CENTER FOR DEMOCRACY & TECHNOLOGY

October 12, 2020

Via Electronic Submission

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

RE: Comment of the Center for Democracy & Technology on DHS Docket Number USCIS-2019-0007, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services

To Whom It May Concern:

The Center for Democracy & Technology (CDT) is a nonprofit advocacy organization dedicated to advancing the rights of the individual in the digital world.[1] We seek to limit unwarranted governmental intrusions on privacy for U.S. and non-U.S persons alike. We respectfully submit these comments urging the Department of Homeland Security (DHS) to withdraw proposed rule DHS Docket Number USCIS-2019-0007 Collection and Use of Biometrics by U.S. Citizenship and Immigration Services. If implemented, the rule would dramatically expand the persons subject to biometric data collection, the purposes for which biometrics are collected, and the types of biometrics DHS could compel from U.S. and non-U.S. persons.[2]

Among the many changes in this massive proposal, DHS would:[3]

- Dramatically expand the universe of people who could be subject to biometrics collection, authorizing the collection of biometrics from a broad array of immigrants and U.S. citizens, including: "*any applicant, petitioner, sponsor, beneficiary, or individual* filing or associated with a certain benefit or request,";[4]

[1] Center for Democracy & Technology, www.cdt.org/about.
[2] 85 Fed. Reg. 56338-56422 (posted Sep. 11, 2020), *available at* https://www.govinfo.gov/content/pkg/FR-2020-09-11/pdf/2020-19145.pdf.
[3] The proposed rule would also lift long standing bars on the biometric collection of children, compel survivors of domestic violence and trafficking to disclose biometric data, and permit DHS agencies to compel DNA testing as evidence of a familial relationship. That these and many other issues are not addressed specifically in this comment should not be interpreted as approval of the proposal. It is simply reflective of the limited time DHS has allowed for comment and review.
[4] 85 Fed. Reg. 56338, 56340.

- Expand the scope of biometric information to be collected, allowing DHS to collect iris scans, facial images (including facial images specifically for facial recognition, as well as photographs of physical or anatomical features such as scars, skin marks, and tattoos), palm prints, and, in some cases, DNA test results, including partial DNA samples;[5] and
- Subject immigrants to an ominous regime of "continuous vetting:" at any point during the years-long (oftentimes decades-long) process of becoming a U.S. citizen, DHS can demand updated biometric information from them, and can periodically require their U.S. citizen or lawful permanent resident relatives to resubmit information as well.[6]

This proposal is breathtaking in scale and impact. It will double the population from which DHS may seek sensitive personal information, it will cost millions of dollars every year to implement, it will introduce further delays into an already backlogged immigration system, and it risks eroding the privacy rights of millions of people in the United States. DHS has not provided the public, including CDT, enough time to properly comment on the many implications this rule if implemented would have on privacy, the protection of civil rights and the exercise of civil liberties. The agency has proffered weak justifications for why this massive data collection scheme is necessary or wise. It spends little ink on protections that might be afforded the data collected, leading to the possibility that few protections would be put in place. The proposal is also seemingly divorced from reality: at a time in which Congress, state legislators and the public are recognizing the need to be thoughtful about biometric data collection, DHS is barreling full steam ahead. We fear that if this proposed rule is implemented as written, immigrants and their loved ones would face a Hobson's choice: forgo family reunification, protection from oppressive governments, protection from abusers, and a path to stability, or forgo a great deal of privacy, security and respite from the watchful eyes of government. For these many reasons we respectfully submit that this rule should be withdrawn.

I. DHS failed to provide the public a meaningful opportunity to review and comment on this proposed rule.

Typically, an agency should allow a comment period of *at least 60* days following publication of a proposed rulemaking.[7] Without explanation, DHS arbitrarily limited the comment period for **this** of all proposed rules to an inadequate 30 days. Where agencies are instructed to provide *at least* 60 days for response, a proposal of this scale and complexity certainly demands even more time than that. The proposed rule, nearly 90 pages in length, dramatically expands who will be subjected to biometrics collection, how long and how frequently the government could

[5] *Id*. at 56341.
[6] *Id*. at 56352.
[7] Executive Order No. 13,563 (2011)."To the extent feasible and permitted by law, each agency shall afford the public a meaningful opportunity to comment through the Internet on any proposed regulation, with a comment period that should generally be at least 60 days." Executive Order No. 12,866 (1993). "In addition, each agency should afford the public a meaningful opportunity to comment on any proposed regulation, which in most cases should include a comment period of not less than 60 days."

demand their information, and what type of information the government can collect about them. If implemented, it will have a seismic impact on the lives of millions of immigrants and their U.S. citizen and lawful permanent resident relatives.

Substance aside, the ongoing COVID-19 pandemic has strained the regular operation of nonprofits, and the lives of the public. In recognition of these challenges, members of both the House of Representatives and Senate wrote to the Office of Management and Budget requesting that additional time be afforded for the public to engage with the rulemaking process stating that "[t]he right of the American people to meet with federal agencies and comment on proposed actions is invariably affected by the ongoing pandemic."[8] Instead, DHS ignored this admonishment from Congress, ignored routine rulemaking practice, and ignored over 100 organizations that requested additional time to grapple with the sweeping changes the department has proposed.[9] Based on this procedural consideration alone, we urge that this proposed rule be withdrawn.

II. If enacted the proposal would be a significant intrusion into the privacy of millions of immigrants, lawful permanent residents, and U.S. citizens.

Currently USCIS collects photographs, fingerprints and signature data from immigrants filing for a benefit. The proposed rule would authorize DHS to collect additional types of biometrics, from more persons, for a longer period of time. It "flip[s] the current construct from one where biometrics may be collected based on past practices, regulations, or the form instructions for a particular benefit, to a system under which biometrics are required for any immigration benefit request unless DHS determines that biometrics are unnecessary."[10] DHS estimates that biometrics collection will increase to 6.07 million people, from 3.9 million currently.[11] The proposed rule is a significant intrusion into the privacy of millions in the United States.

---

[8] Letter from House of Representatives Committee Chairs to Honorable Russell T. Vought, Acting Director, Office of Management and Budget (April 1, 2020), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/OMB.2020.4.1. Letter re Comment Period Extension.OI .pdf. *See also* Letter from Senators to Honorable Russell T. Vought, Acting Director, Office of Management and Budget (April 8, 2020), https://www.tomudall.senate.gov/imo/media/doc/4.8.20%20United%20States%20Senate%20Letter%20to%20OMB%20Acting%20Director%20Vought%20FINAL%5b1%5d.pdf.

[9] Letter from Catholic Legal Immigration Network, Inc., et al., to Chad Wolf, Acting Secretary, Dep't of Homeland Sec. et al. (Sept. 16, 2020), https://www.aila.org/advo-media/aila-correspondence/2020/aila-and-partners-request-dhs-to-extend-comment; Letter from Electronic Frontier Foundation to Chad Wolf, Acting Secretary, Dep't of Homeland Sec. et al. (Sept. 30, 2020), https://www.eff.org/document/eff-comment-re-necessity-60-day-comment-period-dhs-proposed-rule-collection-and-use; Letter from the Electronic Privacy Information Center to Chad Wolf, Acting Secretary, Dep't of Homeland Sec. et al. (Sept. 30, 2020), https://epic.org/privacy/biometrics/EPIC-DHS-Extension-of-Comment-Period-USCIS-2019-0007-Oct-2020.pdf.

[10] 85 Fed. Reg. 56338, 56350.

[11] *Id*. at 56364.

a. The purposes for which DHS seeks biometric data are generally overbroad and vague, and raise significant concerns that those who seek an immigration benefit, or seek to sponsor a family member for one, risk being placed under the specter of long-term surveillance.

i. Overbroad and vague

DHS seeks to compel biometric data for overly broad purposes that are so vaguely described that the individuals compelled to disclose information would not have an adequate sense of how their information may be used by the government. And indeed, the vagueness makes it difficult to provide comment on how DHS may more narrowly tailor its collection, if less intrusive alternatives would suit its purposes, or provide any other kind of constructive feedback.[12] For example, DHS seeks to clarify that it may seek biometric data from immigrants, U.S. citizens and lawful permanent residents for: "[i]dentity enrollment, verification, and management in the immigration lifecycle; national security and criminal history background checks to support determinations of eligibility for immigration and naturalization benefits; the production of secure identity documents; and to perform other functions related to administering and enforcing the immigration and naturalization laws."[13]

Biometric data is easily repurposed and vulnerable to function creep. If DHS proposes to compel more of it, from more persons, for new purposes, the department has an obligation to be more explicit about the applications to which it will be put, and to reasonably limit those applications. The last few years have demonstrated that for example, with respect to government databases of facial images, the public and political representatives were shocked that an image provided for purposes of getting a state driver's license, or a US passport, could end up in the possession of the Federal Bureau of Investigation and Customs and Border Protection, for purposes of criminal investigation and traveler identification respectively.[14] Such surprise should not occur again.

---

[12] There are some limited exceptions to the overbroad nature of the proposed rule. USCIS for example requests feedback on the collection of voice prints to cut down on the time needed to verify the identity of an individual who contacts a call center. There is an incredible backlog at USCIS for processing applications, which keeps individuals and their loved ones living in limbo as they await final resolution. Technology may help USCIS process applications more efficiently. Unfortunately, DHS limited the time for substantial engagement with discrete pieces of this proposal. That said, it is not clear why alternatives to voice prints would not suffice, such as the disclosure of an A-number over the phone. Additionally, if the voice print would be subject to overly permissive data sharing and repurposing, it is a high cost for a gain that could likely be achieved through less intrusive means, including more hiring. 85 Fed. Reg. 56338, 56356.

[13] 85 Fed. Reg. 56338, 56341.

[14] *See* Drew Harwell, *FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches*, WaPo (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/; Lori Aratani, *DHS withdraws proposal to require airport facial scans for U.S. citizens*, WaPo (Dec. 5, 2019), https://www.washingtonpost.com/local/trafficandcommuting/dhs-withdraws-

ii. Enhanced and continuous vetting

One of the more troubling elements of the proposal is DHS's request for comment on the appropriateness of biometric data collection for purposes of enhanced and continuous immigration vetting described as follows:

> "Under continuous vetting, DHS may require aliens to be subjected to continued and subsequent evaluation of eligibility for their immigration benefits to ensure they continue to present no risk of causing harm subsequent to their entry. This rule proposes that any individual alien who is present in the United States following an approved immigration benefit may be required to submit biometrics unless and until they are granted U.S. citizenship. The rule further proposes that a lawful permanent resident or U.S. citizen may be required to submit biometrics if he or she filed an application, petition, or request in the past, and it was either reopened or the previous approval is relevant to an application, petition, or benefit request currently pending with USCIS."[15]

Continuous vetting raises serious human rights concerns and paves the way for discriminatory surveillance of predominantly people of color. Demanding that immigrants and U.S. citizens submit to needlessly invasive biometrics collection is, as described below, a serious and unnecessary infringement upon privacy rights. Potentially requiring them to submit to this invasive collection repeatedly is entirely unjustifiable—and indeed, DHS doesn't even attempt to justify repeated demands for sensitive biometric information, other than citing to President Trump's discriminatory Executive Order No. 13780, Protecting the Nation from Foreign Terrorist Entry into the United States (Mar. 9, 2017). Far from keeping the United States safe, this rule, if implemented, will allow DHS to demand sensitive information of immigrants at any time in the years-long (sometimes decades-long) process of naturalization. It will also, as described below, chill the freedom of speech and association of immigrants and U.S. citizens association if they are concerned that the U.S. government may be paying them specific investigatory interest.[16]

b. *The collection of biometric data threatens the right to privacy, security, and anonymity. If enacted, the rule would chill the speech of immigrants and U.S.*

---

proposal-to-require-airport-facial-scans-for-us-citizens/2019/12/05/0bde63ae-1788-11ea-8406-df3c54b3253e_story.html.

[15] 85 Fed. Reg. 56338, 56352.

[16] Such concern would arise example, if the biometric data were to be used in a manner akin to USCIS's existing Continuous Immigration Vetting tool, which "automates and streamlines the process of notifying USCIS of potential derogatory information in Government databases that may relate to individuals in USCIS systems, as new information is discovered." U.S. Dep't of Homeland Sec., DHS/USCIS/PIA-076, Privacy Impact Assessment for the Continuous Immigration Vetting, 1, (Feb. 14, 2019), https://www.dhs.gov/sites/default/files/publications/pia-uscis-fdnsciv-february2019_0.pdf.

citizens subject to data collection impacting their civic participation in the United States.

The collection of facial images, iris scans, voice prints, fingerprints, and DNA is a great burden on privacy.[17] As information that can be used to identify an individual, the government's possession of biometric data can threaten an individual's ability to participate in society anonymously. This includes what they say, where they go, and with whom they associate. For example, if the government were to possess the types of biometrics contemplated in this proposal, a water bottle thrown away at a protest, facial image collected on a CCTV camera pointed at a mosque or synagogue, or phone call made to a relationship advice radio talk show could be associated with an individual. This could in turn reveal an individual's political beliefs, religious beliefs, and sexual orientation as well as a potentially sensitive personal matter such as infidelity. The stakes for privacy, civil rights and civil liberties are great.

It is surprising then, that the proposed rule pays little attention to data privacy, or how this collection will impact the exercise of fundamental rights. For example, in a discussion of costs privacy is raised and dismissed quickly: "[t]here could be some unquantified impacts related to privacy concerns for risks associated with the collection and retention of biometric information, as discussed in DHS's Privacy Act compliance documentation. However, this rule would not create new impacts in this regard but would expand the population that could have privacy concerns."[18] The proposed rule does not state explicitly where the data would be stored, how long it would be subject to retention, and with whom it can be shared. If it is stored in the major database that houses other DHS biometric data, it will be subject to overly permissive data sharing and retention.[19] Furthermore, as discussed above, the purposes for which DHS seeks to compel biometric data are so broad to create the impression that any data individuals provide an agency within DHS will be widely accessible to other federal and state agencies, and that DHS itself might use the data for all manner of surveillance.[20]

---

[17] DNA in particular is a very sensitive type of personal information. DNA reveals information about heritage, biological relationships, physical characteristics, medical conditions, genetic diseases, and predisposition for genetic disorders and health risks. It's disclosure makes one vulnerable to genetic discrimination, and also impacts the rights of relatives.

[18] 85 Fed. Reg. 56338, 56364.

[19] U.S. Dep't of Homeland Sec., DHS/NPPD/PIA-002, Privacy Impact Assessment for the Automated Biometric Identification System (IDENT), 25, (Dec. 7, 2012), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf (describing the typical retention schedule for information stored in IDENT as well as the agencies within DHS, and external of DHS that have access to the information).

[20] For example, while USCIS seeks biometric data in part for purposes of identity verification, which at least implies a 1:1 biometric match to ensure that an individual presenting for an interview is the same person who filed an application, DHS's interest in the use of biometrics for "enhanced and continuous vetting" indicates a much broader and aggressive type of periodic or regular agency investigatory interest.

Given the breadth of the proposed rule's language and its lack of assurances about privacy, security or limitations on use, the immigrants and U.S. citizens subject to data collection may be chilled from full participation in various aspects of society. For immigrants not yet citizens in particular, a chilling of participation in civic society is particularly damaging as they lack eligibility to vote to change policies. The only way then to express a preference for a policy is through participation in protest activity, organizing, and other manifestations of political expression. If this activity is chilled, immigrants are then effectively precluded from agitating for changes that might benefit themselves or others for whom they care in society. This would be an intolerable cost that strongly cautions against implementation of the proposed rule as written.

c. *The data DHS seeks to collect is vulnerable to data breach and unauthorized use*.

Given the sensitivity of the information DHS is seeking to compel and store, it's important to think about not only the uses to which it will be put in the United States, but also what other entities might do if they obtain this information. The rule does not explicitly state where DHS plans to store the vast amounts of biometric data it will collect. We can make some informed assumptions. Currently, DHS biometric data is stored in IDENT (Automated Biometric Identification System),[21] but going forward DHS biometric data will be stored in DHS's new Homeland Advanced Recognition Technology (HART) database.[22] Both will be an attractive target to foreign adversaries and bad actors. These bad actors will likely have plenty of time to try their hand. While the proposed rule fails to address data retention schedules for the various collections proposed, data in IDENT is retained for 75 years.[23]

Unfortunately the U.S. federal government has repeatedly failed to keep individuals' biometric data secure. The Office of Personnel Management breach in 2015 resulted in the disclosure of sensitive information about 22.1 million people, including 1.1 million sets of fingerprints.[24] And most recently at DHS, a database of 184,000 facial recognition images collected by Customs and

[21] U.S. Dep't of Homeland Sec., DHS/NPPD/PIA-002, Privacy Impact Assessment for the Automated Biometric Identification System (IDENT), 25, (Dec. 7, 2012), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf.
[22] U.S. Dep't of Homeland Sec., Homeland Advanced Recognition Technology System (HART) Increment 1 Privacy Impact Statement (PIA), 2, DHS/OBIM/PIA-004 (February 24, 2020), available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf.
[23] U.S. Dep't of Homeland Sec., DHS/NPPD/PIA-002, Privacy Impact Assessment for the Automated Biometric Identification System (IDENT), 25, (Decc. 7, 2012), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf.
[24] Ellen Nakashima, *Hacks of OPM databases compromised 22.1 million people, federal authorities say*, WaPo (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

Border Protection in Texas was hacked and misused.[25] After this breach of a US Government system, at least 19 of the images were posted on the dark web. In a report on the incident, the DHS Inspector General found that CBP did not satisfy its own security obligations, thereby creating the situation that led to the data breach, and the Inspector General acknowledged that "this incident may damage the public's trust in the Government's ability to safeguard biometric data."[26]

Unlike passwords or even social security numbers, biometric information cannot be changed if it is compromised in a data breach. Once a person's biometric information is obtained by an unauthorized party, it is obtained irrevocably. In the hands of a third party entity, this data could result in genetic discrimination for the data subject in the US or for their family members abroad, identity fraud, or other harms. The risk to immigrants is particularly great if sensitive information about them is disclosed to the very government they are fleeing, and a rejected application for relief or an immigration benefit forces their return.

The lesson from these data breaches caution against unnecessary data collection on the front end, but certainly against retaining data for longer than it is needed. Again, data retention was not discussed in the proposal. DHS should withdraw the proposed rule to address these glaring deficiencies in the document. Barring that, DHS must set stricter retention schedules than exist now in key DHS databases.

III. DHS fails to demonstrate that the collections are necessary.

The proposed rule makes clear what DHS *wants*, but not what the agency *needs*. DHS claims that biographic data is too inaccurate and susceptible to identity fraud. DHS repeatedly asserts that biometric collection is necessary to prevent fraud without attempting to quantify how widespread or frequent this phenomenon is, or how the asserted fraud is perpetuated. DHS appears to be seeking to expand the types of biometrics it collects because the FBI is collecting additional types of biometrics.[27] Simply because the FBI is collecting additional information does not mean DHS needs to, or should, or can. DHS does not explain why biographic data or the submission of fingerprints fail to sufficiently enable a criminal check with the FBI.

---

[25] Drew Harwell & Geoffrey Fowler, *U.S. Customs and Border Protection says photos of travelers were taken in a data breach*, WaPo (Jun. 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/.

[26] *Review of CBPs Major Cybersecurity Incident during a 2019 Biometric Pilot*, Office of Inspector General (Sept. 21, 2020), *available at* https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

[27] From the proposed rule: "DHS needs to keep up with technological developments that will be used by the FBI and agencies with which we will be sharing and comparing biometrics in this area and adjust collection and retention practices for both convenience and security, and to ensure the maximum level of service for all stakeholders." 85 Fed. Reg. 56338, 56355.

IV. If enacted this proposal will chill people from applying for benefits and prevent individuals from sponsoring their family members.

If put into place, these additional obligations will make it more difficult for immigrants and their sponsors to apply for immigration benefits. There are practical constraints: the new fees owed USCIS associated with biometric processing, as well as the time and travel required to appear for a biometrics appointment at a collection center. But the concern about living under perpetual government scrutiny is likely to chill many from seeking consequential immigration benefits. As discussed above, the data DHS collects is generally subject to overly permissive data-sharing regimes, and the data is retained indefinitely.

V. Policy headwinds should caution DHS against moving forward with this proposal because of the inadequate policy framework around the use of the biometric information that would be collected.

Bulk collection of biometric data without a framework to prevent the erosion of fundamental rights—as proposed in the draft rule—is not in line with today's policy discussions. Ironically, the examples of biometric surveillance from abroad that have animated these conversations in the United States are mirrored by DHS in this proposal.[28] Indeed, the United States recently condemned the involuntary collection of DNA from, and its use for surveillance and repression of, disfavored classes by the Chinese government in Xinjiang province.[29] One of the many items on which DHS solicits feedback is the department's use of facial images to include the development of a facial recognition system for "fraud, public safety or criminal history background checks, and national security screening and vetting."[30] The on-going and very active debate in the US about the government's use of facial recognition technology is by itself a clear illustration of just how out of step this proposal is.

Government testing and private testing of popular commercial facial recognition algorithms (including those used by the federal government) have exposed the existence of undemocratic demographic effects—specifically the fact that the technology produces disparate rates of accuracy when used on images of people of color, and women as compared to white persons and men.[31]Additionally there are significant concerns that the technology can result in mass

---

[28] *China: Minority Region Collects DNA from Millions*, Human Rights Watch (Dec. 13, 2017), https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions; *China: Voice Biometric Collection Threatens Privacy*, Human Rights Watch (Oct. 22, 2017), https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy.

[29] Deputy Secretary of State John J. Sullivan, "Remarks at the Human Rights Crisis in Xinjiang Event,"(speech, New York City, New York) Sept. 24, 2019, https://www.state.gov/deputy-secretary-john-j-sullivan-remarks-at-the-human-rights-crisis-in-xinjiang-event/.

[30] 85 Fed. Reg. 56338, 56356.

[31] Patrick Grother, Mei Ngan, Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280, Nat'l Inst. of Standards and Technology (December 2019), *available a*t

unchecked surveillance eroding the right to anonymity in public,[32] and may exacerbate systemic racism in policing.[33] In light of these concerns, Congress has held numerous hearings reviewing existing federal facial recognition technology programs in which members have discussed the need to press pause on the technology or subject it to limits.[34] Members have introduced legislation that would impose a moratorium on use[35] and to regulate the technology's use.[36] Some cities have banned the use of the technology.[37] And in light of protests against systemic racism, a number of technology companies that would be vendors of facial recognition technology have committed to not selling the technology to law enforcement in the absence of a human rights respecting framework regulating the technology's use.[38]

---

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf. See also, Joy Buolamwini and Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research 81:1–15, 2018, 1 http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[32] Clare Garvie, *Public Protest, Face Recognition, and the Shield of Anonymity*, Center on Privacy and Technology at Georgetown Law (June 9, 2020), https://medium.com/center-on-privacy-technology/public-protest-face-recognition-and-the-shield-of-anonymity-44daa8ad1e80.

[33] Joy Boulamwini, *We Must Fight Face Surveillance to Protect Black Lives*, Algorithmic Justice League (Jun 3, 2020), https://onezero.medium.com/we-must-fight-face-surveillance-to-protect-black-lives-5ffcd0b4c28a; Kade Crawford, H*ow is Face Recognition Surveillance Technology Racist*?, ACLU (Jun. 16, 2020), https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/; Malkia Devich-Cyril, *Defund Facial Recognition*, The Atlantic (July 5, 2020), https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/.

[34] House Committee on Oversight and Reform, Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties (May 22, 2019), https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and; House Committee on Oversight and Reform, Facial Recognition Technology (Part II): Ensuring Transparency in Government Use (June 4, 2019), https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-ii-ensuring-transparency-in-government-use; House Committee on Oversight and Reform, Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy (Jan. 15, 2020), https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-iii-ensuring-commercial-transparency.

[35] Facial Recognition and Biometric Technology Moratorium Act of 2020, *available at* https://www.congress.gov/bill/116th-congress/senate-bill/4084/text (introduced by Sens. Edward Markey D-MA, Jeff Merkley (D-OR) and Reps. Pramila Jayapal (D-WA) and Ayanna Pressley (D-MA), imposing a moratorium on government use of facial recognition technology).

[36] Facial Recognition Technology Warrant Act of 2019, *available at* https://www.coons.senate.gov/imo/media/doc/ALB19A70.pdf (introduced by Sens. Chris Coons (D-DE) and Mike Lee (R-UT), imposing a warrant requirement for more than 3 days of tracking facilitated by facial recognition technology). Ethical Use of Facial Recognition Technology Act of 2019, *available at* https://www.merkley.senate.gov/imo/media/doc/20.02.12%20Facial%20Recognition.pdf (introduced by Sens. Jeff Merkley (D-OR) and Cory Booker (D-NJ), prohibiting warrantless use of facial recognition and creating a commission to study facial recognition technology).

[37] *See e.g.*, Rachel Metz, *Portland passes broadest facial recognition ban in the US*, CNN (Sept. 9, 2020), https://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.htm; Aly Jarmanning, *Boston Bans Use Of Facial Recognition Technology. It's The 2nd-Largest City To Do So*, WBUR (June 24, 2020), https://www.wbur.org/news/2020/06/23/boston-facial-recognition-ban.

[38] Letter from IBM CEO Arvind Krishna to Member of Congress, (June 8, 2020), https://www.ibm.com/blogs/policy/wp-content/uploads/2020/06/Letter-from-IBM.pdf (announcing in the context of addressing responsible use of technology by law enforcement, that IBM has sunset its general purpose facial

Indeed, DHS's existing use of the technology has not evaded this scrutiny and criticism. The House Committee on Homeland Security held two hearings at which representatives lambasted DHS and CBP officials for their failure to ensure that Americans could exercise their right to opt out of the biometric-entry exit system and voiced concerns about preserving equality of experience in airport screening.[39] And when the hack of CBP's database of facial images took place, members of Congress voiced significant concern about the future of the collection program. In June of 2019, U.S. Senator Edward Markey called on DHS to halt its use of facial recognition technology and stated that the hack of CBP's data "raises serious concerns about the Department of Homeland Security's ability to effectively safeguard the sensitive information it is collecting." He also stated, "Malicious actors' thirst for information about U.S. identities is unquenchable, and DHS must keep pace with emerging threats."[40] Additionally, the Chairman of the House Committee on Homeland Security, Representative Bennie Thompson, said, "We must ensure we are not expanding the use of biometrics at the expense of the privacy of the American public."[41]

The collection of other biometric data without an adequate policy framework raises similar concerns. The lesson from this recent history should not be to move quickly forward with a biometric collection and screening proposal absent a framework in which to address privacy and equality concerns—certainly not when regulators are currently contemplating how to reign in unchecked surveillance.

***

recognition and analysis software products); Press Release. *We are implementing a one-year moratorium on police use of Rekognition*, Amazon (June 10, 2020), https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition (Amazon announcing a one year moratorium on police use of Amazon's facial recognition technology in the hopes that within that time Congress may "implement appropriate rules"); Jay Greene, *Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM*, WaPo (June 11, 2020), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/ (Microsoft commits to "not sell facial-recognition technology to police departments in the United States until we have a national law in place, grounded in human rights, that will govern this technology.").

[39] House Committee on Homeland Security, About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, (July 10, 2019), https://homeland.house.gov/activities/hearings/about-face-examining-the-department-of-homeland-securitys-use-of-facial-recognition-and-other-biometric-technologies; House Committee on Homeland Security, About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies Part II, (Feb 6, 2020), https://homeland.house.gov/activities/hearings/about-face-examining-the-department-of-homeland-securitys-use-of-facial-recognition-and-other-biometric-technologies-part-ii.

[40] Marie Szanisszlo, *Ed Markey: Customs data breach 'raises serious concerns',* Boston Herald (June 11, 2019), https://www.bostonherald.com/2019/06/11/u-s-sen-markey-dhs-data-breach-raises-serious-concerns/.

[41] Maggie Miller, *House Homeland Security Panel to hold hearings on DHS's use of biometric information in wake of CBP breach*, The Hill (June 10, 2019), https://thehill.com/homenews/house/447806-house-homeland-security-panel-to-hold-hearings-on-dhs-use-of-biometric.

For all of these reasons we respectfully urge you to withdraw this proposal. We welcome the opportunity to answer any questions about these comments and to engage further with you as the Department considers how to respect the privacy rights of immigrants and their loved ones. Questions about these comments can be directed to CDT's Mana Azarmi, at mazarmi@cdt.org.

Respectfully submitted,

Center for Democracy & Technology