October 13, 2020

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

Submitted via http://www.regulations.gov

Comment of the American Civil Liberties Union, ACLU of Illinois, ACLU of Massachusetts, ACLU of San Diego & Imperial Counties, and ACLU of Washington in Opposition to 85 Fed. Reg. 56338, USCIS Docket No. USCIS-2019-0007, EOIR Docket No. 19-0007, CIS No. 2644-19, RIN 1615-AC14; Collection and Use of Biometrics by U.S. Citizenship and Immigration Services

Dear Regulations Docket Clerk:

The American Civil Liberties Union, ACLU of Illinois, ACLU of Massachusetts, ACLU of San Diego & Imperial Counties, and ACLU of Washington (collectively, ACLU) submit this comment in strong opposition to the above-referenced Proposed Rule, published at 85 Fed. Reg. 56338 (proposed Sept. 11, 2020). The Department of Homeland Security (DHS) should immediately rescind the Proposed Rule because it would massively expand the collection of sensitive biometric information out of all proportion to any justifiable need, endangering the rights of millions of individuals, including immigrants, children under the age of fourteen, survivors of violence and trafficking, and U.S. citizens.

In the context of immigration benefits, DHS currently requires biometrics collection only for certain, specific benefits, and the biometrics DHS collects are typically limited to signatures, photographs, and/or fingerprints. DHS exempts children who are younger than fourteen and adults who are older than seventy-nine from biometrics collection. It does not require biometrics from Violence Against Women Act (VAWA) or trafficking (T) visa self-petitioners, and it presumes good moral character for VAWA and T visa applicants who are under the age of fourteen. In addition, DHS only requires biometrics collection from U.S. citizens and lawful permanent residents in the intercountry adoption context. And it does not routinely collect DNA to establish familial relationships.

The Proposed Rule seeks to flip all of this on its head. Pursuant to the Proposed Rule, rather than rely on policy, practice, or form instructions that connect the collection of a specific biometric to a specific purpose for a specific

benefit or application, DHS would be presumptively authorized to collect any biometrics—broadly defined as "the measurable biological (anatomical and physiological) or behavioral characteristics used for identification of an individual"—from "any applicant, petitioner, sponsor, beneficiary, or individual filing or associated with an[y] immigration benefit or request." In particular, this would expand biometric collection to include faceprints, voiceprints, iris scans, palmprints, DNA, and photographs of scars, skin marks, and tattoos.

Under the Proposed Rule, DHS would collect, store, and share the biometrics not only for administering immigration benefits, but also "to perform any functions necessary for . . . enforcing immigration and naturalization laws." Specific uses contemplated by the Proposed Rule include identity verification and secure document production, as well as criminal and national security background checks. Under the Proposed Rule, such background checks would occur even for those individuals applying for or sponsoring benefits that do not require consideration of past criminal convictions. In addition, DHS would not only share the biometrics information between its own agencies—United States Citizenship and Immigration Services (USCIS), Customs and Border Protection (CBP), and Immigration and Customs Enforcement (ICE)—but also with, at a minimum, the Federal Bureau of Investigation (FBI) and the Department of Defense (DOD). Broad language throughout the Proposed Rule also suggests that DHS would seek to retain the ability to use and share the sensitive biometric information it collected far beyond the scope of the stated purpose of the collection, "to the extent permitted by law."

The Proposed Rule would expand the Department's collection of biometrics along every axis: the types of biometrics DHS collects, the individuals it subjects to biometrics collection, and the purposes for which it uses the collected biometrics. By DHS' own estimate, under the Proposed Rule, the Department would capture 2.17 million new biometric submissions, bringing the total number of individuals subject to biometric collection up to 6.07 million people each year—including survivors of domestic violence and human trafficking, tens of thousands of children under the age of fourteen, and a substantially increased number of U.S. citizens and lawful permanent residents.

Such amassing of biometric identifiers is out of all proportion to any legitimate government purpose; it is unnecessary and unjustified. The Proposed Rule does not identify a clear need for or problem that would be solved by the proposed expanded collection of biometrics—particularly where fingerprints are already collected. At the same time, because the new biometrics are not reliably accurate, the Proposed Rule would fail to accomplish even DHS' stated goals of valid identity verification, secure document production, and accurate criminal and national security background checks. Instead, it would result in the erroneous denial of benefits and possibly even lead to false arrests.

The technology used to capture biometric identifiers is known to have discriminatory impacts and has a high potential for misuse. Moreover, implementing the Proposed Rule would grant the government an unprecedented power to pervasively track people's movements, associations, and beliefs in ways that threaten core constitutional values and civil liberties. Troublingly, that power would be focused specifically on immigrants and their communities. For these reasons, as detailed further below, the ACLU strongly opposes the Proposed Rule.

I. The collection of each additional biometric identifier creates new risks of surveillance, identity theft, and misuse.

The increased collection of biometric information envisioned by the Proposed Rule—including DNA tests and prints of our faces, voices, palms, and irises—would pose grave risks to our privacy and civil liberties. Biometric information is biologically unique to each person and it is immutable. Unlike ID cards, social security numbers, addresses, and other personal identifying information, biometric identifiers cannot be changed in the wake of unauthorized disclosure or misuse—once these harms occur, they are irreparable and likely ongoing. And because biometric identifiers can be collected without our knowledge, as collection can occur without bodily intrusion and from a distance, once the information is collected and associated with names and other identifying details, biometrics databases put individuals at serious risk of identity theft and persistent surveillance. Because we wear our biometric identifiers on our bodies and carry them in our voices, it is virtually impossible for us to insulate ourselves from these harms without strong legal protections.

The aggregation of different types of biometric information envisioned by the Proposed Rule poses risks to our privacy and civil liberties at a massive scale. It enables surveillance that can expose where people go, who they associate with, and even what they believe. Moreover, the mass biometric collection envisioned by this Proposed Rule is likely to exacerbate the racial disparities in existing government databases. Collecting biometric identifiers from individuals seeking to immigrate, those seeking to sponsor them, and others in their communities will lead to increased law enforcement scrutiny, surveillance, and investigation of people and communities of color. Imposing this required collection on children who are younger than fourteen and on survivors of violence and trafficking will similarly lead to increased law enforcement scrutiny and surveillance for those individuals. Indeed, this increased scrutiny is an inevitable result of the Proposed Rule's "continuous vetting," which will lead to biometrics collection throughout individuals' years-long immigration processes, in excess of current practice without justification.

Face recognition and iris technologies could be deployed on photos going back decades—or live on video—to determine attendance at an Alcoholics

Anonymous meeting, religious services, or a Black Lives Matter protest.[1] Such technology has already been deployed to surveil demonstrators exercising their First Amendment rights at protests.[2] And government actors have also tried to track protesters by swabbing DNA from cigarette butts left behind at protest sites.[3] Almost by definition, voiceprint technology also promises to erase an avenue for anonymous speech, which has been a core American tradition at least since the publication of *The Federalist Papers*, and continues to be a core protection for whistleblowers, survivors of domestic violence, and dissidents.

In addition to chilling or eradicating avenues for constitutionally-protected freedom of speech, amassing biometric identifiers also poses an inherent security risk. DHS claims that this Proposed Rule would "limit the potential for identity theft," without any supporting evidence or statistics showing any identity theft problem. DHS does not adequately explain why the collection of fingerprints and photographs from applicants for immigration benefits is insufficient to protect against identity theft. In actuality, the amassing of millions of biometric identifiers *creates* an enormous risk for identity theft. Personally identifying information compiled by government agencies is subject to hacking and data breaches.[4] And once information is shared with other government agencies or foreign governments, DHS no longer retains control over how that information is maintained or secured. Breaches of biometric data are particularly harmful since, as explained above, biometrics cannot be changed.

DHS has already had trouble protecting incredibly sensitive databases from data breaches. According to a DHS Inspector General Report, approximately 184,000 faceprints from a CBP pilot referred to in the Proposed Rule were recently the subject of a data breach, compromising the security of the individuals in the database.[5] In addition, easy government access to sensitive biometric data can also facilitate abusive conduct, including enabling rogue law enforcement

---

[1] Evan Selinger and Albert Fox Cahn, *Did you protest recently? Your face might be in a database*, Guardian (July 17, 2020), https://www.theguardian.com/commentisfree/2020/jul/17/protest-black-lives-matter-database.

[2] Russell Brandom, *Facebook, Twitter, and Instagram surveillance tool was used to arrest Baltimore protestors*, The Verge (Oct. 11, 2016), https://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api.

[3] *DNA from cigarette leads to Dakota Access arrest 3 years on*, Associated Press (Sept. 6, 2019), https://apnews.com/article/abb444c2e6f14ca49a675e82d4b0d520.

[4] *See, e.g.*, Devlin Barrett et al., U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say, The Wall Street Journal (June 5, 2015), http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breachsources-say-1433451888.

[5] Dep't of Homeland Sec., Off. of Inspector Gen., *Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot* (Sept. 21, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

officers to more easily stalk and harass current or former intimate partners and others.[6]

The potential harms—and inherent intrusions of collection—are heightened by the fact that biometric identifiers can reveal far more than identity. DNA samples, which include our entire genetic blueprint, offer insights into our ancestry, family tree, and propensities for certain medical conditions.[7] In addition, DHS' purported interest in DNA testing under the Proposed Rule stems not from a need to identify an individual, but rather to identify their family members. Yet not all family relationships are biological, of course. And even biological family relationships can be proven in ways that do not require DNA collection or analysis, including through documentary records and testimonial evidence.

Developers of biometric technologies promise that other identifiers, too, can reveal intimate details about a person. Some companies claim to be able to determine a person's efficacy at work based on their facial movements and speaking voice,[8] while others purport to identify a person's sexual orientation by relying on and perpetuating harmful stereotypes about physical appearance.[9] The National Security Agency (NSA) has looked to voice recognition to "automatically identify not just the speaker in a voice intercept, but also their language, gender, and dialect."[10] And scholars suggest that voiceprints could be used to reveal and track medical information, like the onset of Parkinson's disease.[11] The availability of such sensitive data makes the dangers of data breaches and abuses particularly concerning.

---

[6] *Cf.* Jim Avila, Alison Lynn& Lauren Pearle, *Police Sergeant Had Secret Life as Serial Rapist*, ABC News (Aug. 30, 2010), https://abcnews.go.com/Primetime/illinois-police-sergeant-jeffrey-pelo-doubled-serial-rapist/story?id=11497530 (Bloomington, Ill. police officer used "police computer ... to run license plate searches on three of the victims" he targeted for stalking and rape).

[7] While DHS appears to recognize the highly private nature of raw DNA, and proposes treating the DNA itself as a distinctive biometric modality that will not be handled or shared beyond the original purpose of the submission—which, as noted below, should be a limitation imposed on all of the proposed biometric collection—DHS additionally includes a catchall provision, allowing it to use or share the raw DNA as "required . . . by law."

[8] Drew Harwell, *A face-scanning algorithm increasingly decides whether you deserve the job*, Washington Post (Nov. 6, 2019), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

[9] Vanessa Taylor, *Facial recognition misclassifies transgender and non-binary people, study finds*, Mic (Oct. 30, 2019), https://www.mic.com/p/facial-recognition-misclassifies-transgender-non-binary-people-study-finds-19281490.

[10] Ava Kofman, *Finding Your Voice*, The Intercept (Jan. 19, 2018), https://theintercept.com/2018/01/19/voice-recognition-technology-nsa/.

[11] Hanbin Zhang et al., *DeepVoice: A voiceprint-based mobile health framework for Parkinson's disease identification*, 2018 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI) 214, https://ieeexplore.ieee.org/abstract/document/8333407.

These concerns are not merely theoretical. In other countries, we are already seeing face recognition being used as part of comprehensive surveillance systems that monitor and track people. For example, China has 200 million surveillance cameras and is working to develop the capability to identify any citizen within seconds.[12] The government is amassing face recognition databases of individuals who have mental illnesses, used drugs, or petitioned the government with grievances. The government is also using the technology as a tool to track and oppress ethnic minorities, including the Uighur population. For example, China reportedly keeps a face recognition database of all Uighurs who leave the province of Xinjiang, and is developing systems that can alert police when a Uighur moves into a new neighborhood.[13]

Concerns about surreptitious surveillance and abuses of sensitive biometric information are also warranted by this country's history, which—as Congress has recognized—includes the forcible sterilization of people based on perceived genetic "defects," and discrimination against Black people in everything from marriage to employment because of misperceptions about their DNA.[14] More recently, this administration's actual and attempted policies in the immigration context in particular highlight the dangers of increased biometric collection. For example, ICE has run thousands of faceprint searches on states' license databases unbeknownst to license holders,[15] and it recently signed a contract with Clearview AI, a company that has amassed the faceprints of billions of individuals without their knowledge or consent.[16] USCIS currently allows officials to deny lawful permanent resident status to immigrants who are likely to need public assistance, including the use of public benefits like Medicaid for medical conditions,[17] and to base the determination of some immigration applications on whether applicants have "certain communicable diseases."[18] As

---

[12] Jon Russell, *China's CCTV Surveillance Network Took Just 7 minutes to Identify a Reporter*, Tech Crunch (Dec. 14, 2017), https://techcrunch.com/2017/12/13/china-cctv-bbc-reporter/.

[13] Paul Mozur, *One-month, 500,000 Scans: How China is Using A.I. to Profile a Minority*, N.Y. Times (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racialprofiling.html.

[14] Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233, § 2, 122 Stat. 881 (2008), as amended Pub. L. No. 111–256, § 2(j), 124 Stat. 2643 (2010).

[15] Drew Harwell, *FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches*, Washington Post (Jul. 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

[16] Kim Lyons, *ICE just signed a contract with facial recognition company Clearview AI*, The Verge (Aug. 14, 2020), https://www.theverge.com/2020/8/14/21368930/clearview-ai-ice-contract-privacy-immigration.

[17] Nathaniel Weixel, *Trump administration reimposes 'public charge' rule following court victory*, The Hill (Sept. 22, 2020), https://thehill.com/policy/healthcare/517615-trump-administration-reimposes-public-charge-rule-following-court-victory.

[18] *See* 8 U.S.C. §1182(a)(1)(A).

such, the public has reason to be gravely concerned about the future ways in which expanded biometric databases could be used by government entities, including DHS in particular.

In addition, given the risks inherent in biometric collection, DHS' reliance on statutory text authorizing the Department to collect "evidence" concerning immigration benefits and adjudication should not suffice to justify expansive biometric collection. Indeed, DHS' citation to statutes that authorize specific biometric collection for specific purposes suggests that DHS is not authorized to proceed with the Proposed Rule under current law.

II. The proposed biometric collection is prone to error in ways that will disproportionately harm people of color and will increase, rather than ameliorate, administrative burdens.

ACLU
AMERICAN CIVIL LIBERTIES UNION

In addition to creating the privacy, expressive and associational, and security harms discussed above, the proposed biometric collection would also fail to accomplish DHS' central stated goal: ensuring accurate, reliable, and valid identification of individuals. DHS seeks to expand biometric collection for "identity enrollment, verification, and management . . . ; national security and criminal history background checks; the production of secure identity documents; and to perform other functions related to administering and enforcing the immigration and naturalization laws." Each of these functions can only be accomplished if the biometric identifiers accurately, validly, and reliably identify individuals. But, as described below, scientific studies show that existing technologies for gathering faceprints, voiceprints, and iris scans are flawed, error-prone, and far more complicated than fingerprinting. Importantly, the misidentification rates are higher for people of color.

The risks of false positives and negatives in this context are serious—database or human matching errors can result in the wrongful detention or deportation of people lawfully in the United States, and wrongful arrests for criminal charges. Indeed, at least two Black men have already been falsely identified by facial recognition in Detroit, leading to their wrongful arrests for crimes they did not commit.[19]

Even if a false positive or negative is not dispositive because individuals are offered an opportunity to rebut adverse decisions based on derogatory information, it may prove troublingly influential. Research conducted by the National Institute of Standards and Technology (NIST) and others has shown that people are likely to believe computer-generated results, and that those who are not specially trained in face recognition are poor at identifying people they do not

[19] Elisha Anderson, *Controversial Detroit facial recognition got him arrested for a crime he didn't commit*, Detroit Free Press (Jul. 10, 2020), https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/.

know,[20] even if they perform face identifications as part of their daily work.[21] Even trained facial specialists misidentify subjects about 10% of the time.[22] It is also entirely unclear how an individual can correct an error once it is introduced into the system—not for a particular adjudication, but for their "person-centric" record more broadly.

The new proposed modalities are not reliably accurate. For example, face recognition systems "vary in their ability to identify people, and no system is 100 percent accurate under all conditions."[23] A number of researchers, including a Senior Level Photographic Technologist for the FBI, have reported that face recognition algorithms misidentify Black people, young people, and women at higher rates than white people, older people, and men, respectively.[24] According to a comprehensive study by NIST, African American and Asian people are up to 100 more times likely to be misidentified by a face recognition system than white men, depending on the algorithm and use case.[25] As noted by a 2018 MIT study, face recognition algorithms are trained on datasets "overwhelmingly composed of lighter-skinned subjects," making them far less effective at identifying those with darker skin pigmentation.[26] Higher rates of inaccuracy on darker skin pigmentations have also been noted in products marketed by private companies,

ACLU
AMERICAN CIVIL LIBERTIES UNION

[20] John J. Howard *et al.*, *Human-algorithm teaming in face recognition: How algorithm outcomes cognitively vias human decision-making*, PLoS ONE (2020), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0237855; P. Jonathon Phillips et al., *Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms*, 115 PNAS 6171 (June 2018), https://www.pnas.org/content/115/24/6171; David White, et al., *Error Rates in Users of Automatic Face Recognition Software*, PLoS One (2015), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0139827 (noting participants made over fifty percent errors for adult target faces).

[21] White, *supra* note 20 (finding equivalent performance between untrained examiners and passport officers).

[22] Phillips, *supra* note 20.

[23] Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, Electronic Frontier Foundation 6 (May 2019) https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf.

[24] *See, e.g.*, P. Jonathon Phillips, *et al.*, *An Introduction to the Good, the Bad, & the Ugly Face Recognition: Challenge Problem*, Proceedings, Ninth International Conference on Face and Gesture Recognition 346 (Mar. 2011), https://ieeexplore.ieee.org/document/5771424 (noting only fifteen percent accuracy for face image pairs that are "difficult to match"); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[25] *See* Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*, Washington Post (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-manyfacial-recognitionsystems-casts-doubt-their-expanding-use/.

[26] Buolamwini, *supra* note 24.

including Amazon, Microsoft, and IBM.[27] And many face recognition algorithms also misgender transgender and gender nonconforming people.[28] Additional sources of bias are introduced when face recognition systems rely on digital camera images because, when taking photos of faces with darker skin pigmentation, the cameras fail to provide the degree of color contrast that the algorithms need to produce and match faceprints.[29]

Iris scanning is also imperfect. According to NIST, the best current technology falsely misidentifies a non-match about 1 in 175 times, and the error rates are higher for Asian and Black people than white people.[30] Depending on the precise technology used, error rates also differ by gender and eye color.[31] In addition, according to NIST, relying on iris scanning to confirm an identity established at one location at another location—that is, the point of the Proposed Rule's biometric collection—"is generally recognized to be more difficult" than for fingerprint scanners because "the eye/iris is a more complicated structure" and cannot be captured in two dimensions.[32]

The accuracy of voiceprints similarly varies "considerably depending on how closely the conditions of the collected voice match those of previous recordings"; voiceprints are most accurate where there is "low background noise, a familiar acoustic environment, and good signal quality."[33] "[T]he performance gap . . . remains relatively large" depending on whether individuals are using Public Switched Telephone Networks or Voice over Internet Protocol, and the same or different phone number.[34] In the use cases envisioned by the Proposed Rule—for example, calls from remote locations—such conditions are impossible to guarantee.[35] These avenues for error call the utility of relying on—and

---

[27] Tom Simonite, *Photo Algorithms ID White Men Fine—Black Women, Not So Much*, Wired (Feb. 6, 2018), https://www.wired.com/story/photo-algorithms-id-white-men-fineblack-women-not-so-much/.

[28] Taylor, *supra* note 9.

[29] Georgetown Law Center on Privacy & Technology, *The Perpetual Line-Up* 54 (Oct. 18, 2019), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf.

[30] George Quinn, Patrick Grother, & James Matey, Performance of Iris Recognition Algorithms, 89 (Apr. 18, 2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8207.pdf.

[31] *Id.*

[32] James Mately, *et al.*, *Iris Cameras: Standards Relevant for Camera Selection – 2018*, Nat'l Inst. of Standards and Technology (2018), https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2018.pdf.

[33] Kofman, *supra* note 10.

[34] Seyed Omid Sadjadi, *et al.*, *The 2019 NIST Speaker Recognition Evaluation CTS Challenge* (2019), https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=929506.

[35] UNICEF, *Guidance on Assessing the Value of Including Biometric Technologies in UNICEF-supported programs* (July 2019), https://data.unicef.org/resources/biometrics/#; Carsten

therefore amassing a database of—voiceprints into serious question. And voiceprints will simply be irrelevant in the vast number of instances where applicants' or sponsors' translators or attorneys are calling the government on their behalf.

In addition, children's speech is generally more challenging for voiceprinting technology, raising additional questions about requiring children who are younger than fourteen to submit to biometric collection.[36] In fact, children's biometrics are generally less useful and reliable than biometrics collected from adults, making DHS' collection of biometrics from those under age fourteen particularly gratuitous.[37]

Limited pilot studies have also raised concerns about the accuracy of Rapid DNA machines, including their failure to produce usable profiles, contamination of samples due to leaks in the machine, and the generation of at least one faulty profile.[38]

The collection of photographs of scars, marks, and tattoos ("SMT biometrics") also has no clear value or connection to the sponsor verification process.[39] Such characteristics—known as "soft biometrics"—are far more subjective as unique identifiers, and their accuracy is not well established.[40]

In addition, the inaccuracy rate of biometric identification often increases with the size of a biometrics database, casting further doubt on the utility of a mass biometric database. Face recognition systems can already be extremely poor at accurately finding matches when searching against a large database of images, in part because so many people within a given population look similar to one

---

Gottschlisch, *et al.*, *Modeling the growth of fingerprints improves matching for adolescents*, 6 IEEE Transactions on Information Forensics and Sec. 1165 (Sept. 2011), http://www.stochastik.math.unigoettingen.de/preprints/ModelingTheGrowthOfFingerprintsImprovesMatching.pdf.

[36] Brad Story & Kate Bunton, *Format measurement in children's speech based on spectral filtering*, 76 Speech Communication 93 (Feb. 2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4743040/pdf/nihms741352.pdf.

[37] *See, e.g.*, *supra* note 35.

[38] Adam Bennett, *Rapid DNA technology gets mixed reviews in Houston*, KHOU (Feb. 17, 2019), https://www.khou.com/article/news/local/rapid-dna-technology-gets-mixed-reviews-in-houston/285-0ff53cff-a631-44a3-8961-bd3b021f9f63.

[39] *See* Jung-Eun Lee, Anil K. Jain, & Rong Jin, *Scars, marks and tattoos (SMT): Soft biometric for suspect and victim identification*, 2008 Biometrics Symposium (Sept. 2008), https://ieeexplore.ieee.org/document/4655515.

[40] *See id.;* Hu Han & Anil K. Jain, *Tattoo Based Identification: Sketch to Image Matching*, 6th Int'l Conf. on Biometrics (June 2013), https://ieeexplore.ieee.org/document/6613003/authors#authors (explaining that "a tattoo is not a unique identifier").

another.[41] And the "false-positive risk inherent in large facial recognition databases could result in even greater racial profiling by disproportionately shifting the burden of identification onto certain ethnicities."[42] For certain biometrics, like DNA profiles, the fact that accuracy diminishes as the database grows has led the government to collect increasingly privacy-invasive versions of the biometric.[43]

Thus, the use of these additional biometric modalities, including facial recognition, may increase the risk of false positives and false negatives, making applicant and sponsor identity verification *less*, rather than more, accurate.

Collection of biometrics from children under fourteen years of age is also likely to add to, rather than lessen, administrative complexities, given that children under fourteen remain exempt from biometric collection for applications submitted with DOJ EOIR. This not only highlights the lack of necessity and justification for collecting biometrics from children, but it is also likely to create confusion regarding whether or not a specific child must submit to biometric collection.

These administrative complexities and risks of error will have grave consequences. Because misidentification can lead to the denial of essential benefits, the separation of families, and significant barriers to livelihoods—not to mention the deprivation of liberty if the misidentification is shared with law enforcement—relying on biometric technologies is especially dangerous.

III. The increased biometric collection is not justified by the government's stated goals.

Given the privacy and security interests implicated by increased biometric collection, any additional collection of biometric information must, at a minimum, be justified and necessary for a particular government purpose. The Proposed Rule—which flips the Department's current presumption from one of requiring justification for any collection to presuming that all collection is authorized from all relevant actors for all benefits—fails this standard by definition.

---

[41] *See, e.g.*, Adrienne LaFrance, *The Ultimate Facial-Recognition Algorithm*, The Atlantic (June 28, 2016), https://www.theatlantic.com/technology/archive/2016/06/machine-face/488969.

[42] *What Facial Recognition Technology Means for Privacy and Civil Liberties, Hearing Before the S. Comm. On the Judiciary Subcomm. on Privacy, Technology, and the Law*, 112th Cong. (2012) (Written Testimony of Jennifer Lynch, Staff attorney with the Electronic Frontier Foundation), https://www.eff.org/files/filenode/jenniferlynch_eff-senate-testimonyface_recognition.pdf.

[43] *See* FBI, *Planned Process and Timeline for Implementation of Additional CODIS Core Loci*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis (last visited Oct. 13, 2020); *see also* Douglas R. Hares, *Expanding the CODIS core loci in the United States*, 6 Forensic Sci. Int. Genet. e52 (2012) (describing the Scientific Working Group on DNA Analysis Method's determination that "reduc[ing] the likelihood of adventitious matches as the number of profiles stored at[the National DNA Index System] continues to increase each year" was a major reason for "expanding the CODIS core loci").

In addition, the justifications that DHS has set forth for flipping this presumption are insufficient. First, in cases where identity verification of sponsors and adult household members is required, it is not necessary to collect more than one biometric identifier. DHS has not provided any evidence that its current collection of photographs, signatures, and/or fingerprints does not suffice or has led to misidentification problems (much less major problems). Fingerprint collection is less intrusive, has more established standards for accuracy, and a fingerprint can positively identify an individual whose fingerprints are already enrolled in a database. Collecting multiple biometrics in such a circumstance is disproportionate and unnecessary.

Through footnotes, the Proposed Rule seems to suggest that fingerprints are insufficient because the Department's fingerprint records are incomplete and because its historical fingerprint enrollment records have included individuals with multiple identities[44]—but such mismanagement in the government's current biometrics collection is, if anything, a caution against, rather than a justification for, significantly expanding the universe of the Department's biometrics collection. If the government's current collection of fingerprints has been managed poorly or is missing data, the solution is *not* to authorize the collection of several new biometric modalities that could suffer from the same problems; rather, the solution is to address any issues with existing systems.

In addition, the purported justification for iris scans in addition to fingerprints—that some individuals cannot submit fingerprints due to loss of fingers, hand amputation, normal wear, and deliberate eradication—is neither supported by any data, nor a sufficient justification for collecting iris scans from those individuals for whom fingerprints can be obtained.

The Proposed Rule's justification for collecting palmprints is equally unpersuasive and perhaps even more troubling. DHS seeks to collect palmprints because "capturing and scanning latent palm prints is becoming an area of increasing interest among the law enforcement community." The only existing database of palmprints that the Proposed Rule mentions includes palmprints lifted from crime scenes, not prints connected with a verified identity or linked to past criminal convictions. It is entirely unclear how checking against that database could serve DHS' supposed goals, rather than a generalized law enforcement function that is outside the scope of DHS' identity verification function. Forced collection of palmprints for law enforcement purposes without suspicion of wrongdoing is constitutionally impermissible.

The justification for collecting faceprints—that they can aid DHS in detecting fraud, and conducting public safety, criminal history, and national

[44] Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 Fed. Ref. 177 (proposed September 11, 2020) at 56351, n.26.

security background checks—is undercut both by the inaccuracies of faceprinting technology, discussed above, and the fact that such purposes, to the extent that they are proper, can already be accomplished by fingerprint collection.

The Proposed Rule's justification for collecting voiceprints—that it would improve the efficiency of call center processes, could be used for electronic verification, and could be used for identity verification in remote locations—ignores the reality of voiceprint technology, as discussed above. It also ignores the reality of calls by applicants to DHS, which often involve lawyers and translators whose voiceprints will not match those of the applicants.

In addition, the proposed purpose of collecting raw DNA, partial DNA profiles, and DNA test results stating the probability of a genetic relationship is misguided. Requiring DNA collection and testing for family-based benefits is nonsensical because the relevant relationship for such benefits is *familial*, not genetic—while some of these relationships may also be biological, many are not (such as petitions on behalf of spouses or adopted children). Even for some relationships, such as parent-child relationships, not all such relationships are biological (as described above). Collecting information that is orthogonal to the actual question is likely to complicate, rather than streamline, application processes. Moreover, noncitizens have long proven the relationships required for family-based benefits without the use of DNA, including through the use of documentation the government currently reviews. Accordingly, requiring submission of DNA is not necessary and, as noted above, it raises serious privacy concerns.

The Proposed Rule's DNA collection does not meet the requirement of being necessary to verify a legitimate, good-faith concern about parentage.[45] After the ACLU filed a federal lawsuit successfully challenging the Trump administration's family separation policy, for example, the administration proposed using DNA testing to reunite families it had ripped apart. Even under those circumstances, the court ruled that a DNA test must only be used as a last resort when there is genuine reason to doubt parentage, no less intrusive method would be effective to confirm it, and the collected DNA must be destroyed after its use.[46] Similarly, even when DNA testing is the last resort, there is no justification for DHS retaining or sharing the raw DNA or even the partial DNA profile, given that the relevant result is not the profile, but the probability of a genetic relationship.

Finally, DHS asserts that it must collect biometrics from U.S. citizens and lawful permanent residents filing for a family-based immigrant visa petition or K

---

[45] Order Following Status Conference, *Ms. L v. United States Immigration and Customs Enforcement*, Case No. 18cv0428 (S.D. Cal. Jul. 10, 2018), ECF 101.

[46] *Id*., *see also* Joint Status Report Regarding Suitability Process for Release of UAC to Potential Plaintiffs in the General Public at 7–8, *Ms. L*, Case No. 18cv0428 (S.D. Cal. Jul. 9, 2018), ECF 96.

nonimmigrant fiancée petition in order to comply with the Adam Walsh Child Protection and Safety Act of 2006 and the International Marriage Broker Regulation Act, which requires conviction information for certain crimes. This collection—particularly when paired with the Proposed Rule's insufficient limitations on data sharing, discussed below—burden individuals' constitutional right to informational privacy under the Fourth and Fifth Amendments. The Proposed Rule entirely fails to provide evidence suggesting that existing name-based background checks and information submitted under penalty of perjury have been insufficient for DHS' purposes, and this expanded collection appears unwarranted. If anything, congressional testimony from Daniel M. Renaud, USCIS's Associate Director for Field Operations regarding fiancée visa fraud, suggests that existing safeguards and checks suffice.[47] Current law requires the disclosure of the relevant crimes, but the proposed biometric collection would reveal information far beyond that.

ACLU
AMERICAN CIVIL LIBERTIES UNION

DHS also claims that biometric collection from regional center principals under the EB-5 program would help DHS determine if they are capable of credibly promoting the requisite economic growth. Requiring the submission of a long list of biometrics is completely disproportionate to this purported need. The only effect of such biometric collection will be to either 1) deter sponsors from availing themselves of government benefits they are entitled to, or 2) subject them to prolonged surveillance and the risk of misuse or breach of their sensitive biometric information as a condition of availing themselves of government benefits.

The proposed biometric collection is unnecessary and unjustified. For that reason alone, it is improper.

IV. The Proposed Rule lacks key details that are essential to public evaluation of the proposed biometric collection.

Finally, the Proposed Rule is insufficient and premature. While numbering more than 90 pages, it fails to set forth key details, including a comprehensive and specific list of the particular biometric modalities DHS intends to collect—for example, the particular types of DNA tests, faceprints, voiceprints, and iris scans—much less the particular technologies and/or private vendors upon which it will rely. This lack of specificity leaves important questions about privacy and accuracy unanswerable.

---

[47] *Vows for Visas: Investigating K-1 Fiancé Fraud: Hearing Before the S. Judiciary Comm.*, 115th Cong. (2017) (written testimony of Daniel Renaud, Associate Director of Field Operations, USCIS; Donald Neufeld, Associate Director of Service Center Operations, USCIS; and Matthew Emrich, Associate Director of Fraud Detection and Nat'l Security, USCIS), https://www.judiciary.senate.gov/imo/media/doc/031517%20Renaud,%20Neufeld,%20Emrich%20Joint%20Testimony.pdf.

In addition, the Proposed Rule fails to set forth where and how all of this information will be stored, as well as any limitations on retention, sharing, and access. The Proposed Rule states only that DHS is bound by the confidentiality provisions that apply to victim-based immigration benefits, but it is not clear what, if any, restrictions DHS will impose on biometrics gathered in relation to other benefits.

The details that are known about the Proposed Rule's data-sharing are troubling. For example, the Proposed Rule contemplates sharing biometric identifiers with foreign governments "in accordance with international arrangements." Many individuals who would be subject to biometrics collection under the Proposed Rule are survivors of violence and trafficking who have fled to the United States for safety. This could place immigrants, including asylum seekers, in danger by exposing their biometric information to the very foreign government they have sought to escape. Furthermore, once sensitive biometrics information is shared with foreign governments, DHS will no longer have control over how those biometrics are used and shared by those governments. Therefore, DHS cannot assure that any biometrics it collects will not be used or misused for purposes far outside those contemplated in the Proposed Rule.

Additionally, the Notice of Proposed Rulemaking ignores DHS's statutory duty to complete a Privacy Impact Assessment (PIA) regarding the Department's proposed rulemakings that affect personally identifying information (PII). According to DHS's Privacy Policy Guidance Memorandum, Section 208 of the E-Government Act of 2002, Public Law 107-347; 44 U.S.C. Ch 36, "requires PIAs of all information technology that uses, maintains, or disseminates personally identifiable information or when initiating a new collection of PII from ten or more individuals in the public."[48] In the Notice of Proposed Rulemaking, DHS does not directly address the need to conduct a PIA, but rather sidesteps the question, claiming that although there "could be some unquantified impacts related to privacy concerns for risks associated with the collection and retention of biometric information [...] this rule would not create new impacts in this regard but would expand the population that could have privacy concerns."[49]

This statement reflects both a fundamental misunderstanding of the nature of the biometric collection DHS proposes and a flouting of the agency's statutory duty to conduct a PIA. The claim that the additional biometric collection proposed in the NPRM merely expands the group of people from whom PII is collected is patently false; even members of the public currently subject to certain limited biometric collection would, under this rule, be subject to a wide array of new

[48] *See* Department of Homeland Security, Memorandum Number: 2008-02, Privacy Policy Guidance Memorandum, available at https://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-02_0.pdf (last visited Oct. 13, 2020).

[49] Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 Fed. Ref. 177 (proposed September 11, 2020) at 56343.

forms of biometric identification, including but not limited to DNA collection. Further, DHS's statement *concedes* that the Proposed Rule would expand the population that could have privacy concerns about biometric collection, thus implicating its statutory duty to conduct a PIA. In fact, the NPRM states that the proposed rule would apply to approximately 2.17 million new people,[50] well over the ten or more individuals which would necessitate a PIA. At minimum, DHS needs to conduct a full PIA consistent with its statutory obligations and to comply with its stated policy objectives of informed decision making, life cycle management, transparency, and accountability.[51]

* * *

We therefore urge the Department to rescind the Proposed Rule. If you have any questions, please contact us at veidelman@aclu.org.

Sincerely,

American Civil Liberties Union

American Civil Liberties Union of Illinois

American Civil Liberties Union of Massachusetts

American Civil Liberties Union of San Diego & Imperial Counties

American Civil Liberties Union of Washington

[50] *Id.*

[51] *See* DHS Memorandum 2008-02, *supra* note 48, at 2.