HARVARD IMMIGRATION AND REFUGEE CLINICAL PROGRAM

6 Everett St., Suite 3103
Cambridge, MA 02138
hirc@law.harvard.edu
(617) 384-8165

October 13, 2020

Kenneth T. Cuccinelli
Acting Director
U.S. Citizenship and Immigration Services
Department of Homeland Security
20 Massachusetts Ave. NW
Washington, DC 20529-2240

VIA REGULATIONS.GOV

Re: Request for Comment on Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 Fed. Reg. 56338, Docket No. USCIS-2019-0007

To Whom It May Concern,

The Harvard Immigration and Refugee Clinical Program ("HIRC") at Harvard Law School submits this comment[1] in response to the U.S. Citizenship and Immigration Services ("USCIS") and the Department of Homeland Security ("DHS") request for comments on Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 Fed. Reg. 56338 (Sept. 11, 2020) ("the Rule").

We, the signatories of this letter, are immigration lawyers and academic clinicians. One of the oldest clinical programs in the country, HIRC focuses on the advancement of immigrants' rights while teaching students important lawyering skills. HIRC includes two distinct clinics that represent individuals seeking asylum and other humanitarian protections, some of whom have criminal convictions. The Immigration & Refugee Advocacy Clinic represents clients seeking humanitarian protections in a range of different fora, including administrative tribunals and federal appellate courts. The Crimmigration Clinic is the first and only clinic of its kind that focuses on the growing intersection of criminal law and immigration law. HIRC faculty and staff also teach a range of courses concerning immigration policy, refugees and trauma, the intersection of immigration law and labor law, and the intersection of criminal law and immigration law. They also regularly publish scholarship concerning asylum adjudication, due process protections in removal proceedings, working with traumatized refugees, crimmigration, and immigration detention. HIRC has also submitted numerous administrative comments and *amicus curiae* briefs on issues of importance to immigrant populations.

[1] HIRC thanks the Harvard Law School Cyberlaw Clinic for its assistance in drafting this comment.

DHS and its component agencies already have significant investigative and information collection powers and have not justified their need to expand these powers. On the other hand, the potential for harm from such extensive biometric surveillance is great. The Rule would create a national system of biometric data that would be ripe for abuse by the government. Indeed, the proposed Rule raises serious Constitutional concerns. These harms would be felt disproportionately by vulnerable populations, such as refugees, survivors of violence, and minors, and would be amplified by the unreliability of biometric technologies writ large.

HIRC does not believe these harms can be mitigated by piecemeal redrafting of the Rule. Because the harms posed by this rule clearly outweigh the government's interests, HIRC asks that DHS abandon the Rule in its entirety.

I. DHS already has significant investigative and information collection powers and has not presented a clear rationale for expanding them.

The Rule proposes to increase DHS's biometric data collection powers in three major ways. First, whereas DHS's current system allows for biometric data collection on an as-needed basis, the Rule would make data collection the default for nearly every individual touched by the immigration system, in some cases including U.S. citizens and permanent residents.[2] Second, the Rule would drastically expand the types of biometric data DHS already collects to include palm prints, voice prints, iris images, and, for those claiming genetic relationships, DNA test results.[3] Finally, the Rule would strip current exemptions for minors under the age of fourteen from the biometric data collection process; instead, biometric data from children as young as newborn infants could be collected and stored indefinitely.[4]

DHS provides only a thin justification for such a sweeping expansion of its own power, relying on a handful of administrative directives and some self-serving statements that the current biometric system is outdated.[5] Indeed, DHS's current authority to collect biometric data is significant. DHS claims "the authority to collect biometrics from any applicant, petitioner, sponsor, beneficiary, requestor, or individual filing or associated with a request."[6] This biometric data—which includes photographs, signatures, and fingerprints[7]—is required for certain benefit requests and enforcement actions. [8] Even in cases where biometric data collection is not compulsory, DHS may collect such data after making an individualized determination followed by proper notice.[9]

While DHS proposes making DNA testing compulsory where genetic relationships are claimed, DHS fails to show why the ample mechanisms already in place to prove familial relationships—

---

[2] 85 Fed. Reg. at 56,338.
[3] *Id*.
[4] *Id*.
[5] *See id.* at 56,348.
[6] *Id.* at 56,340.
[7] *Id.*
[8] *Id.* at 56,350.
[9] *Id.*

including voluntary submission of DNA testing results—are suddenly inadequate. DHS requires "documentary evidence such as marriage and birth certificates, and secondary evidence such as medical records, school records, religious documents, and affidavits to support claims based on familial relationships."[10] Where documentation is not enough, DHS accepts DNA test results to establish familial connections.[11] But the proposed Rule, which makes DNA testing the default method for proving genetic relationships, leaves immigrants, including children, with no meaningful choice other than to submit their sensitive genetic information to a government agency with no guarantees about how it will be used in the future.

Indeed, according to guidance from the government itself, DHS's proposed policy of generalized data collection presents considerable privacy risks in both the immediate and the long-term future.[12] DHS's own proposal indicates that it "plans to implement a program of continuous immigration vetting, and require that aliens be subjected to continued and subsequent evaluation to ensure they continue to present no risk of causing harm subsequent to their entry."[13] This extends well beyond the overall picture DHS paints of using data principally for identity verification and point-in-time background checks to comply with its statutory duties and protect national security.

DHS attempts to justify a compulsory data collection scheme by saying the current system is "outdated" because benefit request adjudication and immigration law enforcement "include verifying identity and determining whether or not the individual poses a risk to national security or public safety."[14] However, DHS does not explain why current, already-intrusive modes of data collection such as fingerprinting, photographs, documentation, and criminal background checks are no longer adequate for identity verification and risk assessment. Indeed, in characterizing current practices as "outdated," DHS puzzlingly cites to authorities that indicate that DHS is failing to make the most of its existing fingerprint data—hardly a strong argument for collecting additional biometrics.[15]

The unsupported arguments that DHS makes in order to support the Rule do not justify the establishment of a mass database of millions of people's biometric information. Currently, immigrants make up about 13.7%—or 1/7th—of the U.S. population.[16] Under the proposed Rule, DHS would have access to a wide range of biometric information for every new immigrant, regardless of their age or agency, as well as for some U.S. citizens and lawful permanent residents.[17] Yet, in all 85 pages of its proposed Rule, DHS fails to provide any convincing reason for expanding its power to this extent.

---

[10] *Id.* at 56,353.
[11] *Id.*

[12] U.S. Dep't of Justice, *Privacy and Information Quality Risks: Justice Agency Use of Biometrics, available at* https://www.it.ojp.gov/documents/d/biometrics%20flyer_v2.pdf (last visited Oct. 12, 2020).
[13] 85 Fed. Reg. 56,352.
[14] *Id.* at 56,342.
[15] *Id.* at n.26.
[16] Abby Budiman, *Key Findings About U.S. Immigrants*, PEW RESEARCH CENTER (Aug. 20, 2020), https://www.pewresearch.org/fact-tank/2020/08/20/key-findings-about-u-s-immigrants/.
[17] 85 Fed. Reg. 56,358.

While there is no clear rationale for DHS to expand its biometric collection powers under the Rule, there are ample arguments against it. These arguments include, among others, the potential for misuse of biometric data as a general law enforcement tool; the illegality of mass biometric surveillance of a subset of the population; the undue impact on vulnerable groups such as refugees, survivors of violence, and minors; and the invasive, unreliable nature of biometric technologies in general.

II. The Rule would create an immense database of individuals' most personal data that is ripe for abuse by DHS and other law enforcement agencies.

Even without the proposed Rule going into effect, DHS already maintains "the largest biometric repository in the U.S. government."[18] This system, known as the Automated Biometric Identification System ("IDENT") currently holds more than 260 million unique identities and processes more than 350,000 biometric transactions per day.[19] If this rule were to go into effect, DHS's data collection practices would vastly expand the type of information collected and stored in IDENT while extending the program to millions of new individuals. Although DHS may claim that "is not proposing an absolute biometrics collection requirement,"[20] the amount of discretion it reserves for itself in the Rule gives it the power to implement just such a program without any subsequent public review.

Such a massive expansion in the IDENT system is disturbing for several reasons: (1) it could enable and promote additional mission creep by DHS into the realm of ordinary law enforcement functions; (2) information collected could be utilized by state, local, and federal law enforcement agencies with little public oversight; and (3) it is inherently unfair to allow law enforcement agencies to conduct operations using a database that contains only a specific subset of the population.

First, this program threatens to enable significant mission creep by DHS. As discussed above, DHS has plainly indicated that it plans to segue from use of biometrics for identity verification and background checks to a more invasive program of "continuous vetting" for immigrants.[21]. Recent history shows that DHS and its component agencies frequently overstep their authority and engage in prohibited law enforcement functions. For example, the Supreme Court has made it clear that permanent immigration checkpoints may not be used for drug-search or other law enforcement efforts.[22] However, civil rights groups have documented numerous violations of this

[18] Department of Homeland Security, *Biometrics* (Jul. 13, 2020), https://www.dhs.gov/biometrics.
[19] *Id.*
[20] 85 Fed. Reg. at 56,340.
[21] "DHS also plans to implement a program of continuous immigration vetting, and require that aliens be subjected to continued and subsequent evaluation to ensure they continue to present no risk of causing harm subsequent to their entry." *Id.*
[22] *See United States. v. Martinez-Fuerte*, 428 U.S. 543, 566–67 (1976) (holding that such stops are not unconstitutional to the extent that they involve only brief questioning, but that "[a]ny further detention must be based on consent or probable cause" (quoting *United States v. Brignoni-Ponce*, 422 U.S. 873, 882 (1975)).

limitation by Customs and Border Patrol ("CBP") officers.[23] Likewise, the Supreme Court has expressly found that stops and searches by "roving patrols" of CBP officers are not permitted without probable cause, yet these too continue to occur.[24] Whether these violations are intentional or merely the result of poor training practices, they infringe on individuals' rights. The creation of a massive database of biometric information would provide countless new opportunities for DHS to violate the law, particularly when coupled with a "continuous vetting" program. This Rule should be barred from taking effect to limit these opportunities.

Second, concerns over abuse of the system by law enforcement are exacerbated by the numerous data-sharing agreements that DHS has signed with nearly a thousand state, local, and federal law enforcement agencies.[25] A set of self-imposed "advanced data filtering and privacy controls" are all that protect individuals' data from being shared broadly with other federal agencies such as the Department of Justice.[26] The need for consistent management and privacy practices is especially clear in this instance: once collected, biometric data can identify a person for life. DHS should not be able to control the biometric data of hundreds of millions of individuals without clearer rules for how it can be shared with law enforcement agencies.[27]

Third, it is inherently unfair that this program will create an extensive database of biometric information belonging to only a subset of the population: immigrants, foreign nationals, and others with ties to them. Because IDENT will contain primarily information from this sizable minority, the Rule would increase existing disparities in the application of justice along racial or national lines. Such disparities are even more troubling viewed in light of the likelihood, outlined above, that access to collected biometric information will expand over time.

---

[23] *See e.g.,* JAMES LYALL, JANE YAKOWITZ BAMBAUER & DEREK E. BAMBAUER, RECORD OF ABUSE: LAWLESSNESS AND IMPUNITY IN BORDER PATROL'S INTERIOR ENFORCEMENT OPERATIONS 14–15 (2015), https://www.acluaz.org/sites/default/files/documents/Record_of_Abuse_101515_0.pdf; Gilles Bissonnette, *State Judge Finds New Hampshire Border Patrol Checkpoint Unconstitutional,* AMERICAN CIVIL LIBERTIES UNION (May 9, 2018, 1:45 PM), https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/state-judge-finds-new-hampshire-border-patrol

[24] *See Almeida-Sanchez v. United States*, 413 U.S. 266, 269 (1973) ("Automobile or no automobile, there must be probable cause for the search."); Bob Ortega, *Border Patrol hit with Abuse Complaints*, USA TODAY (Oct. 9, 2013), https://www.usatoday.com/story/news/nation/2013/10/09/border-patrol-abuse-complaints/2954559/

[25] George Joseph, *Where ICE Already has Direct Lines to Law-Enforcement Databases with Immigrant Data*, NPR (May 12, 2017, 1:44 PM), https://www.npr.org/sections/codeswitch/2017/05/12/479070535/where-ice-already-has-direct-lines-to-law-enforcement-databases-with-immigrant-d. Although the program has evolved since this article was published, it still consists of the same regional partnerships. The program therefore likely has a similar reach today.

[26] Department of Homeland Security, *Biometrics* (July 13, 2020), https://www.dhs.gov/biometrics.

[27] The Privacy Act of 1974 and associated privacy impact assessments provide only limited protections in this case. The Privacy Act covers only citizens and permanent residents, leaving millions of those affected by this rule unprotected. 5 U.S.C. § 552a(a)(2) (defining "individuals" under the Act). Privacy impact assessments may provide some transparency, but the most affected group—immigrants who have not yet gained citizenship or permanent residency—are poorly positioned to act on such disclosures.

III. The harms posed by the Rule are even greater for vulnerable populations within the immigration system, such as refugees, survivors of violence, and minors.

If history is any guide, the biometric data gathered under this Rule will not be used equally against all immigrants, but rather selectively against those from certain nations, ethnicities, and religions. President Trump's 2017 Proclamation banning certain immigrants from primarily Muslim-majority countries is evidence of the way immigration policies may be used selectively to target certain groups.[28] The biometric data collected under this Rule could be used to harm vulnerable groups in insidious ways: by invading their privacy and preventing them from seeking safety in the U.S. at all.

The proposed collection of minors' biometric data is one striking example of DHS's overreach in this Rule. Minors are recognized as a particularly vulnerable population, and their privacy is viewed as especially important. Congress has passed at least four major laws intended to protect minors' privacy rights: the Children's Internet Protection Act (CIPA), the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Rule (COPPA), and the Protection of Pupil Rights Amendment (PPRA).[29] These laws define "child" differently, with some applying to children under 13 and some protecting children up to 17. COPPA applies to children under 13 outside of the U.S. so long as companies subject to the law are U.S.-based, which serves as evidence of Congress's intent to protect even those young children who are not U.S. citizens.[30]

Yet with this Rule, DHS proposes to collect biometric information from all children—no matter how young they are and how little say they have in the process. While under the PPRA the U.S. Department of Education is prevented from knowing minors' political affiliations and religious practices, under this Rule DHS would have access to minors' sensitive biometric information, with no guarantee that it would not be stored for the rest of those minors' lives.

Victims of abuse are also particularly vulnerable when it comes to data collection and surveillance.[31] In 2019, "USCIS granted immigration relief to more than 25,000 individuals, including victims of trafficking, crime and Violence Against Women Act (VAWA) recipients."[32]

---

[28] Proclamation 9645 of September 24, 2017, https://www.federalregister.gov/documents/2017/09/27/2017-20899/enhancing-vetting-capabilities-and-processes-for-detecting-attempted-entry-into-the-united-states-by.

[29] DEPARTMENT OF EDUCATION, OFFICE OF EDUCATIONAL TECHNOLOGY, *Privacy*, https://tech.ed.gov/privacy/ (last visited Oct. 12, 2020).

[30] FEDERAL TRADE COMMISSION, *Complying with COPPA: Frequently Asked Questions*, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0#A.%20General%20Questions (last visited Oct. 12, 2020).

[31] HIRC also objects to the Rule's proposed modifications to immigration relief, including its proposal to eliminate the presumption of "good moral character" for VAWA and T-visa beneficiaries under the age of 14, who are by definition victims of battery, extreme cruelty, and/or trafficking. These children are frequently severely traumatized, and the agencies have not offered a reasonable explanation for imposing this new evidentiary burden.

[32] U.S. CITIZENSHIP AND IMMIGRATION SERVICES, *USCIS Final FY 2019 Statistics Available*, https://www.uscis.gov/news/alerts/uscis-final-fy-2019-statistics-available (last visited Oct. 12, 2020).

To qualify as a VAWA recipient, an individual must have been abused by a U.S. citizen spouse, parent, or child.[33] Abusers often use surveillance methods to track, stalk, and maintain control over their victims.[34] In instances where the victim is an immigrant, abusers may threaten their victims with reporting immigration violations—a method of abuse that VAWA was, in part, formulated to mitigate.[35]

DHS's proposed Rule undermines the purposes of VAWA and will likely prevent otherwise-eligible VAWA petitioners from applying for immigration relief. DHS proposes to require VAWA recipients to submit biometric data instead of requiring local police clearance.[36] Further, the Rule proposes removing the presumption of good character for abuse victims under the age of 14—meaning that abused children will have to submit biometrics in order to flee their abusers.[37] Given victims' often traumatic relationship with surveillance, the threat of retraumatization through data collection alone will likely discourage VAWA applicants from coming forward.[38] On top of this, children, for whom seeking VAWA protection is already a remarkably courageous act, must overcome yet another burden on their way to securing permanent residence and citizenship in the United States.

For similar reasons, the proposed Rule threatens to discourage potential refugees, many of whom face threats from authoritarian surveillance in their home countries, from applying for protection in the U.S. This is only exacerbated by provisions in the proposed Rule that would permit DHS to share biometric data with foreign governments.[39]

If implemented, the Rule will have catastrophic effect for immigrants, especially the most vulnerable: children, abuse survivors, and refugees. With this Rule, DHS will introduce more difficulties and trauma into what, for many, is already a difficult and traumatic process.

IV. The Rule is especially suspect given the invasiveness and unreliability of biometric technologies.

While exposing a subset of the population to surveillance is a significant harm in its own right, biometric surveillance is especially concerning. First, biometrics are inherently invasive and jeopardize the privacy not only of individuals subject to surveillance but also their familial relations as well. Second, biometric technologies are often unreliable, biased, or both. History

---

[33] U.S. CITIZENSHIP AND IMMIGRATION SERVICES, *Battered Spouse, Children and Parents*, https://www.uscis.gov/humanitarian/battered-spouse-children-and-parents (last visited Oct. 12, 2020).
[34] Corinne Mason & Shoshana Magnet, *Surveillance Studies and Violence Against Women*, Surveillance & Society, (Sept. 4, 2012), https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/vaw/vaw.
[35] U.S. CITIZENSHIP AND IMMIGRATION SERVICES, *Battered Spouse, Children and Parents*, https://www.uscis.gov/humanitarian/battered-spouse-children-and-parents (last visited Oct. 12, 2020).
[36] 85 Fed. Reg. 56,342.
[37] *Id*.
[38] U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, *Tip 57: Trauma-Informed Care in Behavioral Health Services*, https://www.ncbi.nlm.nih.gov/books/NBK207195/ (2014).
[39] 85 Fed. Reg. 56,415.

has shown that limitations of and flaws in biometric technologies frequently become apparent years or even decades after those technologies are deployed.

Under existing regulations and procedures, DHS collects fingerprints, photographs, and—on a voluntary basis—DNA information. The Rule would not only expand the cases in which biometric information is gathered, making collection mandatory as opposed to discretionary, it would expand the modalities of biometric information collected.[40] Many of these modalities are particularly invasive. Combined with the "continuous immigration vetting" proposed under the Rule,[41] the result would be a surveillance state in which immigrants could be forced to justify their presence in the U.S. at any time, reminiscent of the widely criticized and largely unconstitutional "stop and profile" law in Arizona.[42]

The Rule purports to recognize the special sensitivity of DNA information, noting that DHS will not store raw DNA samples.[43] However, the Rule would permit DHS to retain partial DNA profiles and share those profiles with law enforcement.[44] It is well documented that people of color are over-represented in existing DNA databases, such as the FBI's Combined DNA Index System ("CODIS"), due to the discriminatory practices of federal, state, and local law enforcement agencies.[45] The proposed Rule would recreate the problems of CODIS for the immigrant population. Moreover, given the possibility of familial and partial DNA matching on stored DNA profiles, such a database would permit law enforcement to trawl for matches with the children, parents, and siblings of immigrants as well.[46] With the advent of new DNA matching techniques, more distant family relations may be implicated as well.

DNA is not the only problematic biometric modality proposed under the Rule. For example, the Rule would require DHS to collect images specifically for facial recognition.[47] When combined with other forms of video surveillance used by DHS, such as drones[48] and body cameras,[49] a database of facial recognition imagery would permit real-time monitoring of individuals' movements. Of course, this monitoring would only be effective against individuals in the

---

[40] 85 Fed. Reg. 56,355-56.
[41] *Id.* at 56,352.
[42] *See Arizona's Immigration Enforcement Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES, https://www.ncsl.org/research/immigration/analysis-of-arizonas-immigration-law.aspx (last updated July 28, 2011).
[43] 85 Fed. Reg. 56,354.
[44] *Id.*
[45] Jennifer K. Wagner, *DNA, Racial Disparities, and Biases in Criminal Justice: Searching for Solutions*, 27 ALB. L.J. SCI. & TECH. 95, 117 (2017).
[46] David H. Kaye, *The Genealogy Detectives: A Constitutional Analysis of "Familial Searching"*, 50 Am. Crim. L. Rev. 109, 118-19 (2013).
[47] Proposed Rule, 85 Fed. Reg. at 56,356.
[48] Jason Koebler, Joseph Cox, and Jordan Pearson, *Customs and Border Protection Is Flying a Predator Drone over Minneapolis*, VICE (May 29, 2020), https://www.vice.com/en/article/5dzbe3/customs-and-border-protection-predator-drone-minneapolis-george-floyd.
[49] Sidney Fussell, *Did Body Cameras Backfire?*, THE ATLANTIC (Nov. 1, 2019), https://www.theatlantic.com/technology/archive/2019/11/border-patrol-weighs-body-cameras-face-recognition/600469/.

database, namely immigrants. Other biometric modalities proposed under the Rule such as iris scans and voice prints are equally invasive. These technologies allow rapid identification of individuals and can be conducted remotely over a video or audio system.[50] It is easy to imagine this resulting in a system in which immigrants are subject to virtual "checkpoints" every time they access a government service via telephone or the internet. Combined with the use of biometrics in physical stops and checkpoints,[51] the result would be a system of near-constant surveillance—although, again, only for a subset of the population.

The dragnet surveillance proposed by the Rule is only worsened by the fact that many biometric technologies are or may prove to be biased and unreliable. This is famously the case with facial recognition technology, which is now widely known to have higher error rates on female faces and faces with darker skin.[52] This bias is so significant and difficult to correct that major facial recognition technology developers, including Amazon and IBM, are pausing or completely abandoning development of these tools.[53] Iris recognition technology suffers from similar bias, performing best on White people and worst on Asian people.[54] Voice recognition software performs worse on women[55] and individuals with accents.[56]

Moreover, some of the biometric modalities that would be collected under the Rule, such as voice prints and iris prints, are relatively new technologies. Time and time again, identification technologies appear to be accurate when first developed but, years later, turn out to be severely flawed. Take, for example, the FBI's use of microscopic hair comparison. After three decades of use, the FBI admitted that more than 90% of cases using this technique contained misrepresentations of evidence.[57] If DHS relies on biased, unreliable, or unproven biometric technologies, it may well find itself in a similar position in the future, having wrongfully excluded or deported thousands of immigrants. By adopting unproven technologies, DHS

---

[50] *See, e.g.*, NIST, *Video-based Automatic System for Iris Recognition (VASIR)*, https://www.nist.gov/services-resources/software/video-based-automatic-system-iris-recognition-vasir (last updated Nov. 15, 2019).
[51] Matt Cagle, *Why Are Border Sheriffs Rushing to Adopt Iris-Recognition Technology?*, ACLU (Aug. 30, 2017), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/why-are-border-sheriffs-rushing-adopt-iris.
[52] *See* Irina Ivanova, *Why Face-Recognition Technology Has a Bias Problem*, CBS NEWS (June 12, 2020), https://www.cbsnews.com/news/facial-recognition-systems-racism-protests-police-bias/.
[53] *Id.*
[54] *See* George W. Quinn, Patrick Grother, James Matey, National Institute of Standards and Technology, *IREX IX Part One Performance of Iris Recognition Algorithms*, NISTIR 8207 (April 2018), *available at* https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8207.pdf.
[55] Joan Palmiter Bajorek, *Voice Recognition Still Has Significant Race and Gender Biases*, HARVARD BUSINESS REVIEW (May 10, 2019), https://hbr.org/2019/05/voice-recognition-still-has-significant-race-and-gender-biases.
[56] Claudia Lopez Lloreda, *Speech Recognition Tech Is Yet Another Example of Bias*, SCIENTIFIC AMERICAN (July 5, 2020), https://www.scientificamerican.com/article/speech-recognition-tech-is-yet-another-example-of-bias/.
[57] *See* Press Release, *FBI Testimony on Microscopic Hair Analysis Contained Errors in at Least 90 Percent of Cases in Ongoing Review*, FBI (April 20, 2015), https://www.fbi.gov/news/pressrel/press-releases/fbi-testimony-on-microscopic-hair-analysis-contained-errors-in-at-least-90-percent-of-cases-in-ongoing-review.

undermines the purported justification for the Rule: more accurate immigration determinations (and suggests that DHS is, in fact, concerned first and foremost with surveillance, not accuracy).

Finally, even if DHS could demonstrate that the biometrics it seeks to collect were error free—an undertaking that science does not support—such a massive database of personal information would present an inherent security risk. Just last year, a security breach of a private biometrics database exposed facial image and fingerprint data on millions of users.[58] A similar breach of DHS's proposed database would disclose similar data, plus DNA profiles, iris images, voice prints, and more. While DHS may be confident in its ability to secure biometric data, recent events such as the breach of a CBP image database in 2019[59] show that it is far from immune to malicious or accidental disclosure of sensitive information. Again, this security risk is not shared equally by all residents of the U.S., but rather falls on the shoulders of immigrants, their families, and their sponsors.

The fact that DHS seeks to expand collection of biometrics despite these risks indicates that a lack of concern for immigrants' well-being, a failure to understand the technologies at play, or both.

V. The Rule raises serious Constitutional concerns.

In addition to being poor policy for all the reasons enumerated above, the proposed Rule raises serious Constitutional concerns. Specifically, the Rule infringes on the Fourth Amendment's right to be secure against unreasonable searches and seizures, as well as the Fifth Amendment's Due Process Clause.

With respect to the Fourth Amendment, the Supreme Court has found that there is a reasonable expectation of privacy in one's person, including in one's biometric information.[60] Furthermore, even though the means of collecting different types of biometrics vary in their invasiveness, they still constitute a search subject to judicial review under the Fourth Amendment.[61] Dragnet collection of this information from millions of individuals with no individualized suspicion of wrongdoing implicates the Fourth Amendment. DHS's proposal is also easily distinguished from other cases in which the Supreme Court *has* upheld biometrics collection by law enforcement officers without a separate warrant. In those cases, collection occurred only after individual

---

[58] Zak Doffman, *New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report,* FORBES (Aug 14, 2019), https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#75ce83ec46c6.

[59] Drew Harwell and Geoffry A. Fowler, *U.S. Customs and Border Protection Says Photos of Travelers Were Taken in a Data Breach*, THE WASHINGTON POST (June 10, 2019), https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/.

[60] *Maryland v. King*, 569 U.S. 435, 446 (2013) ("Virtually any intrusion into the human body will work an invasion of cherished personal security that is subject to constitutional security." (internal quotation marks and citations omitted)).

[61] *Id.*

suspects had been arrested for probable cause.[62] Here, DHS seeks to bypass this bar by classifying even the simplest interactions with the immigration system as sufficient reason to collect sensitive biometric information. Collection and long-term storage of biometric information is in many ways more intrusive than other searches courts have found to be invasive and non-routine, thus requiring a warrant or individualized suspicion.[64] Replacing DHS's current system with a system which makes intrusive searches the norm is counter to both our nation's values and established legal standards.

DHS's proposal also implicates the Fifth Amendment's equal protection guarantee. The Rule creates a distinct class of individuals and subjects them to unequal treatment. DHS's proposed biometric collection violates the Equal Protection Clause because it imposes "broad and undifferentiated disability on a single named group...[and] its sheer breadth is so discontinuous with the reasons offered for it."[67]

Additionally, the discretion that DHS reserves to waive the requirement for certain individuals raises narrower concerns over how it may be applied unevenly to different ethnic, racial, or religious groups.[68] DHS's own statement that it "is not proposing an absolute biometrics collection requirement" is cause for additional skepticism and raises further concern that the program will not be applied fairly, given the lack of clear standards for when exceptions will be made.[69]

In short, a Rule that so clearly runs counter to core Constitutional protections and principles of justice should not be adopted.

VI. Conclusion

The flimsy justifications DHS offers for the Rule are completely at odds with the massive scale of the biometric collection program it proposes to undertake. Rather than a rational plan grounded in public safety or national security, the Rule evinces a desire to subject, without suspicion of wrongdoing, a class of people to invasive, ongoing surveillance. DHS has not adequately addressed the potential for misuse of biometric data, the inherent unfairness of

---

[62] *Id.* at 462.
[64] YULE KIM, CONGRESSIONAL RESEARCH SERVICE, PROTECTING THE U.S. PERIMETER: BORDER SEARCHES UNDER THE FOURTH AMENDMENT 10 (2009) (finding intrusions into an individual's physical being invasive).
[66] *Id*.
[67] *Romer v. Evans*, 517 U.S. 620, 632 (1996).
[68] *See e.g.*, Fernando Santos, *Border Patrol Accused of Profiling and Abuse*, N.Y. TIMES (Oct. 14, 2015), https://www.nytimes.com/2015/10/15/us/aclu-accuses-border-patrol-of-underreporting-civil-rights-complaints.html; Kavitha Surana, *How Racial Profiling Goes Unchecked in Immigration Enforcement*, PROPUBLICA (Jun. 8, 2018), https://www.propublica.org/article/racial-profiling-ice-immigration-enforcement-pennsylvania; David Sharp, *Border Patrol Agent Accused of 'Textbook Racial Profiling'*, THE ASSOCIATED PRESS NEWS (Oct. 7, 2019), https://apnews.com/article/3b97425cad3c456289026cd61f5ff6da
[69] 85 Fed. Reg. 56,340.

surveilling already vulnerable populations, the unreliable nature of the technology, or the myriad legal concerns raised by the Rule. In light of these concerns, the proposed Rule is not justified and should be abandoned in total.

We appreciate the opportunity to provide comments on the Rule. If you have questions, please contact us by phone at 617-384-8165 or by email at hirc@law.harvard.edu.

Sincerely,

Harvard Immigration and Refugee Clinical Program
Harvard Law School
6 Everett Street, Suite 3103 (WCC)
Cambridge, MA 02138