epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Department of Homeland Security, Homeland Security Advisory Council

Final Report of the Biometric Subcommittee

Docket No. DHS-2020-0037

December 11, 2020

On November 12, 2020, the Department of Homeland Security's (DHS) Homeland Security Advisory Council (HSAC) published the Final Report of the Biometric Subcommittee.[1] HSAC provides advice and recommendations to the Deputy Secretary of the Department of Homeland Security and conducts research on security policies and related issues.[2] The Biometric Subcommittee, one of several subcommittees under HSAC, was tasked with "examin[ing] the need for and how the Department can better develop and implement a single and reliable approach to biometric identity management."[3] EPIC submits these comments in response to the Final Report of the Biometric Subcommittee. EPIC comments to 1) urge HSAC to revise the report after the committee has comprehensively reviewed DHS's uses and plans for biometric data including reviewing DHS's Proposed Rule on Definition, Collection, and Use of Biometrics[4] and 2) underscore the need for the HSAC Biometrics Subcommittee to comprehensively address the privacy and civil liberties risks of biometric data collection and use.

---

[1] Homeland Security Advisory Council, Final Report of the Biometric Subcommittee (Nov. 12, 2020), https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf.
[2] Department of Homeland Security, Homeland Security Advisory Council (Nov. 16, 2020), https://www.dhs.gov/homeland-security-advisory-council.
[3] Final Report, *supra* fn. 1 at 3.
[4] Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 Fed. Reg. 56338 (notice of proposed rulemaking Sept. 11, 2020).

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in DHS's biometric policies and practices.[5]

I. The Report fails to comprehensively consider how DHS uses or plans to use biometric data.

On September 11, 2020, United States Citizenship and Immigration Services published a proposal for a rule that would expand DHS's collection and use of biometric information.[6] About one month later, the Biometrics Subcommittee finalized their Report. In the beginning of the Report, the Subcommittee noted that it requested a copy of proposed rules relating to biometrics, but "none were furnished."[7] The Report states that the Subcommittee learned of the proposed rule through news sources and that it "takes no position regarding the substantive merits of the proposed rule."[8] The Subcommittee's inability to obtain relevant proposed rules calls into question the comprehensiveness of the entire Report.

Aside from the lack of comment on the proposed rule, the Subcommittee also failed to address ICE's contract with and use of Clearview AI and other facial recognition services.[9] ICE even conducted a specific privacy impact assessment on the agency's use of facial recognition services

---

[5] *See e.g.*, Comments of EPIC to the Transportation Security Administration, Intent to Request Revision of Agency Information Collection Activity Under OMB Review: TSA PreCheck, Docket ID: TSA-2013-0001 (June 22, 2020), https://epic.org/apa/comments/EPIC-TSA-PreCheck-FRT-CommentJune2020.pdf; Comments of EPIC to the Department of Homeland Security, Agency Information Collection Activities: Biometric Identity, Docket No. 1651-0138 (Jul. 24, 2018), https://epic.org/apa/comments/EPIC-CBP-Vehicular-Biometric-Entry-Exit-Program.pdf; EPIC v. CBP (Biometric Entry/Exit Program), https://epic.org/foia/dhs/cbp/biometric-entry-exit/default.html (EPIC obtained a report which evaluated iris imaging and facial recognition scans for border control); EPIC Statement to U.S. House Committee on Homeland Security, "Border Security, Commerce and Travel: Commissioner McAleenan's Vision for the Future of CBP" (Apr. 24, 2018), https://epic.org/testimony/congress/EPIC-HHSC-CBP-Apr2018.pdf.

[6] 85 F.R. 56338.

[7] Homeland Security Advisory Council, Final Report of the Biometric Subcommittee, 5 (Nov. 12, 2020), https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf.

[8] *Id*.

[9] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, NYT (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

earlier this year.[10] Clearview AI allows law enforcement officers to upload a photo of a person in an application that procures public photos of that person and links to where the photos came from such as the subject's (or others') profiles on YouTube, Venmo, Facebook, etc.[11] The use of Clearview AI has been a point of public controversy and EPIC and other privacy experts/advocates have warned against its use.[12] The software Clearview AI uses has yet to be vetted for accuracy by the National Institute of Standards and Technology (NIST) and Clearview's scraping of billions of photos from millions of websites is a threat to privacy.[13]

Prior to making any recommendations to DHS, HSAC should ensure that the Subcommittee has an appropriate and comprehensive understanding of DHS's use of and plans to use biometrics. EPIC urges HSAC to table the Report until the Subcommittee can address DHS's use and plans to use biometric data without omission.

II. The Report largely ignores the fact that pushback in response to DHS's collection and use of biometrics, particularly facial recognition, is not a result of DHS's failure to communicate they agency's implementation plan.

The Subcommittee focused significantly on DHS's communication regarding biometrics and new biometric programs. As such, several of their recommendations involved new communication requirements but failed to appropriately address the reasons there have been pushback against DHS's expanding collection and use of biometrics. The Subcommittee recommends that DHS should establish a Biometrics Oversight and Coordination Council which would review implementation and communication plans submitted by DHS agencies.[14] They also recommend that a novel use of

[10] *See e.g.*, Department of Homeland Security, Privacy Impact Assessment for the ICE Use of Facial Recognition Services (May 13, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf.
[11] Hill, *supra* fn. 9.
[12] Angela Chen, *40 Groups have called for a US Moratorium on Facial Recognition Technology*, MIT TECH. REV. (Jan. 27, 2020), https://www.technologyreview.com/2020/01/27/276067/facial-recognition-clearview-ai-epic-privacy-moratorium-surveillance/.
[13] Hill, *supra* fn. 9.
[14] Homeland Security Advisory Council, Final Report of the Biometric Subcommittee, 42 (Nov. 12, 2020), https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf.

biometrics by DHS should require a separate communication and outreach plan.[15] Other recommendations focus on who leads biometric related operations, like the recommendation that DHS Office of Policy should be the primary office to negotiate or communicate with other nations regarding international disclosure of biometric data.[16] While better communications regarding DHS's collection and use of biometrics are welcomed, the pushback from EPIC and other privacy, civil liberties, and immigration groups over DHS's use of biometrics is not the result of DHS's failure to effectively communicate their plans. There are several other issues that EPIC urges HSAC to address further including the sensitivity of biometric data, the power of surveillance, privacy and civil liberty issues, the collection of DNA, expansion of face recognition, and the overall lack of federal regulation.

a. The Sensitivity of Biometric Data

Biometric data is highly sensitive. A person's biometric data, particularly facial images, is linked to that person's dignity, autonomy, and identity.[17] A person's biometrics cannot be changed like a compromised password or account number. Collection of a person's biometrics can cause psychological harm due to fear of identity theft and surveillance.[18] As such, and in line with DHS's commitment to the Fair Information Practice Principles, collection and use of biometric data must be limited and minimized, the purpose of that collection and use must be specified, and the data must be secure.[19] EPIC urges HSAC to recommend that DHS strictly follow the FIPPs to facilitate a

[15] *Id*. at 45.
[16] *Id*. at 44.
[17] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI NOW INSTITUTE, https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf; Woodrow Hartzog, Facial Recognition Is the Perfect Tool for Oppression, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.
[18] *See e.g.*, Comments of EPIC to the Department of Homeland Security, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 F.R. 56338, 4 (Oct. 13, 2020), https://epic.org/apa/comments/EPIC-DHS-BiometricNPRM-Oct2020.pdf.
[19] Department of Homeland Security, Privacy Policy Guidance Memorandum, No. 2008-01 (Dec. 29, 2008), https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

consistent approach to biometric identity management and immediately review the agency's implementation of biometrics to minimize the use, collection, retention, and dissemination to the bare minimum that is needed to perform DHS's missions.

DHS has a history of failing to fulfill their commitment to the FIPPs.[20] For example, the Report incorrectly indicates that there has been no evidence of compromised data since IDENT was implemented in 1994.[21] Despite the previous statement, the Subcommittee admitted to a data breach at CBP subcontractor Perceptics, LLC that resulted in the release of at least 19 facial recognition images on the dark web because of CBP's failure to adequately fulfill its security responsibilities.[22] This breach is only one, unfortunate, example of exactly why DHS should be limiting its collection, retention, and disclosure of highly sensitive biometric data. The consequences of compromised biometric data, such as photos populating on the dark web, were severely overlooked, and downplayed by the Subcommittee's Report. This oversight by the Subcommittee significantly dismisses the sensitivity of biometric data.

b. The Power of Surveillance

Surveillance is a powerful technique that can lead to asymmetry between the U.S. government and the people. This asymmetry becomes especially apparent when people are being surveilled without knowledge or consent, or for example, when their photographs are taken from a distance. In two sentences, only, the Subcommittee mentioned this risk: "Facial recognition does, indeed, pose a unique set of privacy concerns. For instance, it is possible for photos to be taken at a

[20] Comments of EPIC, *supra* fn. 18, at 14.
[21] Homeland Security Advisory Council, Final Report of the Biometric Subcommittee, 36 (Nov. 12, 2020), https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf.
[22] Homeland Security Advisory Council, Final Report of the Biometric Subcommittee, 36 (Nov. 12, 2020), https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf; Comments of EPIC to the Department of Homeland Security, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 F.R. 56338, 12-13 (Oct. 13, 2020), https://epic.org/apa/comments/EPIC-DHS-BiometricNPRM-Oct2020.pdf.

distance, covertly, and without consent of protesters exercising their First Amendment rights."[23] This is possibly a reference to a facial recognition program run by the Secret Service outside the White House. They employed facial recognition technology which monitored open areas, where protestors might convene.[24] The Subcommittee never explicitly referenced this program and did not address this concern further. The Privacy Impact Assessment for the USSS program declared that "individuals who do not wish to be captured by White House Complex CCTV and cameras involved in this pilot may choose to avoid the area."[25] This is not an adequate "opt out" option as many people are unaware of the facial recognition surveillance until they are already within the photographable area, if they become aware at all. This type of nonconsensual surveillance is an abuse of government power and creates an asymmetric dynamic between the government and U.S. citizens.

Without elaborating on the expansion, the Report notes that several DHS agencies have plans to expand collection and use of biometrics.[26] As discussed previously, DHS has a commitment to use limitation. Expansion of biometric collection and use increases the risks to privacy and civil liberties. The expansion of DHS facial recognition services in particular, without adequate regulation, can lead to mass surveillance, loss of individual freedoms, and mission creep.[27] Mission creep is the expansion of a group's actions over time, beyond the originally intended scope.[28] For DHS, mission

---

[23] Homeland Security Advisory Council, Final Report of the Biometric Subcommittee, 26 (Nov. 12, 2020), https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf.
[24] Department of Homeland Security, Privacy Impact Assessment for the Facial Recognition Pilot, 4 (Nov. 26, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-usss-frp-november2018.pdf.
[25] *Id*.
[26] Homeland Security Advisory Council, Final Report of the Biometric Subcommittee, 12, 15, 18, 31 (Nov. 12, 2020), https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf.
[27] Woodrow Hartzog, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.
[28] *See e.g.*, Comments of EPIC to the Department of Homeland Security, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 F.R. 56338, 4 (Oct. 13, 2020), https://epic.org/apa/comments/EPIC-DHS-BiometricNPRM-Oct2020.pdf; Comments of EPIC to Department of Homeland Security, Border and Transportation Security Doctorate, Docket No. BTS 03-01 (Jan. 5, 2003), https://www.epic.org/privacy/us-visit/usvisit_comments.pdf; EPIC, *Spotlight on Surveillance: Homeland Security ID Card is Not So Secure* (Apr. 2005), https://epic.org/privacy/surveillance/spotlight/0405.html; Comments of EPIC to Department of Homeland Security Customs and Border Protection, Agency Information Collection Activities: Arrival and Departure Record (Forms I-94

creep might mean becoming overly involved with local law enforcement or monitoring protected activities like the BLM protests in 2020, resulting in massive surveillance.[29]

c. Privacy and Civil Liberty Issues

The unnecessary expansion of biometric collection and use can lead to the loss of individual rights and freedoms. For example, the expansion of certain modalities, like DNA testing and facial recognition services, can cause increased risks of oppression and exploitation.[30] A person's right to privacy, even in public spaces, is protected by the Fourth Amendment.[31] Additionally, the Privacy Act of 1974 sought to restrict the amount of data federal agencies can collect.[32] EPIC urges HSAC to recommend that DHS abide by their commitment to the FIPP's and limit their collection, use, and disclosure, and retention of biometrics to the bare minimum that is required for their mission(s). This commitment would help protect the right to privacy and enjoyment of civil liberties.

1. Collection of DNA

The collection of DNA requires serious consideration of privacy rights given the sensitivity of a person's genetic code.[33] DNA test results can expose medical conditions and information about race and heredity.[34] The Report indicates that Customs and Border Patrol (CBP/BP) has coordinated with Immigration and Customs Enforcement, Homeland Security Investigations (ICE/HIS) for the collection of DNA samples "where there was a question of a false claim of parentage by an adult

---

and I-94W) and Electronic System for Travel Authorization, Docket No. 1651- 0111 (Aug. 22, 2016), https://epic.org/apa/comments/EPIC-Comments-DHS-Social-Media-IDs.pdf.

[29] Zolan Kanno-Youngs, *U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance*, NYT (June 19, 2020), https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html.

[30] Hartzog, *supra* fn. 27.

[31] *Id*.

[32] *See* Comments of EPIC to the Department of Homeland Security, U.S. Citizenship and Immigration Services, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 F.R. 56338, 4 (Oct. 13, 2020), https://epic.org/apa/comments/EPIC-DHS-BiometricNPRM-Oct2020.pdf.

[33] *See e.g.*, Brief for EPIC as Amicus Curiae, Maryland v. King, 569 U.S. 435 (2013), https://www.epic.org/amicus/dna-act/maryland/EPIC-Amicus-Brief.pdf (arguing in part that retaining "junk DNA" used in CODIS has substantial privacy implications); Anita LaFrance Allen, Genetic Testing, Nature, and Trust, 27 Seton Hall L. Rev. 887 (1997) (noting that DNA testing creates "the potential for social stigma, discrimination in employment, barriers to health insurance, and other problems.").

[34] Comments of EPIC, *supra* fn. 32 at 11.

with a minor child."[35] The Subcommittee also notes that the DOJ rule, "DNA-Sample Collection from Immigration Detainees," published in early 2020, removed a prior limitation to DHS's DNA collection.[36] The new rule, allowing DHS to collect DNA on a non-voluntary basis, received over 40,000 comments, many of which asserted that the DNA collection is based on immigration status, not criminal arrest.[37]

EPIC has previously explained the harms associated with the expansion of DNA collection, especially because all law enforcement agencies in the U.S. have access to the same database, Combined DNA Index System (CODIS), that stores the biometric data collected.[38] The implications of this DNA collection and storage, in combination with the storage of other biometrics, are far-reaching. The massive storage of biometrics, without appropriate use limitation, is ripe for opportunities of mission creep and exploitation. Additionally, the non-voluntary collection of DNA also implicates privacy rights of family members whose DNA is a close enough match.[39] In consideration of the data minimization principle, DHS should strive to limit their storage of DNA to what is absolutely essential for carrying out the mission.

2. Facial Recognition

As mentioned in the Report, several facial recognition algorithms have been proven to exhibit both gender and racial bias.[40] For example, the NIST study found false positives and

[35] Homeland Security Advisory Council, Final Report of the Biometric Subcommittee, 12 (Nov. 12, 2020), https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf.
[36] *Id.* at 35.
[37] DNA-Sample Collection from Immigration Detainees, Docket ID: DOJ-OAG-2019-0004, https://www.regulations.gov/docket?D=DOJ-OAG-2019-0004.
[38] *See e.g.*, Comment of the American Civil Liberties Union, Center for Democracy & Technology, Center on Privacy & Technology at Georgetown Law, EFF, EPIC, Mijente, National Immigration Project of the National Lawyers Guild, and Project South, 9 (Nov. 12, 2019), https://epic.org/apa/comments/Coalition-Comments-Immigration-Detention-DNA-Collection.pdf.
[39] Natalie Ram, *Fortuity and Forensic Familial Identification*, 63 STAN L. REV. 751, 767–71 (Apr. 2011) (noting that, as of 2010, 19 states had approved or reported the use of a partial match in an effort to associate a crime-scene profile with the family member of a person whose profile is in CODIS though 15 of those states ostensibly prohibited the practice at the time).
[40] Homeland Security Advisory Council, Final Report of the Biometric Subcommittee, 27 (Nov. 12, 2020), https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf.

negatives to be higher for people of color, females, children, and the elderly.[41] Accordingly, several U.S. cities have banned the use of facial recognition, including Portland, Boston, Oakland, and San Francisco.[42] The Subcommittee notes that some algorithms, like the ones used by CBP, did not demonstrate "statistically significant demographic matching variances."[43] However, as EPIC has iterated previously, *any* demographic variance through automation cannot be tolerated. EPIC urges DHS not to tolerate *any* discrimination through automation even if those variances are the result of insufficient and non-inclusive data input.

Despite the Subcommittee's conclusion of NIST's results and assurances of "statistically insignificant" variances, EPIC urges HSAC to recommend that DHS discontinue their use of facial recognition. There has been no independent, non-governmental, auditing of CBP's use of facial recognition algorithms to confirm non-discriminatory effects. Finally, even "flawless" facial recognition algorithms poses serious implications for privacy and civil liberties.[44]

d. *Lack of Federal Regulation*

Currently, the public is relying on DHS agency policies and procedures for protection. These policies and procedures can and do change, and they do not have the force of law behind them. For example, DHS proports to follow the Fair Information Practice Principles, outlined in their Privacy Policy Guidance Memorandum, but as mentioned previously, the agency often falls short of this commitment.[45] The fact that DHS does not follow its own commitment to protection, reinforces the

[41] National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2-3 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[42] EPIC, Ban Face Surveillance, https://epic.org/banfacesurveillance/.
[43] Final Report, *supra* fn. 40 at 26-27.
[44] Woodrow Hartzog, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.
[45] Department of Homeland Security, Privacy Policy Guidance Memorandum, No. 2008-01 (Dec. 29, 2008), https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf; Comments of EPIC to the Department of Homeland Security, U.S. Citizenship and Immigration Services, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 F.R. 56338, 13 (Oct. 13, 2020), https://epic.org/apa/comments/EPIC-DHS-BiometricNPRM-Oct2020.pdf.

need for regulation on the collection and use of biometrics. EPIC urges HSAC to recommend that DHS discontinue its collection and use of facial recognition services, until there are adequate regulations in place to protect U.S. citizens.

III. Conclusion

The Final Report of the Biometric Subcommittee failed to address several pressing privacy and civil liberty concerns regarding DHS's collection and use of biometrics. Largely ignoring pressing biometric issues and DHS's plans for expanding their collection, the Subcommittee instead focused on DHS communication strategies. EPIC urges HSAC to table the Report until the Biometrics Subcommittee can address DHS's use of and plans to use biometrics in full, after careful review of relevant rules and proposals. HSAC and by extension DHS need to fully engage the privacy and civil liberties issues presented by the collection and use of biometrics if the agency hopes to ever have a reliable approach to biometric identity management.

Respectfully Submitted,

Jeramie Scott
Jeramie Scott
EPIC Senior Counsel

Hannah McDonnell
Hannah McDonnell
EPIC Clerk