United States Senate

October 16, 2020

The Honorable Chad F. Wolf
Acting Secretary
Department of Homeland Security
2707 Martin Luther King Jr. Ave SE
Washington, DC 20528-0385

Dear Acting Secretary Wolf:

We write regarding the proposal by the U.S. Citizenship and Immigration Services (USCIS) to significantly expand its collection of biometric information (USCIS Docket No. USCIS2019-0007). According to the Notice of Proposed Rulemaking published in the Federal Register on September 11, 2020, USCIS intends to update the Department of Homeland Security's (DHS) biometric information-collection regulations in connection with its "administration and enforcement of immigration and naturalization laws as well as the adjudication of benefit requests."[1] The proposal would allow DHS to collect biometric information as it conducts removal proceedings, processes family-based immigration applications, and vets immigrants seeking naturalization. In light of the threats that these policy changes would pose to the public's privacy, we urge you not to move forward with this regulatory update.

The USCIS proposal would dramatically expand the populations subject to invasive biometric data collection. Currently, DHS reportedly requires only individuals undergoing background checks to provide biometric data.[2] But under the proposed rule change, DHS may require *any* "applicant, petitioner, sponsor, beneficiary, or individual filing or associated with an immigration benefit or request" to "appear for biometrics collection."[3] Consequently, this regulation would allow DHS to force both *U.S. citizens* and non U.S. citizens alike to share with the federal government personal information about their bodies, a requirement that may violate constitutionally protected privacy and search and seizure rights. Additionally, the proposed rule expressly eliminates existing age-based data-collection restrictions, which exempt individuals

---

[1] Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 FR 56338, at 56339 (proposed Sept. 11, 20202) (to be codified at 8 C.F.R 1, 103, 204, 207, 208, 209, 210, 212, 214, 215 ,216,235, 236, 240, 244, 245).

[2] Geneva Sands, *Homeland Security Proposes Expanded Biometric Collection, Including DNA for Family Relationships*, CNN (Sept. 2, 2020) https://www.cnn.com/2020/09/02/politics/dhs-expanded-biometric-collection-dna/index.html.

[3] 85 FR at 56340.

under the age of 14 from biometric-data collection.[4] The USCIS proposal would allow DHS to subject children, a uniquely vulnerable population, to this invasive practice. By your own estimates, this expanded program would amass highly sensitive, biological information from more than six million people.[5] Compelling non-citizens navigating the U.S. immigration system to submit to data collection involving highly sensitive and immutable information carries serious privacy risks; subjecting U.S. citizens and children to this surveillance would be unacceptable.

We are also concerned that the proposal would increase the types of data that USCIS collects, allowing the agency to create detailed biological profiles of individuals involved in the immigration system. USCIS currently uses fingerprint technology. The proposed rule would permit collection of voice prints, eye scans, facial images, and palm prints. Additionally, the proposal would allow DHS to require certain individuals to submit "DNA test results" in order to "verify a claimed genetic relationship."[6] Expanding biometric-data collection in this manner would chill legal immigration, be inconsistent with our privacy values, and pose disproportionate risks to individuals of color.[7] The scope, sensitivity, and invasiveness of the proposed DHS biometric data collection program would amount to an unacceptable escalation of government surveillance.

Your agency's record of failing to protect the biometric data it already collects underscores the problematic nature of this regulatory proposal. According to a recent report from the DHS Office of the Inspector General, a data breach involving a facial recognition pilot program at U.S. Customs and Border Protection (CBP) resulted in the exposure of more than 180,000 traveler images.[8] According to the same report, more than a dozen of these images later appeared on the dark web. A privacy invasion of this nature is particularly harmful because victims of biometric data theft—as opposed to episodes involving credit card numbers or login credentials, for example— cannot easily protect themselves by changing the breached information. The Inspector General's conclusion that DHS "did not adequately safeguard sensitive data on an unencrypted device used during its facial recognition technology pilot" cast serious doubt on your agency's ability to responsibly manage its current biometric-data collection. It raises even more questions about how USCIS could conduct a vastly expanded program consistent with safeguarding the public's privacy.[9]

The timing of the USCIS proposal adds concerns. Congress is currently debating important legislation that would govern biometric data practices, including the government's collection of

---

[4] Preparing for Your Biometric Services Appointment, U.S. Citizenship and Immigration Service, https://www.uscis.gov/forms/filing-guidance/preparing-for-your-biometric-services-appointment (last visited Oct. 9, 2020).
[5] 85 FR 56338 at 56343.
[6] *Id.* at 56353.
[7] Patrick Grother et. al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* National Institute of Standards and Technology Interagency or Internal Report 8280 (2019).
[8] *Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot OIG-20-71*, United States Department of Homeland Security, Office of the Inspector General (Sept. 21, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.
[9] *Id.*

this information.[10] Moreover, against the backdrop of the ongoing, devastating health crisis in the United States and around the world, the public faces difficulty in timely commenting on a regulatory proposal of this magnitude.

In light of all our concerns, we urge you to abandon this regulatory proposal at this time.

Sincerely,

Edward J. Markey
United States Senator

Bernard Sanders
United States Senator

Ron Wyden
United States Senator

Elizabeth Warren
United States Senator

Jeffrey A. Merkley
United States Senator

[10] Press Release, Senator Edward J. Markey, *Momentum Builds for Markey-Merkley-Jayapal-Pressley Legislation to Ban Government Use of Facial Recognition, Other Biometric Technologies* (July 22, 2020), https://www.markey.senate.gov/news/press-releases/momentum-builds-for-markey-merkley-jayapal-pressley-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technologies.