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,
DC 20529–2240
(202) 272–8377

Re: 85 FR 56338; EOIR Docket No. 19-0007, CIS No. 2644-19; RIN 1615-AC14; Comments in Opposition to Proposed Rulemaking: Collection and Use of Biometrics by U.S. Citizenship and Immigration Services

To Whom It May Concern:

I appreciate the opportunity to comment on the Department of Homeland Security's (DHS) proposal to amend DHS regulations concerning the use and collection of biometrics in the enforcement and administration of immigration laws by U.S. Citizenship and Immigration Services (USCIS), U.S. Customs and Border Protection (CBP), and U.S. Immigration and Customs Enforcement (ICE) (Proposed Rule).

The Cato Institute is a public policy research organization dedicated to the principles of individual liberty, limited government, free markets, and peace. Cato's Project on Emerging Technologies, of which I am director, is dedicated to proposing technology policies consistent with those principles.

Summary

Biometric technology analyzes physical measurements as a means to verify identity. Current biometric technologies range from the relatively old (e.g. fingerprints) to the relatively new (e.g. voice recognition). Law enforcement's use of biometric technologies raises significant civil liberties concerns. Regrettably, for decades successive administrations have embraced biometric technology as a tool of immigration enforcement without adequately protecting civil liberties or adequately addressing bias present in the technology. The Proposed Rule continues this trend, and if implemented would make the current situation worse by expanding the categories of biometric data DHS collects while also including American citizens on the list of those who have to submit biometric data as part of the immigration process.

If implemented, this rule would deter immigration to the United States, put the civil liberties of law-abiding American citizens at risk, and grow the surveillance capabilities of federal, state, and local law enforcement.

A Shift from the Status Quo

Some immigration benefits are currently contingent on the submission of biometrics, and DHS must justify biometric collections that goes beyond what is required (typically a photograph and fingerprints). DHS currently oversees Automated Biometric Identification System (IDENT), the federal government's automated biometric identification system.[1] IDENT contains 220 million unique biometric identities and shares biometric data with law enforcement at the state and local level as well as other federal agencies.[2]

DHS is phasing out IDENT, but its data will be included in the new Homeland Advanced Recognition Technology (HART).[3] According to DHS, the biometric data includes "but is not limited to fingerprints, iris scans, and facial images."[4]

The proposed rule changes would alter the current state of affairs by:

1) Expanding the categories of people who must submit biometric data to DHS, including "*any* applicant, petitioner, sponsor, beneficiary, or individual filing or associated with an immigration benefit or request, *including United States citizens*" (emphasis mine).[5]
2) Authorizing the collection of biometric data from any alien for the purposes of "processing, care, custody, and initiation of removal proceedings."[6]
3) "[D]efin[ing]the term, 'biometrics,' to clarify and expand its authority to collect more than just fingerprints in connection while administering and enforcing the immigration and naturalization benefits or other services. To do this, DHS proposes to expressly define 'biometrics' to include a wider range of modalities than just fingerprints and photographs."[7]

[1] Department of Homeland Security. *NPPD at a Glance- Biometric Identity Management*. Washington D.C.: Cybersecurity & Infrastructure Security Agency, 2018. https://www.cisa.gov/sites/default/files/publications/nppd-biometric-identity-management-02132018-508.pdf
[2] Ibid.
[3] Department of Homeland Security. *NPPD at a Glance- Homeland Advanced Recognition Technology System.* Washington D.C.: Cybersecurity & Infrastructure Security Agency, 2020. https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf
[4] Department of Homeland Security. *Privacy Threshold Analysis Version number: 01-2014* Washington D.C.: Department of Homeland Security, 2014. https://epic.org/foia/dhs/hart/EPIC-2018-06-18-DHS-FOIA-20190422-Production.pdf
[5] Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 Fed. Reg. 56338 (September 11, 2020) https://www.federalregister.gov/d/2020-19145/p-3
[6] Ibid.
[7] Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 Fed. Reg. 56338 (September 11, 2020) https://www.federalregister.gov/d/2020-19145/p-214

4) Growing the number of biometric modalities to include: "[f]ingerprint; palm print; photograph (including facial images specifically for facial recognition, as well as photographs of physical or anatomical features such as scars, skin marks, and tattoos); signature; voice print; iris image; and DNA (DNA test results, which include a partial DNA profile attesting to genetic relationship)."[8]
5) Allowing DHS to require DNA tests as a means to verify claimed familial relationships.[9]
6) Changing how Violence Against Women Act petitioners and those applying for the T nonimmigrant status – an immigration benefit for victims of human trafficking - can demonstrate good moral character, including removing a presumption of good moral character for applicants under the age of 14.[10]
7) Clarifying the purposes of DHS biometric collection.[11]

In addition, the rule proposal outlines a plan for "continuous immigration vetting" Under such vetting those applying for U.S. citizenship could be asked to resubmit biometric data. Such vetting could also require applicants' relatives who are citizens or permanent residents to also submit biometric data.

Usually, an administration would provide at least sixty days for comment on a proposed rulemaking.[12] In this case, DHS has given the public thirty days to provide comment on a proposal that takes up more than eighty pages in the federal register.[13] DHS has not extended the deadline for the responses despite a request for extension.[14] The decision not to extend the comment deadline is regrettable. A rule change this sweeping and potentially devastating to Americans' civil liberties warrants, at the very least, a deadline for public commentary within the historic norm.

Civil Liberty Concerns

Biometric analysis is one of the most intrusive methods of identity verification and in many cases is not necessary. Before the rise of automated biometric technology identity verification was largely based on possession of particular items or facts linked to an identity. A passport of driver's license includes information about the person legally permitted to use the document for identity verification. They include data that in sum are unique to the individual (e.g. full name, date of birth, etc.) as well as a photograph. Passwords have been used for millennia for identity

[8] Ibid.

[9] Collection and Use of Biometrics by U.S. Citizenship and Immigration Services", 85 Fed Reg 56338 (September 11, 2020) https://www.federalregister.gov/d/2020-19145/p-3

[10] Ibid.

[11] Ibid.

[12] Executive Order No. 12866, Regulatory Planning and Review, 58 Fed. Reg. 51735 (Oct. 4, 1993) (requiring that the public generally be given 60 days to comment on a proposed rule); Executive Order No. 1356376, Improving Regulation and Regulatory Review, Fed. Reg. 3821 (Jan. 18, 2011)

[13] 85 Fed. Reg 56338-56422

[14] "More Than 100 Organizations Join to Urge DHS to Provide 60-Day Comment Period to Respond to DHS's Proposed Biometrics Expansion Rule", *CLINIC, Inc.*, September 17, 2020. https://cliniclegal.org/resources/federal-administrative-advocacy/more-100-organizations-join-urge-dhs-provide-60-day

verification (among other things). Today, passwords are often used as a means to confirm identity to distant institutions. When people today access their bank account online, they validate their identity and association with the account. The bank is supposing that only John Smith knows John Smith's password and username, so when someone visits the bank's website to view John Smith's bank account and uses John Smith's password and username the bank can be reasonably confident that the person seeking John Smith's bank account is John Smith. Such methods are not perfect. John Smith may have a password that is easy for criminals to guess. Two factor authentication helps address such concerns by adding another layer of security.

Law enforcement can access identity items and passwords under certain conditions, but they are nonetheless more secure than biometric data. We expose our biometric information in public regularly, potentially allowing for law enforcement to identify us absent our knowledge. For example, in 2015 authorities used facial recognition technology to identify and track protesters advocating for reform in the wake of the police killing of Freddie Gray.[15] In the age of facial recognition police need not ask you for your driver's license to identify you, they only need access to footage in which you appear.

Although ostensibly tasked with enforcing immigration and customs laws, DHS has conducted aerial surveillance on protesters in at least fifteen cities across the United States. This is only one example of state and local law enforcement using DHS surveillance tools. Earlier this year, a DHS predator drone flew over Minneapolis, Minnesota in the wake of the police killing of George Floyd.[16] My colleague David Bier and I discussed the concerns associated with DHS predator drones in a May 2018 Cato Institute white paper.[17]

DHS sharing surveillance tools and data ought to concern the American public, as information collected for immigration purposes could be used for the investigation of First Amendment-protected activities such as protests. Although the use of biometric surveillance technology on drone and body camera footage is fortunately not the norm, lawmakers and officials should nonetheless consider how present surveillance authorities could be used at a time when real-time biometric surveillance is widely available.

Many of the biometric technologies DHS listed in the Proposed Rule allow for increased surveillance and are associated with bias. The racial bias issues linked to facial recognition are

[15] Kevin Rector and Alision Knezevich, "Maryland's use of facial recognition software questioned by researchers, civil liberties advocates", *The Baltimore Sun*, October 18, 2016. https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html

[16] Tal Axelrod, "Democrats press DHS over use of drone during Minneapolis protests", *The Hill*, June 6, 2020. https://www.msn.com/en-us/news/politics/democrats-press-dhs-over-use-of-drone-during-minneapolis-protests/ar-BB156yua

[17] David J. Bier and Matthew Feeney, "Drones on the Border: Efficacy and Privacy Implications", *Cato Institute*, May 1, 2018 https://www.cato.org/publications/immigration-research-policy-brief/drones-border-efficacy-privacy-implications

perhaps the most noteworthy given how often they are discussed in the media. However, similar issues are linked to other biometric technologies discussed in the Proposed Rule.[18]

1) Iris Images
    - DHS justifies expanding biometric modalities to include iris images noting that they are valuable "especially for individuals whose fingerprints are unclassifiable or unattainable through loss of fingers, hand amputation, normal wear in the ridges and patterns over time (i.e., due to age, types of employment, etc.), or deliberate eradication/distortion of fingerprint ridges to avoid identification and detection."[19]
    - DHS presents iris images as a valuable means to verify identity but using iris images to confirm identity is not without concerns.
        1. Law enforcement poses risks associated with surveillance.[20] According to the Electronic Frontier Foundation, the New York Police Department (NYPD) began using mobile iris identification in 2010.[21] In 2012, *The New York Times* reported that the NYPD were holding arrested persons in custody longer than necessary if they did not submit optional iris scan images.[22] Local law enforcement are not alone. The Federal Bureau of Investigation collected iris scans from 434,000 arrestee between 2013 and 2016.[23] Such collection absent adequate privacy protections poses the risk of a biometric database. Although iris scan technologies have yet to develop to the stage where they are cost-effective and feasible real-time surveillance tools lawmakers and officials should nonetheless be preparing for a time when such capabilities are practicable.
        2. Iris scans are not perfect. In 2018, the National Institute of Standards and Technology (NIST) conducted a study of iris recognition technology.[24] The study found that iris recognition has improved since 2012.[25] More than half of the iris recognition tools NIST analyzed in its 2018 study (24 out of 46) yielded a false negative rate of less than 0.02 and a false

[18] "Collection and Use of Biometrics by U.S. Citizenship and Immigration Services", 85 Fed. Reg. 56338 (September 11, 2020) https://www.federalregister.gov/d/2020-19145/p-214

[19] Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 Fed Reg 56338 (September 11, 2020) https://www.federalregister.gov/d/2020-19145/p-228

[20] "Street-level Surveillance", *Electronic Frontier Foundation*, *October 25, 2019*, https://www.eff.org/pages/iris-recognition

[21] Ibid.

[22] "*Some Who Decline an Optional Iris Photo Are Kept Longer in Jail, Critics Say*", *The New York Times*, February 12, 2012, https://www.nytimes.com/2012/02/13/nyregion/new-objections-to-nypds-iris-photographing-program.html

[23] Colin Lecher and Russell Brandom, "The FBI has collected 430,000 iris scans in a so-called 'pilot program'", *The Verge*, July 12, 2016, https://www.theverge.com/2016/7/12/12148044/fbi-iris-pilot-program-ngi-biometric-database-aclu-privacy-act

[24] "NIST Releases IREX IX Part One Performance of Iris Recognition Algorithms (NISTIR 8207)", News, National Institute of Standards and Technology, *Updated April 23, 2018*, https://www.nist.gov/news-events/news/2018/04/nist-releases-irex-ix-part-one-performance-iris-recognition-algorithms

[25] Ibid.
See also: https://www.nist.gov/itl/iad/image-group/irex-iii-homepage

positive rate of less than 0.001. DHS should note which false positive and false negative rates it considers tolerable before deploying iris recognition technology. DHS should also note what degree of racial bias it considers acceptable. Racial bias is of particular concern to an agency tasked with enforcing immigration laws.[26] The 2018 NIST iris recognition study found that iris scan technology performed best on whites and worst on Asians.

2) Voice prints
    - According to DHS, voice print analysis can assist in identity verification at call centers and while processing immigration benefit claims submitted electronically.
    - DHS' proposed use of voice prints raises civil liberty concerns.
        i. Authorities in Australia, the United Kingdom, and Canada, use voice recognition technology to verify identities. In Australia and the United Kingdom, tax and revenue officials can use voice prints.[27] Australian taxpayers can request to have their voice print deleted, and British taxpayers can opt into the voice recognition system.[28] In Canada, border officials use voice recognition to monitor refugee claimants who have yet to confirm their identity. Canada's scheme is part of the "Alternatives to Detention" program.[29] The DHS proposal does not allow for immigrants or sponsors to request deletion of data. Nor is it optional.
        ii. Like other biometric technologies, voice prints have been associated with race and gender bias.[30] This is of particular concern during immigration procedures where DHS inevitably has to communicate with immigrants with non-American accents.[31] Such bias disproportionately affects minority groups.

3) DNA
    - The Proposed Rule would allow DHS to require DNA (deoxyribonucleic acid) tests in order to establish family relationships.[32] Using DNA to prove a family relationship risks infringing on civil liberties and fails to account for the composition of many families.

[26] "NIST Releases IREX IX Part One Performance of Iris Recognition Algorithms (NISTIR 8207)", News, National Institute of Standards and Technology, updated April 23, 201*8* https://www.nist.gov/news-events/news/2018/04/nist-releases-irex-ix-part-one-performance-iris-recognition-algorithms

[27] "Voice authentication", Online services, Australian Taxation Office, last modified September 6, 2017 https://www.ato.gov.au/general/online-services/voice-authentication/
"Voice Identification Privacy Notice," HM Revenue and Customs, July 27, 2018. https://www.gov.uk/government/publications/voice-identification-privacy-notice/voice-identification-privacy-notice

[28] Ibid.

[29] Canadian Authorities to Track Unverified Refugees with Voice Recognition", *FindBiometrics*, July 26, 2018, https://findbiometrics.com/canadian-authorities-refugees-voice-recognition-507261/

[30] 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

[31] Ibid.

[32] Collection and Use of Biometrics by U.S. Citizenship and Immigration Services", 85 Fed. Reg. 56338 (September 11, 2020), https://www.federalregister.gov/d/2020-19145/p-71

i. DNA reveals the unique genetic code associated with each person. It can uncover features about a person that they may not be aware of, such as their likelihood of passing certain traits or conditions to their children. DNA can also be used to determine biological parenthood and biological sex. DNA data is extremely sensitive, and the DHS rule does note this sensitivity: "DHS proposes to treat raw DNA (the physical sample taken from the applicable individual) that is taken as a distinctive biometric modality from the other biometric modalities it is authorized to collect, and not handle or share any raw DNA for any reason beyond the original purpose of submission (e.g., to establish or verify a claimed genetic relationship), unless DHS is required to share by law."[33] This is not reassuring given the number of circumstances in which a government agency might request DNA.

ii. It is not uncommon for children to be adopted. In addition, there are stepchildren and stepparents whose legal relationship cannot be verified via DNA analysis. Accordingly, DHS notes: "To the extent the rule discusses using DNA evidence to establish qualifying relationships in support of certain immigration benefit requests, it is referring only to genetic relationships that can be demonstrated through DNA testing."[34] But in families where parents do have close genetic ties to their children legal documents can provide better evidence of familial relationship without running the risk of law enforcement abusing access to a biometric database.

iii. In 2013, Supreme Court Justice Scalia wrote a dissent (joined by Justices Ginsburg, Sotomayor, and Kagan) in *Maryland v. King*, a case concerning whether police taking a DNA sample from a person arrested for a serious crime for identification purposes violated the Fourth Amendment, which protects against unreasonable searches and seizures.[35] Scalia's dissent warns of a "genetic panopticon" designed to tackle crime.[36] There may be cases in which it is difficult for DHS officials to establish family relationships thank to legal documents being unreliable or unavailable. But this difficulty does not justify the creation of an ever-growing genetic panopticon that is contrary to the ideals of a liberal republic. As Scalia correctly noted, "Perhaps the construction of such a genetic panopticon is wise. But I doubt that the proud men who wrote the charter of our liberties would have been so eager to open their mouths for royal inspection."[37]

[33] Collection and Use of Biometrics by U.S. Citizenship and Immigration Services", 85 Fed. Reg. 56338 (September 11, 2020), https://www.federalregister.gov/d/2020-19145/p-82

[34] "Collection and Use of Biometrics by U.S. Citizenship and Immigration Services", 85 Fed. Reg. 56338 (September 11, 2020), https://www.federalregister.gov/d/2020-19145/p-82

[35] *Maryland v. King,* 569 U. S. (2013), https://www.supremecourt.gov/opinions/12pdf/12-207_d18e.pdf

[36] Ibid.

[37] Ibid.

Conclusion

The DHS Proposed Rule threatens the civil liberties of Americans and immigrants. A history of American surveillance should make any lawmaker or agency official wary of attempts to increase the amount of sensitive data related to citizens and immigrants law enforcement can access.[38] The Proposed Rule is unfortunately the latest Trump administration proposal that would dissuade immigration rather than make DHS more efficient and transparent.

Thank you for the opportunity to comment on this important issue. I would be happy to answer any questions you may have. I can be reached via email at mfeeney@cato.org.

Sincerely,

Matthew Feeney
Director, Project on Emerging Technologies
Cato Institute

[38] "American Big Brother: A Century of Political Surveillance and Repression", *Cato Institute*, March 24, 2016, https://www.cato.org/american-big-brother