass DNA *sample* collection, not just collection of DNA profiles. DHS fails to discuss, much less address, these privacy and security issues in the NPRM.

DHS also fails to fully acknowledge and address the privacy threats from collecting DNA profiles. DHS describes the profile it plans to extract from a DNA sample as "actually a very small portion of an individual's full characteristics."[71]

https://www.themarshallproject.org/2019/05/13/is-there-a-connection-between-undocumented-immigrants-and-crime; Michael T. Light & Ty Miller, *Does Undocumented Immigration Increase Violent Crime?*, 56:2 Criminology 370 (May 2018), https://onlinelibrary.wiley.com/doi/abs/10.1111/1745-9125.12175; Walter Ewing et al., The Criminalization of Immigration in the United States, American Immigration Council (July 13, 2015), https://www.americanimmigrationcouncil.org/research/criminalization-immigration-united-states.

[67] *State v. Medina*, 102 A.3d 661, 682 (Vt. 2014) (citations omitted).

[68] *People v. Buza*, 413 P.3d 1132, 1173 (Cal. 2018) (Cuéllar, J., dissenting) (citations omitted).

[69] 85 Fed. Reg. at 56353 ("DHS will not store or share any raw DNA or biological samples, other than to the extent necessary to facilitate the DNA testing[.]")

[70] *Id.* at 56354.

[71] *Id.* at 56353.

However, one study—conducted when the FBI's Combined DNA Index System ("CODIS") database relied on 13 loci, rather than the 20 loci it now includes—found that the short tandem repeat ("STR") profiles in CODIS can identify information about individuals' ancestry, which may, in turn, be used to reveal information about their phenotypic traits (i.e., physical appearance) based on assumptions about race and ethnicity.[72] Another recent study suggested that the profiles maintained in CODIS can now be matched to single-nucleotide polymorphism ("SNP") profiles in other publicly accessible databases, which include intimate details like "precise ancestry estimates, health and identification information."[73] This study's findings suggest that DNA profiles stored in government databases could be used to identify anonymized genomes from health-research databases or other sources.[74]

Data aggregation—combining genetic profiles with other government-maintained or publicly available data—increases these privacy risks. In the NPRM, DHS proposes to store DNA information in an immigrant's "A-file," along with all other biometric and biographic information collected on that person, making DNA data and relationship information easily accessible to other users of the database.[75] It is unclear where DHS plans to store DNA data collected from U.S. citizens and nonimmigrants, but DHS states in the NPRM that it wants to transition to a "person-centric model for organizing and managing its records,"[76] indicating it will store DNA data with all other information collected on the individual. These plans to store DNA with other government-collected data clearly violate the federal government's own established practices on DNA data management. The FBI's CODIS database does not store any names or personal identifiers with the DNA profiles, and the FBI keeps DNA separate from other biometric data in its Next Generation Identification database.[77]

[72] Bridget Algee-Hewitt et al., *Individual Identifiability Predicts Population Identifiability in Forensic Microsatellite Markers*, Current Biology (Mar. 17, 2016), https://doi.org/10.1016/j.cub.2016.01.065.

[73] Michael D. Edge et al., *Linkage disequilibrium matches forensic genetic records to disjoint genomic marker sets*, Proceedings of the National Academy of Sciences (May 15, 2017), https://doi.org/10.1073/pnas.1619944114 (finding that the STR profiles maintained in CODIS can be matched to SNP profiles).

[74] Lindzi Wessel, *Scientists concerned over US plans to collect DNA data from immigrants*, Nature (Oct. 7, 2019), https://www.nature.com/articles/d41586-019-02998-3.

[75] 85 Fed. Reg. at 56354.

[76] *Id.* at 56347.

[77] *See* FBI, *Frequently Asked Questions on CODIS and NDIS*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last accessed Oct. 12, 2020) ("No names or other personal identifiers of the offenders, arrestees, or detainees are stored using the CODIS software.").

Further, unlike the FBI's public disclosures about the CODIS database and loci collected,[78] DHS fails to specify the precise alleles it plans to extract, stating only that "at present, DHS relationship tests profile between 16 and 24 genetic markers."[79] By failing to provide this information in the NPRM, DHS prevents scientists and the general public from fully assessing the privacy risks attendant to DHS's DNA profile collection.

(b) *DHS's Proposed DNA Collection Not Only Threatens Individual Privacy Interests, It Threatens the Privacy Interests of Whole Communities*

DHS further compounds these threats to individual privacy and autonomy by intentionally collecting and maintaining information on genetic familial relationships and sharing that information with other law enforcement agencies.

DHS states repeatedly that it plans to collect, retain, and share "partial DNA profile[s],"[80] but it never defines in the Proposed Rule what it believes to be a "partial DNA profile."[81] DHS may intend by this term to mean it stores data on genetic familial relationships along with each individual's profile. In that case, DHS would be building a familial DNA database with no public debate and no congressional oversight. This violates privacy, autonomy, and societal norms. Even the FBI has disclaimed association with familial searching,[82] and the handful of states that expressly allow for familial searches of their criminal DNA data only use this technique in unsolved criminal investigations where the "crime at issue is serious and has critical public safety implications."[83] Law enforcement's familial searches of DNA databases has also been hotly debated within the American public, with many people choosing to opt-out of these

[78] *Id.* (noting in question #19 the loci collected).

[79] 85 Fed. Reg. at 56353.

[80] *See, e.g.*, *id.* at 56341.

[81] There is no accepted definition of this term in the scientific literature except perhaps to refer to a forensic sample that is so degraded as to only be able to generate a "partial profile." *See, e.g.*, Naomi Elster**,** *How Forensic DNA Evidence Can Lead to Wrongful Convictions*, JSTOR Daily (Dec. 6, 2017), https://daily.jstor.org/forensic-dna-evidence-can-lead-wrongful-convictions/ (noting how partial profiles can lead to wrongful convictions). The FBI and many others frequently use the term "partial match" to describe "a moderate stringency candidate match between two single source profiles having at each locus all of the alleles of one sample represented in the other sample." *See* FBI, *supra* n.77. However, this describes the process, not the resulting DNA profiles.

[82] *See* FBI, *supra* n.77(noting "familial searching is not currently performed at NDIS.").

[83] *See, e.g.*, California Dep't of Justice DNA Data Bank Program, Memorandum of Understanding Familial Searching Protocol,
https://oag.ca.gov/sites/all/files/agweb/pdfs/bfs/fsc-mou-06142011.pdf?.

searches where they can.[84]

Yet DHS's Proposed Rule appears to make familial DNA searches accessible to any agency or user who has access to the database and a law enforcement- or immigration-related need. If DHS is allowed to proceed with collecting genetic relationship data from immigrants and U.S. persons, in the near future, it will be able to map whole generations of family members, and by extension, whole immigrant communities.

(c) *Government-Mandated DNA Collection Links Immigration with Criminality and Puts Innocent People at Risk of Being Accused of Crimes They Did Not Commit*

The Proposed Rule further erodes civil liberties by basing DNA collection solely on an individual's immigration status or an LPR or U.S. citizen's desire to—legally—bring family members to the United States. In *Maryland v. King*, the Supreme Court upheld government-mandated DNA collection from certain classes of arrestees, holding that a DNA swab did not violate the arrestee's expectation of privacy "[i]n light of the context of a valid arrest supported by probable cause."[85] However, for immigrants, LPRs, and U.S. citizens covered by the NPRM, there is neither a valid arrest nor probable cause that the individual has committed a crime. Despite this, the Proposed Rule will link immigrants and U.S. citizens with crime because the data may be stored and shared with other law enforcement agencies.[86]

This could put U.S. citizens and non-citizens at risk of being identified for a crime they did not commit, merely because their DNA already exists in a government database. The sensitivity of forensic DNA collection has improved exponentially over the last few decades, and forensic investigators are now able to detect, collect, and analyze trace amounts of DNA at a crime scene. Because a person can shed as many as 50 million skin cells a day, DNA may be found not only on items that a person has touched,[87] but also on other items with which the person never came into contact—a phenomenon known as "secondary transfer."[88] Crime scene samples may also contain genetic material from more than one person and could even contain DNA from someone who was never at the

[84] Heather Murphy, *Why a Data Breach at a Genealogy Site Has Privacy Experts Worried*, N.Y. Times (Aug. 1, 2020), https://www.nytimes.com/2020/08/01/technology/gedmatch-breach-privacy.html.

[85] 569 U.S. at 465 (2013).

[86] 85 Fed. Reg. at 56353 ("DHS may store or share DNA test results . . . with other law enforcement agencies"); *see also* proposed 8 C.F.R. pt. 103.16(e).

[87] Katie Worth, *Framed for Murder by His Own DNA*, Wired (Apr. 18, 2019), https://www.wired.com/story/dna-transfer-framed-murder/.

[88] *Id.*

crime scene. In California, a man spent five months in jail after a database search linked his DNA to DNA found on the fingernails of a murder victim—although he was in the hospital when the murder occurred.[89] Prosecutors believe paramedics may have transferred his DNA to the murder victim when they responded to the crime scene hours after dropping him off at the hospital.[90] He never would have been linked to the crime if his DNA had not already existed in a government database. Given this, researchers have recognized, "[a] DNA hit does not show that the subject is the offender and there are many reasons why the DNA of an individual may be found at a crime scene."[91] Nevertheless, this has not stopped prosecutors from arresting someone solely based on a DNA hit.

Collection of DNA and the extraction of DNA profiles will undoubtedly exacerbate racial disparities that are already present in existing DNA databases. In 2011, it was estimated that Black individuals made up 40 percent of profiles in the FBI's CODIS database, and that it was "possible to use the database to identify up to 17 percent of the country's entire African-American population."[92] The Proposed Rule cannot even estimate the number of immigrants and their U.S.-based family members it will collect DNA from; however, collection of these DNA profiles will undoubtedly skew the racial disparities of DNA collection, by disproportionately impacting people of color, and thus subjecting them to more risk of being identified for a crime they did not commit.

U.S. citizens, LPRs, immigrants, and others should not be put at risk of being linked to a crime solely because they desire to begin a new life in, or bring a loved one to, the United States. USCIS has, for years, managed this process without mass, mandated DNA collection, and it has not shown the goals it is trying to achieve with DNA collection now outweigh the very serious threats to privacy and autonomy.

B. The NPRM Fails to Adequately Address the Security Risks of Collection and Storage of Over 6 Million People's Biometric Data Annually

The massive expansion of biometrics collection necessarily leads to a significant increase in attendant security risks. Unlike a Social Security number or a driver's license, a biometric is permanent, unique, and cannot be changed. The NPRM allows for nearly indefinite retention of biometrics, creating the possibility of breach or data misuse well

[89] Henry Lee, *How Innocent Man's DNA Was Found at Killing Scene*, SF Gate (June 26, 2013), http://www.sfgate.com/crime/article/How-innocent-man-s-DNA-was-found-at-killing-scene-4624971.php.
[90] *Id.*
[91] Aaron Opoku Amankwaa & Carole McCartney, *The effectiveness of the UK national DNA database*, 1 Forensic Science International: Synergy 45, 49 (2019), https://www.sciencedirect.com/science/article/pii/S2589871X19300713.
[92] Jason Silverstein, *The Dark Side of DNA Evidence*, The Nation (Mar. 27, 2013), https://www.thenation.com/article/dark-side-dna-evidence/.

into the future. DHS's own history makes the possibility of such a breach likely. DHS's planned "person-centric model" increases these security risks—storing all biometric data together with biographic and family relationship data means that a security breach could be catastrophic.

The many recent security breaches and reports of falsified data—including biometric data—show that the government must maintain extremely rigorous security measures and audit systems to protect against data loss. DHS and other agencies in the federal government have shown they are not up to this challenge. For example, in September 2020, the DHS Office of the Inspector General ("OIG") chastised U.S. Customs and Border Protection ("CBP") for its inadequate security practices that enabled bad actors to steal nearly 200,000 travelers' face images from a subcontractor's computers.[93] CBP's systems had no technical measures in place to prevent its subcontractor from downloading the images to unencrypted USB drives on at least three separate occasions.

The OIG report comes on the heels of a Government Accountability Office ("GAO") report that noted that CBP has failed to conduct necessary audits to ensure its airline partners are complying with privacy requirements in its biometric exit program—a program that uses face recognition on U.S. citizens as well as foreign travelers.[94] And CBP has no plans to conduct such audits in the future.[95] One of the authors of the GAO Report noted that the GAO has "done a number of reviews looking at CBP's efforts to develop and implement a biometric entry and exit system[,] and we have, over the years, identified long-standing challenges in CBP's efforts to develop and implement that system."[96]

USCIS also has suffered serious security breaches in the past, including from insiders. In 2007 and 2008, employees and supervisors at the agency's Texas Service Center "abused system logon privileges, gained unauthorized access in some instances[,] and then allegedly sabotaged audit logs to leave behind no traces of their illicit

[93] Office of the Inspector Gen., Dep't Homeland Sec., Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot 5–6 (2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.
[94] Gov't Accountability Office, Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues (2020), https://www.gao.gov/assets/710/709107.pdf.
[95] *Id.* at 36.
[96] Mila Jasper, *Customs Deploying Biometric Tech at Ports Without Fully Addressing Privacy Requirements, GAO Finds*, Nextgov (Sept. 3, 2020), https://www.nextgov.com/cio-briefing/2020/09/customs-deploying-biometric-tech-ports-without-fully-addressing-privacy-requirements-gao-finds/168228/.

activities."[97] Similar activity occurred within the agency's Fraud Detection and National Security Directorate in Vermont around the same time.[98] These vulnerabilities "raise troubling questions about the agency's ability to police insider threats and employee and contractor access to critical government networks."[99]

Other federal agencies have had similar challenges securing biometric and biographic data on individuals. In 2015, sensitive data on more than 25 million people stored in Office of Personnel Management databases was stolen.[100] This data included biometric information and addresses, health and financial history, travel data, and data on people's friends and neighbors.[101] And in the international context, as the multiple security breaches of India's Aadhaar national biometric database have shown, these breaches can make millions of individuals subject to fraud and identity theft.[102]

DHS has admitted that it cannot currently provide adequate protection for its existing biometric data. DHS's initial Privacy Impact Assessment ("PIA") for the HART

[97] Aliya Sternstein, *Investigation reveals widespread insider hacking at immigration agency*, Nextgov (Aug. 18, 2011), https://www.nextgov.com/technology-news/2011/08/investigation-reveals-widespread-insider-hacking-at-immigration-agency/49624/ (The Texas Service Center "is one of four regional centers that handle a variety of immigration-related petitions and applications."); Aliya Sternstein, *DHS insider hacking case reveals serious network security vulnerabilities*, Nextgov (Sept. 12, 2011), https://www.nextgov.com/technology-news/2011/09/dhs-insider-hacking-case-reveals-serious-network-security-vulnerabilities/49757/.

[98] Sternstein, *Investigation reveals widespread insider hacking at immigration agency*, *supra* n.97.

[99] *Id.*

[100] Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. Times (July 9, 2015), http://www.nytimes.com/2015/07/10/ us/office-of-personnel-management-hackers-got-data-of-millions.html; *see also* David Stout & Tom Zeller, Jr., *Vast Data Cache About Veterans Is Stolen*, N.Y. Times (May 23, 2006), https://www.nytimes.com/2006/05/23/washington/23identity.html.

[101] *Id.*

[102] *See, e.g.*, Vidhi Doshi, *A security breach in India has left a billion people at risk of identity theft*, Wash. Post (Jan. 4, 2018), https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/. Other government databases have suffered similar breaches. *See also, e.g. MEPs question Commission over problems with biometric passports*, European Parliament News (Apr. 19, 2012), http://www.europarl.europa.eu/news/en/headlines/content/20120413STO42897/html/MEPs-question-Commission-over-problems-with-biometric-passports (noting that, at the time, "In France 500,000 to 1 million of the 6.5 million biometric passports in circulation are estimated to be false, having been obtained on the basis of fraudulent documents").

database notes that, as of mid-2020, the agency had thus far failed to complete a system security plan for HART.[103] Given the work shutdowns due to the COVID pandemic, it is unlikely this has changed in the five months since the PIA was uploaded to DHS's website. Further, DHS has only conducted a PIA for the first increment of HART, which the agency is rolling out in four increments. The Increment 1 PIA indicates that "Increment 2 will provide additional biometric capabilities to HART to meet customer needs."[104] Therefore, DHS has not yet conducted the privacy assessment process for the functionalities within the overall design of HART that implicate the data that is the subject of this Proposed Rule. Through this NPRM, then, a vast array of data would be slipped into a system without a prior privacy impact assessment concerning its processing and use.

The risk of security breaches to children's biometrics is especially acute. A recent U.S. Senate Commerce Committee report collects a number of studies that "indicate that large numbers of children in the United States are victims of identity theft."[105] Breaches of children's biometric data further exacerbate this security risk because biometrics cannot be changed. As a recent UNICEF report explains, the collection of children's biometric information exposes them to "lifelong data risks" that are not possible to presently evaluate.[106] Never before has biometric information been collected from birth, and we do not know how the data collected today will be used in the future.

Given the government's poor track record on securing data and DHS's excessively long retention periods for personal data, DHS must do more than merely assert it has adequate security protocols in place to protect this sensitive data.

III. The Proposed Rule's Vast Expansion of Biometrics Collection Threatens First Amendment Protected Activity

This massive expansion of biometrics collection also threatens First Amendment protected activity. By collecting and retaining biometric data like face recognition and sharing it broadly with federal, state, and local agencies, as well as with contractors and foreign governments, DHS lays the groundwork for a vast surveillance and tracking network that could impact individuals and communities for years to come. DHS could soon build a database large enough to identify and track all people in public places, without their knowledge—not just in places the agency oversees, like at the border, but

[103] Dep't of Homeland Sec., *supra* n.50, at 14–15.
[104] *Id.* at 3.
[105] Minority Staff Report, Senate Committee on Commerce Science, and Transportation, Children's Connected Toys: Data Security and Privacy Concerns 5 (2016), https://www.hsdl.org/?view&did=797394.
[106] UNICEF, Faces, Fingerprints and Feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programmes 19 (2019), https://data.unicef.org/resources/biometrics/.

anywhere there are cameras. This burden falls disproportionately on communities of color, immigrants, religious minorities, and other marginalized groups.

Face recognition and similar technologies make it possible to identify and track people in real time, including at lawful political protests and other sensitive gatherings.[107] Widespread use of face recognition by the government—especially to identify people secretly when they walk around in public—will fundamentally change the society in which we live. This risk is especially acute given the NPRM's stated goal of continuous vetting. If immigrants and their U.S. citizen and permanent resident family members know the government can request, retain, and share with other law enforcement agencies their most intimate biometric information at every stage of the immigration lifecycle, many may self-censor and refrain from asserting their First Amendment rights. Studies show that surveillance systems and the overcollection of data by the government chill expressive and religious activity. For example, in 2013, a study involving Muslims in New York and New Jersey found excessive police surveillance in Muslim communities had a significant chilling effect on First Amendment-protected activities.[108] Specifically, people were less inclined to attend mosques they thought were under government surveillance or to engage in religious practices in public, or even to dress or grow their hair in ways that might subject them to surveillance based on their religion.[109]

Further, when biometric data is combined with data that implicates core First Amendment rights, collected by USCIS and other DHS components, the data together will provide a detailed portrait of individuals and their habits and relationships. For example, a 2020 Privacy Impact Assessment noted that ICE Homeland Security Investigations agents collect images during investigations, including "mugshots, surveillance photos, social media posts and images confiscated from phones or other data devices," and can also take still shots from video recordings and streams.[110] Similarly,

[107] *See* Rebecca Heilweil, *New surveillance AI can tell schools where students are and where they've been*, Vox (Jan. 25, 2020), https://www.vox.com/recode/2020/1/25/21080749/surveillance-school-artificial-intelligence-facial-recognition.

[108] Diala Shamas & Nermeen Arastu, Mapping Muslims: NYPD Spying and its Impact on American Muslims 4 (2013), https://www.law.cuny.edu/wp-content/uploads/page-assets/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

[109] *Id.* at 12–25.

[110] Dep't of Homeland Sec., Privacy Impact Assessment for the ICE Use of Facial Recognition Services DHS/ICE/PIA-054 3 (May 13, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf.; *see also* Derek B. Johnson, *Privacy report outlines scope, limitations of ICE facial recognition*, FCW (May 27, 2020), https://fcw.com/articles/2020/05/27/ice-facial-recognition-privacy.aspx (noting that the PIA "lays out more than a dozen potential

DHS collects social media data from visa applicants and other travelers to the United States for vetting purposes.[111] And a 2018 System of Records Notice for the HART database noted that HART will combine biometric data with "miscellaneous officer comment information," "encounter data," and "records related to the analysis of relationship patterns among individuals" including "non-obvious relationships."[112] This data combined has broad First Amendment implications.

This data is also often collected under extremely questionable legal circumstances. For example, ICE officers use mobile devices to collect biometric and biographic data from people they "encounter" in the field, including via unauthorized entry into people's homes and Bible study groups, and in public places where people congregate with other members of their community, such as on soccer fields, in community centers, and on buses.[113] "Encounters" like these, whether they are conducted by ICE or by state or local police, are frequently not based on individualized suspicion[114] that a civilian has done anything wrong,[115] but that does not prevent the officer from stockpiling any information obtained from the civilian during the encounter.

IV. The NPRM Fails to Adequately Address the Risk of Error in Biometric Technologies and Databases that Store Biometric Data

The NPRM allows for the collection and retention of biometric information from both immigrants as well as their U.S.-based family members. However, the Proposed Rule fails to consider the lack of reliability of many of these biometric technologies and the databases that store this information.

privacy risks associated with [ICE's] use of and access to numerous databases and algorithms to identify travelers or suspects.").

[111] Saira Hussain & Sophia Cope, *DEEP DIVE: CBP's Social Media Surveillance Poses Risks to Free Speech and Privacy Rights*, EFF Deeplinks Blog (Aug. 5, 2019), https://www.eff.org/deeplinks/2019/08/deep-dive-cbps-social-media-surveillance-poses-risks-free-speech-and-privacy.

[112] Lynch, *supra* n.25.

[113] National Immigration Law Center, Untangling the Immigration Enforcement Web 13–14 (2017), https://www.nilc.org/wp-content/uploads/2017/09/Untangling-Immigration-Enforcement-Web-2017-09.pdf.

[114] *See* Benjamin Mueller, *New York Police Dept. Agrees to Curb Stop-and-Frisk Tactics*, N.Y. Times (Feb. 2, 2017), https://www.nytimes.com/2017/02/02/nyregion/new-york-police-dept-stop-and-frisk.html.

[115] *See* Dave Maass & Jennifer Lynch, *San Diego Gets in Your Face With New Mobile Identification System*, EFF Deeplinks Blog (Nov. 7, 2013), https://www.eff.org/deeplinks/2013/11/san-diego-gets-your-face-new-mobile-identification-system.

A. Errors in Biometric Identifiers

1. Errors in DNA Technology

One of the methods DHS contemplates using to test for claimed genetic relationships is through Rapid DNA.[116] Rapid DNA machines are self-contained, automated desktop units that process DNA data and conduct analysis without human review, except in the case of inconclusive results.[117] However, Rapid DNA testing has shown to be error-prone. In 2017, the Swedish National Forensic Centre published a report detailing serious problems with certain Rapid DNA analyzers, including

> numerous issues with the system related to the hardware, firmware, software as well as the cartridges. The most severe issues are the retrieval of an incorrect DNA profile, PCR product or sample leakage and the low success rate. In total 36% of the runs had problems or errors effecting two or more samples resulting in a 77% success rate for samples consisting of . . . amounts where complete DNA profiles are expected.[118]

Notably, DHS has provided no statistical or peer-reviewed studies as to the accuracy of the Rapid DNA systems already in use.

2. Errors in Face Recognition Technology

Accuracy issues abound with DHS's collection and retention of facial imaging under the Proposed Rule. Face recognition systems are notoriously unreliable for identifying Black people, women, and young people. An MIT study from 2016 found significant error rates across face recognition systems for people with darker skin, and especially for Black women.[119] A 2019 comprehensive report by the National Institute on Standards and Technology reiterated the MIT study's findings, identifying algorithms that were 10 to 100 times less accurate for West and East African, American Indian,

[116] 85 Fed. Reg. at 56353.

[117] *See* U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the Rapid DNA Operational Use DHS/ICE/PIA-050 2 (June 25, 2019), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-rapiddna-june2019_1.pdf.

[118] Swedish National Forensic Centre, Experiences from operating the RapidHIT® System 3 (2017), https://nfc.polisen.se/siteassets/dokument/informationsmaterial/rapporter/nfc-rapport-2017-02_experiences-from-operating-the-rapidhit-system.pdf.

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

African American, and Asian populations.[120] The algorithms were also less accurate for women, the elderly, and children.[121]

In addition, due to years of well-documented racially-biased policing and immigration practices, criminal databases unjustifiably include a disproportionate number of African Americans, Latinos, and immigrants.[122] If facial imaging collected through this Proposed Rule's biometric process is shared widely with local, state, and federal law enforcement agencies, immigrants could be subject to misidentifications, as well as continuous surveillance and monitoring.

3. Accuracy Challenges in Biometrics Collected from Children

Finally, there are real questions as to whether biometric technology can accurately analyze children's information. A recent DHS assessment stated unequivocally that there is an unmitigated risk that "retaining the fingerprint, face, or iris biometric for juveniles may result in inaccurate results due to factors including growth and image quality."[123] That finding is consistent with UNICEF's assessment that currently "there are no biometric technologies capable of consistently providing high levels of accuracy in very young children (less than five years)" and "[e]vidence is also weak for use of biometrics in children aged 5–15 years."[124] This is not surprising since, as the UNICEF reports notes, there is relatively little data analyzing biometric technologies' accuracy over long periods of time.[125]

B. Errors in Databases

DHS claims that by collecting biometrics and linking them to one person, the agency will better be able to track the person for their immigration lifecycle. This rings hollow. In fact, in a recent case challenging the reliability of DHS databases, a federal district court found that independent investigations of several DHS databases highlighted high error rates within the systems.[126] For example, in 2017, the DHS OIG found that the

[120] U.S. Gov't Accountability Office, Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues 76 (2020), https://www.gao.gov/assets/710/709107.pdf.
[121] *Id.*
[122] *See, e.g.*, NAACP, *Criminal Justice Fact Sheet* (2009), https://www.naacp.org/criminal-justice-fact-sheet/.
[123] Dep't of Homeland Sec., *supra* n.50, at 24–25.
[124] UNICEF, *supra* n.106, at 5.
[125] *See id.*
[126] *Gonzalez v. Immigr. & Customs Enf't*, 416 F. Supp. 3d 995 (C.D. Cal. 2019), *rev'd on other grounds sub nom. Gonzalez v. Immigr. & Customs Enf't*, 2020 WL 5494324 (9th Cir. Sept. 11, 2020). The Ninth Circuit remanded the case to the district court for more

database used for information about visa overstays was wrong 42 percent of the time.[127] Other databases used to identify lawful permanent residents and people with protected status had a 30 percent error rate.[128] One DHS database had a class of admission field that was incorrect for 12 percent of people studied.[129]

Part of the reason for these significant error rates is because DHS often exempts its databases from privacy and accuracy requirements under the federal Privacy Act, 5 U.S.C. § 552a *et seq*. The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government."[130] The Homeland Security Act of 2002, which established DHS, specifically calls on DHS's Chief Privacy Officer to assure that DHS's use of technologies "sustains, and do[es] not erode, privacy protections" and ensure that all personal information held in DHS systems of records "is handled in full compliance with fair information practices as set out in the Privacy Act of 1974."[131]

One of the most important of these fair information practices requires that agencies "[m]aintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."[132] Nevertheless, DHS and its component agencies have chosen to exempt many of their databases from Privacy Act mandates. Several DHS databases—including ones that store biographical information, aid in civil and criminal investigations, and store information about student visa holders—are exempt from Privacy Act provisions requiring that a system of records contain "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency" and "accuracy, relevance, timeliness, and completeness" requirements.[133]

DHS similarly sought exemptions from the Privacy Act for its External Biometric Records ("EBR")—biometric and biographic records DHS receives from external agencies, and which are integral to building out its HART database.[134] EFF submitted

fact-finding on the reliability of each of 16 databases before evaluating whether reliance on the databases to make probable cause determinations violates the Fourth Amendment.

[127] *Id.* at 1010.

[128] *Id.* at 1009.

[129] *Id.* at 1008.

[130] S. Rep. No. 93-1183, at 1.

[131] 6 U.S.C. § 142.

[132] 5 U.S.C. § 552a(e)(5).

[133] 5 U.S.C. § 552a(e)(1), (e)(5).

[134] Dep't of Homeland Sec., Notice of a new system of records, 83 Fed. Reg. 17829 (Apr. 24, 2018).

comments in 2018 opposing the exemption of EBR from the Privacy Act, noting the significant inaccuracies in other DHS records and the lack of transparency about exactly what data would be maintained and shared about individuals.[135]

Moreover, the biometrics covered in the Proposed Rule will also be combined with unverified data from federal, state, and local agencies outside DHS as well as data from foreign governments. Many of these partners will be able add in their own "derogatory and disposition information to the records."[136] In the NPRM, DHS asserts, without support, that it "has internal procedural safeguards to ensure technology used to collect, assess, and store the differing modalities is accurate, reliable, and valid."[137] However, in the Privacy Impact Assessment for the HART database, DHS recognizes that it cannot mitigate the privacy risk that those with direct access to the database will manually enter inaccurate derogatory information or data of insufficient quality.[138]

DHS's use of gang databases (its own and those from states), is a prominent example of this problem. These databases often contain unsubstantiated data concerning people's status and associations and are notoriously inaccurate.[139] In fact, a 2016 California state audit of the CalGang database found "42 individuals in CalGang whose birthdates indicated that they were less than one year old at the time their information was entered, 28 of whom were entered into the system in part because they admitted to being gang members."[140] DHS components rely on these state-level databases to make immigration and benefit determinations. Because immigration laws provide no clear definition of what constitutes gang involvement, immigration officers are able to rely on flimsy or false evidence, including evidence that touches on core First Amendment protected activity, such as social media posts and observations about attire, tattoos, or affiliations to label someone a gang member. Even painting their fingernails a certain color, wearing certain undergarments, or wearing their hair a certain way can get a person labeled as a gang member.[141] DHS has even fabricated gang status as an excuse to deport

[135] Jennifer Lynch, Electronic Frontier Foundation, Comment Letter on Notice of a New System of Records: Department of Homeland Security/All-041 External Biometric Records (EBR) System of Records & Proposed Privacy Act Exemptions 14–15 (May 24, 2018), https://www.eff.org/document/eff-comments-dhs-its-proposal-exempt-its-new-biometrics-and-relationship-data-us-privacy.
[136] Dep't of Homeland Sec., *supra* n.50, at 24.
[137] 85 Fed. Reg. at 56341.
[138] *See* Dep't of Homeland Sec., *supra* n.50, at 24.
[139] *Id.* at 11–12.
[140] California State Auditor, The CalGang Criminal Intelligence System 3 (2016), http://www.voiceofsandiego.org/wp-content/uploads/2016/08/CalGangs-audit.pdf.
[141] Los Angeles Police Dep't, How Are Gangs Identified, http://www.lapdonline.org/la_gangs/content_basic_view/23468 (last visited Oct. 13, 2020).

people.[142] This burden disproportionately falls on immigrant youth, a class of individuals who will also be burdened with biometrics collection if this Proposed Rule goes into effect.[143]

Given DHS's existing record of outdated, inconsistent databases that the agency has repeated fought to exempt from Privacy Act protections, there is little reason to expect that expanding biometric collection will help the agency maintain more accurate records about immigrants.

V. DHS Has Not Provided an Adequate Justification for Its Proposed Changes.

The NPRM does not adequately explain why a sweeping expansion of biometrics collection is necessary. In fact, DHS even seems to concede as much, stating that "[t]he proposed rule would provide benefits that are not possible to quantify."[144] To the extent that DHS does attempt to articulate potential benefits of the NPRM, DHS suggests that the new system will "provide DHS with the improved ability to identify and limit fraud."[145] However, the scant evidence that the NPRM offers to demonstrate the existence of fraud cannot justify its expansive changes. For example, DHS purports to justify its collection of DNA from children based on the fact that there were "432 incidents of fraudulent family claims" between July 1, 2019 and November 7, 2019 along the southern border.[146] Not only does the NPRM not define what constitutes a "fraudulent family," but also it leaves out that during that same period, an estimated 100,000 family units crossed the southern border, meaning that the so-called "fraudulent family" units made up less than one-half of one percent of all family crossings.[147]

In addition, the NPRM does not address the privacy costs discussed in depth above. The NPRM merely notes that "[t]here could be some unquantified impacts related to privacy concerns for risks associated with the collection."[148] And of course, the NPRM would come at a considerable financial cost to taxpayers, at a time when USCIS is

[142] Mark Joseph Stern, *Bad Liars*, Slate (May 16, 2018), https://slate.com/news-and-politics/2018/05/federal-judge-accused-ice-of-making-up-evidence-to-prove-that-dreamer-was-gang-affiliated.html.
[143] Immigrant Legal Resource Center, Deportations by Any Means Necessary (2018), https://www.ilrc.org/sites/default/files/resources/deport_by_any_means_nec-20180521.pdf
[144] 85 Fed. Reg. at 56344.
[145] *Id.* at 56344.
[146] *Id.* at 56352.
[147] U.S. Customs and Border Patrol, *Southwest Border Migration FY 2019*, https://www.cbp.gov/newsroom/stats/sw-border-migration/fy-2019 (analyzing same time period of data as in NPRM).
[148] 85 Fed. Reg. at 56385.

already experiencing fiscal challenges.[149] Even with the millions of dollars in new fees USCIS will collect, the NPRM is estimated to cost anywhere from $2.25 to $5 billion over the next 10 years.[150] DHS also notes that additional costs could manifest.[151]

VI. The NPRM's Expansion of Biometric Collection Exceeds DHS's Statutory Authority

The NPRM cites numerous statutes that it claims authorize it to collect biometrics from U.S. citizens and non-citizens in processing routine immigration applications. However, there is no federal statute that authorizes such broad collection of biometrics. The statutes DHS relies upon are many decades old and cannot plausibly be construed to authorize the use of modern biometric technology. For example, the core statutory provision that DHS cites, 8 U.S.C. § 1225(d)(3), authorizes immigration officials to "take and consider evidence" in order to enforce the nation's immigration laws.[152] The basic formulation of that statute was first passed as part of the 1917 Immigration Act and was later codified in its current form as part of the 1952 Immigration and National Act ("INA").[153] And while Congress used generalized terms in the Act, it did not grant immigration authorities unlimited power. In the House Judiciary Committee Report accompanying the INA, the Committee wrote: "It is not intended by this provision to sanction the indiscriminate questioning or harassment of citizens returning to the United States."[154] Additionally, where Congress has approved the use of biometrics, it has said so clearly. For example, after 9/11, Congress directed DHS to "develop a plan to accelerate the full implementation of an automated biometric entry and exit data system."[155] But DHS can point to no such authorization in this instance.

DHS also does not have statutory authority nor regulatory authority to mandate DNA collection from U.S. citizens and from non-citizens seeking to immigrate to the United States. DHS elides this point by stating that it is "expanding its regulatory authority" to mandate DNA collection in this context. However, the only statute that provides DHS with explicit authority to collect DNA is the DNA Fingerprint Act of 2005, which authorizes the Attorney General to collect DNA "from individuals who are arrested, facing charges, or convicted or from non-United States persons who are

[149] *See* Doug Rand & Lindsay Miliken, *The Case of the Insolvent Federal Agency: A Forensic Analysis of Public Data on U.S. Citizenship & Immigration Services*, N.Y.U. J. Legis. & Pub. Pol'y Quorum (2020), https://nyujlpp.org/quorum/the-case-of-the-insolvent-federal-agency-a-forensic-analysis-of-public-data-on-u-s-citizenship-immigration-services/.

[150] 85 Fed. Reg. at 56383 (Table 22).

[151] *Id.* at 56388.

[152] *Id.* at 56347.

[153] H.R. Rep. No. 1365, at 164 (1952).

[154] *Id.* at 65.

[155] 8 U.S.C.§ 1365b(c)(1).

detained under the authority of the United States" and to delegate that authority.[156] Those seeking to prove a genetic familial relationship in immigration proceedings are not, by any stretch, arrested, facing charges, or "detained under authority of the United States."

DHS plainly does not have the statutory authority to collect biometric information from children under the age of 14. At least three separate federal statues establish that immigration officials can only collect fingerprints and photographs from people over the age of 14.[157] But DHS reads these statutes as "not [] imposing a lower age limit" and relies on 8 U.S.C. § 1357(b), a statute generally giving immigration officials the ability to "take and consider evidence," to permit it to collect any type of biometric from all children younger than 14.[158] That construction defies both common sense and ordinary principles of statutory interpretation. First, the statutes only authorize the collection of certain personal information from people over the age of 14. Therefore, accordingly, they prevent the government from taking fingerprints from children younger than 14. DHS's claim to the contrary would essentially render meaningless Congress's inclusion of the age of 14 in multiple statutes. Second, DHS cannot use the general provision of 8 U.S.C. § 1357(b) to override the more specific provision in 8 U.S.C. § 1357(f)(1) regarding the collection of information from children, which gives the attorney general the power to make rules governing the "fingerprinting and photographing of each alien 14 years of age or older." Such specific provisions always govern over more general ones.[159] And clearly, since Congress limited the collection of biometrics like fingerprints and photographs to individuals over the age of 14, it is not plausible that DHS has the authority to collect other far more invasive and revealing biometrics from children, as it purports in this NPRM.

The statutes limiting fingerprint collection from children under the age of 14 are part of a broader body of law that recognizes special privacy protections for children.[160]

[156] *See* 34 U.S.C. § 40702(a)(1)(A).

[157] 8 U.S.C. § 1357(f)(1), 8 U.S.C. § 1302, and 8 U.S.C. § 1304.

[158] 85 Fed. Reg. at 5637.

[159] *See, e.g.*, *Fourco Glass Co. v. Transmirra Products Corp.*, 353 U.S. 222, 228 (1957) ("However inclusive may be the general language of a statute, it will not be held to apply to a matter specifically dealt with in another part of the same enactment.").

[160] *See* Children's Online Privacy Protection Act of 1998, (15 U.S.C. § 6501, *et seq.*); *see also* Dissenting Statement of Commissioner Rohit Chopra, *In the Matter of Google LLC and YouTube, LLC*, File No. 1723083 (Sept. 4, 2019) ("When individuals use a mobile device with Google's Android operating system or give commands to a Google Home device, Google is able to glean more and more insights about their personal lives. Google then monetizes these insights by using them to psychologically profile each user and predict in real time what content will be most engaging and which ads will be most persuasive. For any person, this is worrisome. But when it happens to a child, it can be illegal.").

In the context of children involved in the immigration system, the need for those protections is evident.[161] First, children need special protections because they do not have their own autonomy nor can they understand the risks of turning over their biometric information. Second, as discussed above in Part II.B, the collection of children's biometric information exposes them to "lifelong data risks" that are not possible presently to evaluate.[162]

Finally, members of Congress have expressed concern about DHS's statutory overreach and are currently considering legislation on many of the biometrics that DHS claims to have regulatory authority to collect. U.S. Senators Ed Markey (D-MA) and Mike Lee (R-UT) have repeatedly expressed deep concern that DHS's biometric-related actives reach beyond its statutory mandate. In a recent letter, they wrote in regard to DHS's collection of biometrics from U.S. citizens leaving the country, "[w]e are concerned that the use of the program on U.S. citizens remains facially unauthorized[.] . . . We request that DHS stop the expansion of this program and provide Congress with its explicit statutory authority to use and expand a biometric exit program on U.S. citizens."[163] Calling for the need to reconsider DHS's mandate with respect to biometrics collection, both senators have introduced legislation to limit it. Building on pledges from the nation's leading technology companies not to sell facial recognition software to the government, members of both houses of Congress have introduced a bill that would impose a prohibition on the federal government's use of all biometrics.[164] Another bipartisan bill would require federal law enforcement to obtain a court order before using facial recognition technology to conduct targeted ongoing public surveillance.[165] And, in a series of hearings, many members of the House of Representatives have expressed serious concerns about the privacy risks of biometrics.[166] Meanwhile, states and cities

[161] *See* UNICEF, *supra* n.106, at 19.

[162] *Id.*

[163] Letter from Sens. Edward J. Markey & Mike Lee to Kirstjen Nielson, Secretary of Homeland Sec. (Dec. 21, 2017), https://www.markey.senate.gov/imo/media/doc/DHS%20Biometrics%20Markey%20Lee%20.pdf.

[164] Office of Senator Ed Markey, *Senators Markey And Merkley, And Reps. Jayapal, Pressley To Introduce Legislation To Ban Government Use Of Facial Recognition, Other Biometric Technology* (June 25, 2020), https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology.

[165] Office of Senator Chris Coons, *Facial Recognition Tech: Sens. Coons, Lee bill requires court orders for law enforcement use of facial recognition technology* (Nov. 14, 2019), https://www.coons.senate.gov/news/press-releases/facial-recognition-tech-sens-coons-lee-bill-requires-court-orders-for-law-enforcement-use-of-facial-recognition-technology.

[166] *See* About Face: Examining The Department Of Homeland Security's Use Of Facial Recognition And Other Biometric Technologies, 116th Cong. (2019).

have passed legislation restricting the use of biometrics, and similar bills are currently pending in state legislatures.[167] It is not the appropriate role for a federal agency to supersede debate in Congress. Elected lawmakers must resolve these important matters first before DHS can put forward a proposal like this that seeks to perform an end run around the democratic process.

VII. CONCLUSION

This Proposed Rule vastly expands both the modalities of biometrics collected and the population from whom these biometrics will be collected, yet it fails to address key concerns we have outlined in this comment, including privacy, security, impacts on civil liberties and vulnerable communities, and statutory authority. Therefore, we strongly urge DHS to rescind the NPRM. If you have any questions, please contact Jennifer Lynch at jlynch@eff.org.

Sincerely,

Jennifer Lynch
Saira Hussain
Nathaniel Sobel
Electronic Frontier Foundation

Signed also on Behalf of:

The Center on Privacy & Technology at Georgetown Law
Immigrant Legal Resource Center
National Hispanic Media Coalition
National Immigration Law Center
New America's Open Technology Institute
Open Society Justice Initiative
Open The Government
Restore The Fourth

[167] Electronic Frontier Foundation, Bans, bills and moratoria, https://www.eff.org/aboutface/bans-bills-and-moratoria (last visited Oct. 13, 2020).