October 13, 2020

Via Federal e-Rulemaking Portal

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

Re: Comments in Opposition to Proposed Rulemaking: Collection and Use of Biometrics by U.S. Citizenship and Immigration Services
85 Fed. Reg. 56338 (September 11, 2020)
USCIS Docket No. USCIS-2109-0007-0001
EOIR Docket No. 19-0007
CIS No. 2644-19
RIN 1614-AC14

To Whom It May Concern:

Brooklyn Defender Services ("BDS") submits these comments in opposition to the Department of Homeland Security ("DHS") Proposed Rule on Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 Fed. Reg. 56338, issued on September 11, 2020 (hereinafter, "Proposed Rule"), Docket No. USCIS-2109-0007-0001.

BDS is a full-service public defender organization in Brooklyn, New York, that provides multi-disciplinary and client-centered criminal defense, family defense, immigration, and civil legal services, along with social work and advocacy support. BDS represents low-income people in nearly 30,000 criminal, family, civil, and immigration proceedings each year. Since 2009, BDS has counseled, advised, or represented more than 15,000 clients in immigration matters including deportation defense, affirmative applications, advisals, and immigration consequence consultations in Brooklyn's criminal court system. About a quarter of BDS's criminal defense clients are foreign-born, roughly half of whom are not naturalized citizens and therefore risk losing the opportunity to obtain lawful immigration status as a result of criminal or family defense cases. Our criminal-immigration specialists provide support and expertise on thousands

of such cases. In addition, BDS is one of three New York Immigrant Family Unity Project ("NYIFUP") providers and has represented more than 1,400 people in detained deportation proceedings since the inception of the program in 2013. BDS's immigration practice also represents people in applications for immigration relief, adjustment of status, and naturalization before the United States Citizenship and Immigration Services ("USCIS"), and in non-detained removal proceedings in New York's immigration courts.

As set forth below, BDS strongly opposes the Proposed Rule in its entirety and, specifically, the Rule's dramatic expansion of the federal biometrics collection scheme on the backs of marginalized people. The Proposed Rule exponentially increases the scope of permissible mass surveillance, unduly burdens the lawful immigration process, allows for the collection of unreliable data from vulnerable people – including young children – subjects U.S. citizens and lawful permanent residents to invasive and unnecessary data collection, and threatens to destroy all remaining vestiges of privacy in the United States.

Further, the Proposed Rule seeks to circumvent due process and administrative rulemaking requirements by burying massive policy changes in footnotes, granting the federal government overly broad and unchecked discretion, and shifting the burden for justifying individual data collection away from DHS. Moreover, while these effects would be felt across racial, religious, ethnic, and immigration status lines, they would disproportionately impact people of color in low-income communities.

In the face of these near-certain harms, the Proposed Rule serves no legitimate governmental purpose and represents a slippery slope towards a true surveillance state. In order to prevent these immediate and far-reaching impacts, BDS asks that DHS immediately halt implementation of the Proposed Rule.

A. A 30-day Comment Period is Insufficient

The 30-day comment period set forth in the Notice of Proposed Rulemaking issued September 11, 2020, is woefully inadequate to allow the public a meaningful opportunity to digest, analyze, and comment on a rule that would upend privacy and dramatically expand mass surveillance in the United States.

The Proposed Rule changes the procedures, standards, and practices for biometrics collection by DHS, and would significantly impact all individuals who touch the United States' immigration system, including United States citizens, lawful permanent residents, and vulnerable immigrants. The Proposed Rule threatens to undermine due process, administrative rulemaking procedures, and established legal norms. Given the breadth of the Proposed Rule, which runs 85 pages in the Congressional Record and more than 325 pages of a PDF, the significant price tag associated with this rule change of nearly $300 million each year, and the potential

impact of mass data collection from more than six million people, the 30-day comment period is far too short to allow individuals, practitioners, and advocates to fully digest the rule and meaningfully craft feedback. Notably, 30 days is the minimum time allotted for a comment period.[1]

Although 30 days would be too short a comment period for such an extensive proposed regulation in any circumstance, it is especially egregious during the current COVID-19 pandemic, after months of a near-complete government shutdown, which threatened to furlough thousands of DHS employees and continues to wreak havoc and cause public health and economic devastation. Across the country, the physical offices of many legal organization—including BDS—have been closed, with staff working from home and advising clients, developing case strategy, and litigating cases remotely. The country's largest immigration court—26 Federal Plaza in New York—has been closed since March 18, 2020, and as of the date of this comment is still not open for hearings.[2] Against this backdrop, the DHS is proposing an overhaul of biometric and data collection practices that requires legal organizations to divert resources to carefully review the Proposed Rule and provide meaningful feedback.

Even more alarmingly, DHS flatly ignored a request from more than 100 organizations to extend the comment period.[3] The request, submitted merely five days after the expansive rule issued, described the need for additional time to consider the rule and touched on some of the substantive concerns. Nonetheless, DHS provided no response and instead pushed forward with the rulemaking process on an expansive Proposed Rule that will have devastating impacts.

BDS substantively objects to the entirety of the Proposed Rule; however, given the limited time allowed for comments, we have not addressed every proposed regulation or provision. Our silence regarding a proposed regulation or provision does not mean acquiescence. To be clear, we object to the entirety of the Proposed Rule. At a minimum, DHS should rescind the Proposed Rule in its entirety. Should the agency seek to re-issue a subsequent rule, it should grant a minimum of a 60-day comment period.

B. The Proposed Rule Undermines Constitutional Guarantees and Authorizes Constitutionally Suspect Invasive Search and Data Collection

[1] Office of the Federal Register, *A Guide to the Rulemaking Process Prepared by the Office of the Federal Register*,
https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf.

[2] *See* EOIR Operation Status During Coronavirus Pandemic, https://www.justice.gov/eoir-operational-status.

[3] *See* Ltr. From Organizations to Chad Wolf, Sept. 16, 2020, https://cliniclegal.org/resources/federal-administrative-advocacy/more-100-organizations-join-urge-dhs-provide-60-day.

Across the United States in communities large and small, the issue of data privacy is the subject of discussion, debate, and legislation. Numerous bans on facial recognition technology have been passed by municipalities (from Portland and San Francisco to Boston and Somerville). National and state level bans or moratoriums on biometric data systems—banning the collection and use of biometric data by government—are being proposed and debated.[4] Corporations from Microsoft to IBM have publicly denounced the use of technology for mass surveillance and pledged to divest from technology that is used to effect or contribute to racial injustice.[5] Despite this widespread outcry, the Proposed Rule imposes a new biometric data collection regime that runs directly contrary to current American beliefs and countless state and local laws and policies. The proposed regime would inaugurate a new version of the mass surveillance state that is diametrically opposed to the mandate of the People.

Hidden within the Proposed Rule's footnotes is the statement that the newly authorized stream of biometric data collected pursuant to the Proposed Rule will be aggregated within DHS's cloud-based, massive Homeland Advanced Recognition Technology (HART") database. Housed on Amazon's servers, HART is currently the second largest biometric databasing system in the world. The data aggregation and analysis capabilities introduced by this Proposed Rule are antithetical to a free democracy. Tellingly, the Proposed Rule provides no detail about HART, data already available to DHS, or the mechanics of adding the much more robust data stream generated by this Proposed Rule into HART. What is abundantly clear is that the Proposed Rule's data collection and aggregation program—including the use of the HART database—has not undergone a full privacy impact assessment. In the absence of a full privacy impact assessment, this Proposed Rule should be rescinded.

Furthermore, the Proposed Rule directly violates fundamental constitutional principles. Underlying the First Amendment's rights to free speech, free press, free religion, free assembly, and free association is the foundational right to freedom of thought. And underpinning the exercise of free thought is the universal right to public anonymity. The Supreme Court has explained: "Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation-and their ideas from suppression-at the hand of an intolerant society." *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 357 (1995) (internal citation omitted). By imposing the foundations of a true mass surveillance state without providing adequate justification for surveillance's expansion, the Proposed Rule represents a direct assault on anonymity and thus the Bill of Rights.

---

[4] Facial Recognition and Biometric Technology Moratorium Act of 2020, S.4084, 116th Congress (2019-2020)

[5] Letter from IBM CEO Arvind Krishna to U.S. Congress (June 8, 2020), https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/

In addition to its assault on the First Amendment, the Proposed Rule similarly abridges the essential spirit of the Fourth Amendment's protection. Guaranteeing the People's right to be "secure," the Fourth Amendment constrains the Government's unreasonable search and seizure of persons, houses, papers and effects. Indeed, even when considering arguments that privacy protections will undermine law enforcement, the Supreme Court has recognized that "the forefathers, after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of some criminals from punishment." United States v. Di Re, 332 U.S. 581, 595 (1948).

Here, without articulating any legal standard or requirement of even reasonable suspicion, the Proposed Rule imposes a presumption that the most intimate data about a person (from an individual seeking status to a United States citizen) will be demanded, collected, and aggregated by the federal government. DHS will then facilitate national and international sharing of that collected data among undefined "law enforcement" entities. Despite the significant privacy and legal implications to sharing such data, much less if it is used inappropriately, the Proposed Rule places no limitations on this data collection or the subsequent information sharing. Instead, the Proposed Rule contemplates a world of "continuous vetting," in which United States citizens and those who aspire to be citizens of this country are subjected to a constant lack of security, recurrent observation, and persistent uncertainty.

Regulatory schemes already exist that are designed to limit such broad-based, unjustified data gathering in this very type of scheme. For example, 28 CFR Pt. 23 requires all criminal intelligence systems to "collect information concerning an individual *only if* there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity." Further, that law requires that data only be disseminated to law enforcement agencies and officers when "there is a need to know and a right to know the information in the performance of a law enforcement activity." By contrast, the Proposed Rule fundamentally violates these existing regulations by divorcing data collection and aggregation from any individualized justification.

Finally, the Proposed Rule impinges upon local and state laws nationwide that protect data privacy. DHS has attested in the Proposed Rule that a federalism assessment is unnecessary but provided no rationale for that assessment. Instead, by funneling the data collected pursuant to the Proposed Rule into the HART database, the new paradigm would make a vast amount of private data available to local and state entities that are constrained by diverse state laws. By failing to conduct a federalism assessment, DHS is blindly ignoring the Proposed Rule's possible preemption of existing state privacy laws.

C. The Proposed Rule Vilifies Immigrants, Burdens Lawful Immigration, and Targets Vulnerable People

The Proposed Rule makes little effort to mask its true purpose: To expand DHS's monitoring and surveillance program and to dissuade immigration, even if such expansion comes at the expense of due process, constitutional protections, or the complete destruction of privacy norms. To accomplish these twin goals, the Proposed Rule requires anyone that stands to benefit from the U.S. immigration system — including U.S. citizens, lawful permanent residents, and vulnerable individuals — to endure invasive electronic searches as a prerequisite to benefiting from, or even advocating under, immigration law. Further, the Proposed Rule undermines lawful immigration by shifting the legal burden for establishing or challenging the appropriateness of a biometric search from the government to individuals navigating the immigration system.

Under current established regulations and practice, there is no blanket authorization for biometric data collection for civil law enforcement purposes, much less to assess a person's eligibility for affirmative immigration benefits. Instead, the law only authorizes blanket data collection for a narrow category of national security and criminal history background checks. Currently, if the government seeks to collect biometric information more broadly, it must justify its reasoning in each individual case. The Proposed Rule seeks to upend this narrowly tailored authorization and instead require any person petitioning an immigration agency, or that person's sponsor, beneficiary, or "individual filing or associated with an immigration benefit or request," or any person arrested by DHS, to submit to invasive searches of their "measurable biological (anatomical and physiological) or behavioral characteristics." The Proposed Rule would effectively require people to subject themselves to substantial and repeated invasions of personal and community privacy and significant monitoring as a requirement for touching the immigration system. Alarmingly, this prerequisite would apply not just to those people seeking to directly benefit from the immigration system but even to those U.S. citizens or immigrants with legal status who advocate for others within the system. Equally disturbing, the Proposed Rule allows the government to target children, who have historically been excluded from data collection both because of their unique vulnerabilities and because of the unreliable nature of biometric data about children and teenagers.

The impact of the Proposed Rule's expansion will be significant, harmful, and long-lasting. Family, friends, and community members will be discouraged from speaking for noncitizens because of the knowledge that their private information will be captured by the federal government. Individuals seeking to access immigration benefits or regularize their immigration status will be dissuaded from doing so for fear that the data collection may be used against them in the future. Vulnerable immigrants – including children and those asserting persecution-based claims for relief – will face additional threats as

their private information is captured and potentially exposed to the public,[6] including human traffickers and persecutors. Contrary to DHS's claims, the Proposed Rule will actually undermine security and violate fundamental principles of democracy in the United States.

* * *

Each instance of biometric data collection mandated by the Proposed Rule is harmful. The cumulative effect of the ongoing tracking, monitoring, and storage of biometric data authorized by the Proposed Rule's "continuous vetting" paradigm threatens the very fabric of the United States' democracy and undermines our entire immigration system. BDS strongly opposes the Proposed Rule. We request that DHS consider these recommendations and immediately halt the implementation of the Proposed Rule. Please do not hesitate to contact us if you have questions regarding our comments. Thank you for your attention and considering our concerns.

Sincerely,

/s/ Nyasa Hickey
Nyasa Hickey
Director of Immigration Initiatives

/s/ Elizabeth Daniel Vasquez
Elizabeth Daniel Vasquez
Special Forensic Science Counsel

/s/ Brooke Menschel
Brooke Menschel
Director, Civil Rights and Law Reform

[6] In addition to the inherent threat to individual privacy posed by governmental aggregation of this type, multi-modal biometric databases are particularly susceptible to catastrophic hacking events. DHS and its operational components are no strangers to cyber-attacks and the dumping of private DHS-held data onto the dark web. *See, e.g.,* Sidney Fussell, "This is Exactly What Privacy Experts Said Would Happen," The Atlantic (June 11, 2019) https://www.theatlantic.com/technology/archive/2019/06/travelers-images-stolen-attack-cbp/591403/; Drew Harwell, "Hacked documents reveal sensitive details of expanding border surveillance," The Washington Post (June 21, 2019), https://www.washingtonpost.com/technology/2019/06/21/hacked-documents-reveal-sensitive-details-expanding-border-surveillance/; Officer of the Inspector General for the Department of Homeland Security, "CBP Has Not Ensured Safeguards for Data Collected Using Unmanned Aircraft Systems," OIG-18-79 (Sept. 21, 2018) https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-79-Sep18.pdf.