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, U.S. Citizenship and Immigration Services

Collection and Use of Biometrics by U.S. Citizenship and Immigration Services

85 F.R. 56338

October 13, 2020

By notice published September 11, 2020 the Department of Homeland Security (DHS) and its sub-component U.S. Citizenship and Immigration Services (USCIS) propose a rule to permit DHS to expand the collection and use of biometric information.[1] EPIC submits these comments in opposition to the proposed rule. EPIC comments to 1) draw attention to the agency's failure to comply with the Fair Information Practice Principles by authorizing substantially more biometric collection than is necessary, 2) assert that over-collection poses a threat to individual's privacy by exposing personally identifiable data to data breach and by increasing the risk of misuse within the agency, 3) underscore the risk of mission creep as the agency seeks to find a use for unnecessarily collected and retained biometric data, and 4) urge DHS to suspend the use of facial recognition technology.

EPIC and over 100 civil society organizations requested DHS extend the comment period to the standard 60 days provided for rulemakings.[2] DHS refused and pushed ahead, allowing the public

[1] Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 Fed. Reg. 56338 (notice of proposed rulemaking Sept. 11, 2020).
[2] EPIC, Letter to DHS Requesting Extension of Time to Submit Comments (Sept. 30, 2020) https://epic.org/privacy/biometrics/EPIC-DHS-Extension-of-Comment-Period-USCIS-2019-0007-Oct-2020.pdf https://epic.org/privacy/biometrics/EPIC-DHS-Extension-of-Comment-Period-USCIS-2019-0007-

only 30 days to comment on a 85-page notice published that substantially expands DHS's collection and use of extremely sensitive personal information. The short time for comment and the breadth of the proposed rule will prevent the public from being adequately informed of the rulemaking and undermines the purpose of the comment process. Due to the short time-frame EPIC's comments cannot cover all of the threats to privacy and civil liberties contained within the 85-page federal register notice. The issues discussed below are not exclusive, but they are among the most serious concerns with DHS's proposal.

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 preserving the Privacy Act safeguards enacted by Congress.[3] EPIC also has a sustained interest in DHS's biometrics policies and practices.[4]

Oct-2020.pdf, *and* 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.americanimmigrationcouncil.org/advocacy/letter-requesting-60-day-comment-period-proposed-rule-expanding-collection-biometrics.

[3] *See, e.g.*, Comments of EPIC to the Department of Homeland Security, Correspondence Records Modified System of Records Notice, Docket No. DHS-2018-0029 (Oct. 26, 2018), *available at* https://epic.org/apa/comments/EPIC-Comments-DHS-Correspondence-Records.pdf; Comments of EPIC to the Department of Homeland Security, Terrorist Screening Database System of Records Notice and Notice of Proposed Rulemaking, Docket No. DHS-2016-0002, DHS-2016-0001 (Feb. 22, 2016), available at https://epic.org/apa/comments/EPIC-Comments-DHS-TSD-SORN-Exemptions-2016.pdf; Comments of EPIC to the Department of Homeland Security, Notice of Privacy Act System of Records, Docket No. DHS-2011-0094 (Dec. 23, 2011), available at http://epic.org/privacy/1974act/EPIC-SORN- Comments-FINAL.pdf; Comments of EPIC to the Department of Homeland Security, 001 National Infrastructure Coordinating Center Records System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2010-0086, DHS-2010-0085 (Dec. 15, 2010), available at http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0086_0085.pdf; Comments of EPIC to the United States Customs and Border Protection; Department of Homeland Security on the Establishment of Global Entry Program, Docket No. USCBP-2008-0097 (Jan. 19, 2010), *available at* http://epic.org/privacy/global_entry/EPIC-Comments-Global-Entry-2010.pdf.

[4] *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) *available at* https://epic.org/apa/comments/EPIC-TSA-PreCheck-FRT-Comment-June2020.pdf; Comments of EPIC to the Department of Homeland Security, Agency Information Collection Activities: Biometric Identity, Docket No. 1651-0138 (Jul. 24, 2018) *available at*

I. DHS plans to massively expand the population of individuals submitting biometrics. That expansion poses a privacy risk to each individual with information in DHS's databases.

DHS currently collects biometric information for a variety of discreet purposes. DHS proposes to "flip" that procedure and instead require biometrics for all immigration benefits, collecting biometrics from applicants/petitioners, their sponsors, beneficiaries, families, or associates.[5] The "flip" expands biometrics collection by collecting biometrics on all applicants for immigration benefits instead of only a subset and by pulling in a new population, individuals with some connection to the applicant. DHS would also remove the 14 and under age restriction on biometric collection and subject children to the full range of biometric data collection.[6] In addition to expanding the population from which DHS collects biometrics, the department proposes to engage in "Enhanced and Continuous Vetting" in which immigrants must subject themselves to continuous biometric analysis until they receive U.S. citizenship.[7] The consequence is the collection of biometrics from roughly 2,170,000 more individuals each year under the proposed rule, according to DHS estimates.[8] Whether DHS may collect information from those individuals, and all individuals, is governed by the Privacy Act of 1974.

When Congress passed the Privacy Act of 1974, it recognized that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies"[9] and that "the right to privacy is a personal and fundamental right

---

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.

[5] 85 F.R. 56350.

[6] 85 F.R. 56357.

[7] 85 F.R. 56352.

[8] 85 F.R. 56378 Table 15.

[9] S. Rep. No. 93-1183 at 1 (1974).

protected by the Constitution of the United States."[10] At its core the Privacy Act seeks to restrict the amount of personal data that federal agencies are able to collect.

The GAO recently identified a range of harms from the disclosure of PII including various forms of identity theft, fraud, lost time restoring identity, emotional distress, reputational harm, and harm from state-based actors.[11] With the increased use of biometrics for commercial identification (fingerprint locked phones, facial recognition to access bank accounts, etc.) loss of biometric data poses similar risks. The GAO concluded that current identity theft services were of limited value to individuals and could not address all of the risks from a data breach.[12] The risks of data breaches, and the fact that harms are not easily remedied, requires extra caution when collecting PII.

Each new individual added to DHS's biometric databases is exposed to risks of data breach, unwarranted surveillance, and psychological harms from concerns over identity theft and surveillance. DHS should have strong justifications for adding new individuals to its databases. The department should also implement security measures and meaningful limits on use to protect individuals from potential harms. The Fair Information Practice Principles provide guidelines for the department to responsibly collect biometric data and other personally identifiable information (PII) which can help mitigate those risks.

II. Broad authorization of biometrics collection does not comply with DHS's Fair Information Practice Principles (FIPPs) by failing to minimize the data collected, failing to implement meaningful use limitations, and failing to adequately safeguard sensitive biometric information from data breaches or accidental disclosure.

DHS intends to add new "modalities" to its definition of biometrics and expand the use of already approved modalities.[13] Modalities are specific methods of information collection and types

[10] Pub. L. No. 93-579 (1974).
[11] U.S. Gov't. Accountability Off., GAO-19-230, DATA BREACHES: Range of Consumer Risks Highlights Limitations of Identity Theft Services 5-6 (Mar. 2019) https://www.gao.gov/assets/700/697985.pdf.
[12] *Id* at 9-14.
[13] 85 F.R. 56341.

of information, like iris images or fingerprints. When DHS collects information, including new modalities of biometric information, it should comply with the FIPPs to reduce the risks posed by collection and aggregation of PII.

a. The FIPPs set benchmarks for data collection and use.

DHS's FIPPs memo outlines the core principles around which the department should structure its data collection practices. [14] The FIPPs comprise eight mandates: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability.[15] Importantly, the FIPPs "must be considered whenever a DHS program or activity raises privacy concerns or involves the collection of personally identifiable information from individuals, regardless of their status."[16] The principles of Data Minimization, Use Limitation/Purpose Specification,[17] and Security are the basis for the analysis in these comments. While the other FIPPs are important, these get to the core of the threats posed by unchecked biometric data collection.

1. Data Minimization

To meet the principle of Data Minimization, "DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s)."[18] This standard breaks down into a) necessity of collection and b) limited retention. DHS has only met this standard when the department has ensured

[14] Hugo Teufel III, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security Memorandum Number 2008-01, Dep't. of Homeland Sec. (Dec. 29, 2008) https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.
[15] *Id* at 4.
16 Privacy Policy Guidance Memorandum, https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.
[17] Although these are separate principles, they function together as checks on oversharing and misuse of data.
[18] *Id* at 4.

that the data it collects is necessary for a legitimate purpose and has ensured that data is retained only long enough to complete that legitimate purpose.

2. Use Limitation and Purpose Specification

Use Limitation requires that DHS, "use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected. "[19] To comply with the Purpose Specification principle, "DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used."[20] Purpose specification requires that DHS both provide the authority for each data collection and elaborate the reason for collection, the intended use. Use Limitation defines the outer bounds of acceptable use for data already collected, the legitimate purpose of collection. Failure to meet either standard defeats both, purpose specification governs the decision to collect data, while use limitation governs the department's handling and exploitation of that data once collected. The result is over-use, when information is exploited beyond the legitimate, specific purpose it was collected for. Failure to define the purpose and limit the use of biometric data collection may lead to mission creep, as discussed below.

3. Security

In order to meet Privacy Act requirements and protect individuals, "DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure."[21] This principle requires proactive and comprehensive steps to guard against the release of PII. Where DHS cannot

[19] *Id*.
[20] *Id* at 3.
[21] *Id* at 4.

guarantee the security of PII, the agency should not collect it. In cases where DHS already possesses PII that is at risk of breach the department should delete it post-haste.

b. DHS plans to collect several new biometric modalities, and expand the collection of others, without a clear purpose or sufficient privacy protections.

DHS's current standard practice is to use fingerprints for identification, photographs for visual verification, and signatures for document production.[22] Where DHS collects other biometric modalities, the department has been engaged in limited tests, has obtained the biometric voluntarily as in a submitted DNA sample, or has determined that a specific practice or regulation requires the use additional biometrics.[23] DHS plans to expand its practices to routinely collect palm prints, photographs for facial recognition, voice prints, iris images, and DNA. While the department's past practices have been far from the minimized, use-limited collection of biometrics which the FIPPs call for, this new regulation would indiscriminately vacuum up biometric information.

1. Palm Print

DHS plans to collect palm prints in addition to fingerprints as standard practice, to align with the FBI's planned background check system.[24] DHS has also suggested that it may use palm prints as an identifier for immigration benefit applications.[25] However the department does not claim that it needs palm prints in addition to fingerprints as identifiers for immigration benefits. While capturing palm prints may be "of increasing interest"[26] to the law enforcement community, the broad compilation and storage of biometrics for "law enforcement" use is not a sufficiently descriptive purpose. As with other modalities, sweeping up palm prints without a unique, limited justification risks over-use.

---

[22] 85 F.R. 56355.
[23] To be clear, this is not an endorsement of DHS's past practices which have often collected far more biometric information than is necessary to DHS's mission, resulting in real privacy harms.
[24] 85 F.R. 56355-56.
[25] 85 F.R. 56380.
[26] 85 F.R. 56356.

2. Photographs

DHS has to date used routinely used photographs for in-person identification.[27] Although the agency has experimented with using facial recognition in pilots such as the Biometric Entry/Exit Program, such uses were not standard practice for all applicants. DHS's proposal to maintain databases of photographs including distinguishing features and facial recognition capabilities on all applicants would substantially expand the department's current practices.

3. Voice Print

DHS has not articulated a unique need to collect voiceprints distinct from other biometric modalities. The agency cites four potential uses of voice print matching: 1) electronic submission of immigration benefits applications, 2) voice identification of callers to USCIS call centers, 3) voice identification for remote adjudication interview, and 4) general fraud prevention and national security uses.[28] At this time there are no direct plans to acquire equipment to collect voice prints, though DHS is "searching" for a device with "similar features to a web-cam" to record voice prints.[29]

Indeed, DHS is not even clear on what type of voice recognition the agency would use. The NPRM identifies both active and passive voice identification as options but fails to consider the substantial privacy differences between them.[30] Active voice ID asks the user to say a passphrase each time she seeks to be identified and compares the voiceprint to a pre-recorded version of the phrase, a 1:1 matching approach.[31] Passive voice ID compares how an individual speaks generally to a pre-recorded sample. Passive voice ID is easily expanded beyond legitimate authentication

[27] 85 F.R. 56355.
[28] 85 F.R. 56356.
[29] 85 F.R. 56384.
[30] 85 F.R. 56356.
[31] Matt Smallman, *Good Call: the hybrid answer to voice authentication*, 2020 Biometric Tech. Today 10-12 (2020) https://doi.org/10.1016/S0969-4765(20)30051-5.

functions to identify any recorded sample of an individual speaking. EPIC has consistently testified in favor of 1:1 matching technologies as substantially more privacy protective.[32]

DHS's proposal to collect voice biometrics fails to meet the principle of Data Minimization as there are other identification technologies available, including those presently in use. In particular the proposal to add voiceprint identification to webcams when they already offer reliable means of identification indicates an intent implement a new biometric modality without any need.[33] The failure to identify active voice identification as a safer technology for the public fails both the principle of Data Minimization and Security. The broad purposes behind DHS's proposal including general fraud prevention and national security interests render voice ID vulnerable to over-use. Failure to implement strong use limitation, particularly if DHS adopts passive voice ID, will contribute to mission creep if DHS seeks to leverage a database of voiceprints beyond caller identification.

4. Iris Images

DHS proposes to add iris images as a new biometric modality to collect at Application Support Centers and as mobile biometrics, include these in the IDENT biometric database, and use iris images in the adjudication process.[34] To justify collecting iris images for all applicants, DHS cites the need to identify individuals missing hands or lacking fingerprints.[35] However current DHS policy sufficiently covers these situations. Where an individual has only a partial set of fingerprints

[32] *See* EPIC Statement on Face Surveillance to U.S. House Committee on Homeland Security (Feb. 5, 2020) https://www.epic.org/testimony/congress/EPIC-HHSC-FRT-Feb2020.pdf, *and* EPIC Statement on Facial Recognition to Massachusetts General Court Joint Committee on the Judiciary (Oct. 22, 2019) https://epic.org/testimony/congress/EPIC-FacialRecognitionMoratorium-MA-Oct2019.pdf.
[33] 85 F.R. 56384.
[34] 85 F.R. 56355.
[35] *Id*.

(e.g. is missing a hand), DHS simply collects the partial prints.[36] In the rare situations where an individual has a permanent loss of fingerprints, DHS may grant a waiver.[37] DHS therefore justifies collecting a new biometric modality for all applicants based on the extremely limited need to identify a small class of individuals. The stated purpose of the collection is so much smaller than the intended use that DHS's collection of iris images cannot in its current form comply with FIPPs guidance. Expanding the already massive IDENT database with more biometrics will not improve DHS's functioning, but does threaten individual privacy.

5. DNA

DHS proposes for the first time to require DNA testing as evidence of a family relationship.[38] Immigrants are already required to provide bevy of documentary evidence, including birth and marriage certificates, medical records, religious documents, and affidavits.[39] The department claims to protect privacy by classifying the raw genetic material as a distinct biometric modality which will only be used for the original purpose of submission.[40] However DHS intends to treat DNA test results as any other biometric modality, to be stored and shared for "adjudication purposes, or to perform any other functions necessary for administering and enforcing immigration and naturalization laws".[41] The extra privacy protections claimed by DHS are an empty promise, protecting only raw genetic material, the mouth-swab or spit-sample, without protecting the sensitive information contained within a DNA test. A person's genetic code is widely understood to be among

[36] USCIS Policy Manual Volume 1 General Policies and Procedures: Part C Biometrics Collections and Security Checks, Chapter 2 Biometrics Collection C. – Fingerprint Waivers (Oct. 6, 2020) *available at* https://www.uscis.gov/policy-manual/volume-1-part-c-chapter-2.
[37] *Id.*
[38] 85 F.R. 56341.
[39] *Id.*
[40] *Id.*
[41] *Id.*

the most sensitive types of personal information.[42] DHS claims that the partial genetic profile it produces, containing 16-24 genetic markers "does not reveal medical or hereditary conditions."[43] However, recent advances in genetic science have revealed that the "junk DNA" used for DNA fingerprinting can reveal the presence of disease.[44] Even if DHS is right, the privacy implications of DNA do not begin and end with medical conditions. Partial DNA profiles can reveal race and heredity as well.[45] Disclosure of DNA test results, even a partial analysis, exposes a unique biometric identifier capable of revealing medical conditions and sensitive information around race and heredity.

DHS's proposal flies in the face of the principles of purpose specification and use limitation. DHS would extract DNA for the limited purpose of confirming a family relationship and then leverage that information across the entirety of its work ignores the FIPPs entirely. DHS has further failed the principle of data minimization. If DHS truly needs to collect DNA to verify a family relationship, the department can retain only the result of the analysis (e.g. match/no match) in its records.

In total, DHS's new and expanded biometric modalities would collect up to seven different modalities from an applicant for other individual.[46] DHS would then have a stunning amount of

---

[42] *See e.g.* Brief for EPIC as Amicus Curiae, Maryland v. King, 569 U.S. 435 (2013), *accessible at* 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.");

[43] 85 F.R. 56353.

[44] *See e.g. Sieving through 'junk' DNA reveals disease-causing genetic mutations*, Science Daily (Oct. 3, 2013) https://www.sciencedaily.com/releases/2013/10/131003142321.htm (finding nearly 100 genetic variants in non-coding DNA are implicated in the development of breast cancer).

[45] Felipe Queiros, The visibilities and invisibilities of race entangled with forensic DNA phenotyping technology, 68 J. of Forensic and Legal Medicine 101858 (Nov. 2019) https://www.sciencedirect.com/science/article/pii/S1752928X19300873#bib26.

[46] This assumes DHS would collect fingerprints, palm prints, signature, iris images, facial photographs, and voice prints for most if not all applicants, and that DHS here also required DNA.

information about the individual, down to a partial DNA profile, stored in the department's databases. DHS cannot need all of this information to identify an applicant for immigration benefts

c. **The recent surge in government data breaches, particularly within DHS, puts the sensitive biometric information of individuals at significant risk of compromise**.

In 2016 the U.S. Government Accountability Office warned that "[c]yber-based intrusions and attacks on federal systems have become not only more numerous and diverse but also more damaging and disruptive."[47] The GAO called on DHS to enhance cybersecurity protection in key areas including intrusion detection and prevention. At the time DHS had not even put in place an adequate process for sharing information on intrusions and potential malicious activity.[48] Since that time DHS and its subcomponents have not shown that they are capable of safeguarding personally identifiable information, particularly biometric data.

In 2019 a data breach at CBP subcontractor Perceptics, LLC exposed approximately 184,000 images of travelers from CBP's Biometric Entry/Exit pilot.[49] Perceptics staff were able to violate several DHS security and privacy protocols to download the images used for facial recognition without CBP's IT security controls preventing the unauthorized action or sounding an alarm.[50] When Perceptics, LLC was subsequently hacked outside agents had access to those 184,000 images and an additional 105,000 license plate images.[51] At least 19 facial recognition images were released on the dark web.[52] DHS's Office of the Inspector General found that, "Perceptics was able to make

[47] U.S. Gov't Accountability Office, *DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System* (Jan. 2016), http://www.gao.gov/assets/680/674829.pdf.
[48] *Id* at 27.
[49] Joseph Cuffari, Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot, Dep't of Homeland Sec. Off. of Inspector Gen. (Sept. 21, 2020) https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf .
[50] *Id* at 6.
[51] *Id* at 8.
[52] *Id* at 13.

unauthorized use of CBP's biometric data, in part because CBP did not implement all available IT security controls, including an acknowledged best practice."[53] OIG concluded that CBP "Did not adequately fulfill its responsibilities for IT security".[54]

The 2019 breach is far from the only example of DHS and its' subcomponents failing to safeguard sensitive information. The Federal Emergency Management Agency (FEMA) unnecessarily disclosed sensitive information of victims of the 2017 California wildfires, exposing up to 2.3 million people.[55] FEMA shared details of victims financial institutions and personal lives including EFT and bank transit numbers and complete addresses.[56] The unidentified subcontractor then failed to notify FEMA of receiving extra information.[57] A 2017 data breach by an agency employee exposed the personal information, including Social Security numbers, of 247,167 DHS employees.[58] In February 2016 hackers gained access to DHS and DOJ databases, exposing information on up to 9,000 DHS employees and 20,000 F.B.I. employees. [59] DHS's recent track record demonstrates that the agency has failed to implement adequate safeguards for personal data.

Data breaches are common across the federal government as well, exposing the PII of millions to exploitation and abuse. As recently as August 24, 2020 a cyber-attack compromised a

---

[53] *Id* at 12.
[54] *Id*.
[55] Christopher Mele, Personal Data of 2.3 Million Disaster Victims Was Released by FEMA, Report Says, N.Y. Times (Mar. 22, 2019) https://www.nytimes.com/2019/03/22/us/fema-data-breach.html, John V. Kelly, Management Alert – FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information, OIG-19-32 Dep't of Homeland Sec. Off. of Inspector Gen. (Mar. 15, 2019) https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-32-Mar19.pdf.
[56] OIG FEMA Memorandum at 4.
[57] *Id*.
[58] Steven Musil, Homeland Security breach exposes data on 240,000 employees, CNET (Jan. 3, 2018) https://www.cnet.com/news/homeland-security-breach-exposes-data-on-240000-employees/; Dep't. of Homeland Sec., Privacy Incident Involving DHS Office of Inspector General Case Management System (Update) (Jan. 18, 2018) https://www.dhs.gov/news/2018/01/18/privacy-incident-involving-dhs-oig-case-management-system-update.
[59] Eric Lichtblau, Hackers Get Employee Records at Justice and Homeland Security Depts., N.Y. Times (Feb. 8, 2016) https://www.nytimes.com/2016/02/09/us/hackers-access-employee-records-at-justice-and-homeland-security-depts.html.

federal agency and documents were stolen.[60] As an example of the trend across the federal government, a 2015 data breach at the Office of Personnel Management (OPM) exposed social security numbers and other personal data from 21.5 million individuals.[61] Around the same time OPM reported another major data breach exposing records on about 4 million federal employees.[62] Again in 2015, approximately 390,000 tax accounts with the Internal Revenue Service were compromised, revealing SSNs, dates of birth and street addresses among other PII.[63] In September 2014, a breach at the United States Postal Service led to the loss of PII from more than 800,000 employees.[64] In sum, data breaches at federal agencies have grown exponentially more common in the last decade, from a reported 5,503 breaches in 2006 to 67,168 discovered in 2014.[65]

Both DHS and the federal government have broad track records of failing to secure personally identifiable information, resulting in the disclosure of sensitive information on millions of individuals. DHS expects to collect biometrics from over 2.1 million new people per year, bringing the total yearly collection of biometrics to an estimated 5,790,219 individuals.[66] Holding that volume of biometric information without proper safeguards is a substantial threat to the privacy and security of millions. Aside from mission creep or overuse concerns, DHS should not expand its collection of biometric data where the department cannot guarantee its safety. At the present time, the evidence

[60] Cybersecurity and Infrastructure Security Agency, Federal Agency Compromised by Malicious Cyber Actor, AR20-268A, Dep't. of Homeland Sec. (Sept. 24, 2020) https://us-cert.cisa.gov/ncas/analysis-reports/ar20-268a, Duncan Riley, DHS discloses data breach of US agency but doesn't name which was hacked, SiliconAngle (Sept. 24, 2020) https://siliconangle.com/2020/09/24/dhs-discloses-data-breach-us-agency-doesnt-name-hacked/.
[61] 2016 GAO Report, *supra* note 45, at 8.
[62] *Id*.
[63] *Id* at 7-8.
[64] *Id* at 8.
[65] U.S. Gov't Accountability Office, Federal Agencies Need to Better Protect Sensitive Data 4 (Nov. 17, 2015), http://www.gao.gov/assets/680/673678.pdf.
[66] 85 F.R. 56378.

points to an inability to safeguard information from hacks, data breaches by subcontractors, or inadvertent disclosure by the agency.

d. **Overcollection of biometric information increases the chances of mission creep and privacy/civil liberties violations as the agency seeks to leverage its biometric databases beyond its core objectives.**

Mission creep is the gradual expansion of a group's actions beyond its original scope or goals. EPIC has consistently warned of the dangers of mission creep at DHS.[67] But EPIC is far from the only voice concerned about DHS expanding beyond its core national security mission. A 2013 report from the Congressional Research Service found that DHS had failed to clearly prioritize or strategize to implement it's 'homeland security' mission.[68] The report warns, "There is no clarity in the national strategies of federal, state, and local roles and responsibilities; and, potentially, funding is driving priorities rather than priorities driving the funding".[69] Even former Homeland Security Secretary Tom Ridge voiced concerns about DHS ever-expanding mission, "They've kind of lost their way. … The focus – the primary focus – has been substantially diminished."[70] Concerns of mission creep resurfaced with added urgency this year as DHS's role in the Black Lives Matter protests came under scrutiny.[71] Mission creep occurs in three major ways, 1) DHS's mission expands

[67] *See e.g.* 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/us-visit_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 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.
[68] Shawn Reese, Cong. Rsch. Serv., R42462 Defining Homeland Security: Analysis and Congressional Considerations (2013), https://fas.org/sgp/crs/homesec/R42462.pdf.
[69] *Id* at 13.
[70] Michael Coleman, MISSION CREEP: Homeland Security a 'runaway train', Albuquerque J. (Apr. 27, 2014), https://www.abqjournal.com/390438/homeland-security-a-runaway-train.html.
[71] *See e.g.* Nick Miroff, DHS's changing mission leaves its founders dismayed as critics call for a breakup, Washington Post (Aug. 13, 2020), https://www.washingtonpost.com/national/dhs-mission-creep-protests/2020/08/13/44a287ce-dc8b-11ea-b4af-72895e22941d_story.html.

beyond its Congressional mandate, 2) DHS becomes more involved in local law enforcement, and 3) DHS operates with "opaque accountability and [a] visible heavy hand".[72]

Albuquerque is a prominent example of mission creep at DHS. A three-part investigation by the Albuquerque Journal found that "Department of Homeland Security's mission in the state has also grown beyond the narrow counterterrorism and disaster relief mandate outlined in the 2002 federal law that established the department."[73] Homeland Security Investigations (HSI) agents were deployed to the New Mexico Attorney General's Office and police departments across the state.[74] As a result federal agents were tasked with investigating local gang activity, pursuing rings of pick-pocketers, and searching for fake Native American art. HSI agents also undertook to train adult dancers on recognizing sex trafficking, inform older residents at retirement centers about lottery and IRA fraud, and teaching schoolchildren about the dangers of online predators.[75] In short, DHS in New Mexico has performed the role of local law enforcement, right down to grade-school outreach. That involvement was paired with a $28.6 million federal grant to New Mexico's homeland security department in 2014.[76] As DHS's mission-in-practice expanded from anti-terrorism, disaster relief, and border protection to broadly assisting local law enforcement, the department embedded HSI agents across New Mexico. A larger DHS, embedded and involved in local law enforcement, means more interactions with the public.

Those interactions come at a cost to privacy and civil liberties. As DHS's size and mission expanded from 2004 to the present, civil liberties complaints skyrocketed. In 2005-06, the first year

---

[72] Editorial Board, Editorial: Homeland's 'mission creep' works on three levels, Albuquerque J. (May 4, 2014), https://www.abqjournal.com/393959/homelands-mission-creep-works-on-3-levels.html.
[73] Michael Coleman, MISSION CREEP: NM footprint grows: 'We've up-armored', Albuquerque J (Apr. 28, 2014), https://www.abqjournal.com/390807/nm-footprint-grows-weve-uparmored.html.
[74] *Id.*
[75] *Id.*
[76] *Id.*

on record, DHS's Office for Civil Rights and Civil Liberties (CRCL) received 300 complaints.[77] Thirteen years later, in 2018, CRCL reports receiving 4,244 complaints a 20 percent increase over 2017 and a 1,300 percent increase over 2005-06.[78] The 2018 complaints included 228 allegations of discrimination/profiling, 1,866 complaints of denial of due process, 99 complaints of excessive force, 5 complaints of free speech violations, 32 complaints of Fourth Amendment search and seizure violations, 28 complaints of failure to provide religious accommodations, and 108 allegations of sexual abuse or assault.[79]

Beyond individual complaints, DHS's expanding mission led to extraordinary surveillance of Black Lives Matter protests this summer. The department flew surveillance planes, helicopters, and drones over at least 15 cities to monitor First Amendment protected activities in the wake of George Floyd's death.[80] At the end of June DHS began collecting personal information on individuals believed to be a threat to "damage or destroy any public monument, memorial, or statue".[81] Although few, if any, would consider defacing a statue to be a threat to homeland security, DHS appears to have expanded its reach to include monitoring individual protesters.

While funding has traditionally been identified as driving mission creep, access to information can serve the same function. In short, when you give someone a hammer, he will find that most things he encounters need a pounding. Here adding millions of individuals to DHS

---

[77] Michael Chertoff, 2005-06 U.S. Department of Homeland Security Office for Civil Rights and Civil Liberties Report to Congress at 35 (Feb. 28, 2007), https://www.dhs.gov/sites/default/files/publications/crcl-annual-2005-2006.pdf.
[78] Cameron P. Quinn, Fiscal Year 2018 Report to Congress, U.S. Dep't. of Homeland Sec. Off. for Civil Rights and Civil Liberties at 4 (Nov. 18, 2019), https://www.dhs.gov/sites/default/files/publications/crcl-fy-2018-annual-report_0.pdf.
[79] *Id* at 40.
[80] Zolan Kanno-Youngs, U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance, N.Y. Times (June 19, 2020), https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html.
[81] Steve Vladek and Benjamin Wittes, DHS Authorizes Domestic Surveillance to Protect Statues and Monuments, Lawfare (July 20, 2020) (quoting a DHS memo), https://www.lawfareblog.com/dhs-authorizes-domestic-surveillance-protect-statues-and-monuments.

biometric databases runs the risk that the department will expand its involvement in local law enforcement and monitoring of protected activities. In particular, adding biometrics from US citizens as standard practice will enable surveillance of populations beyond DHS's historical ambit. The new modalities, particularly facial recognition, may open up avenues of comprehensive surveillance previously impossible for the department. Use of these tools risks sweeping up 1st Amendment protected activity like protesting as well as involving DHS deeper in local law enforcement.

III. Facial recognition is a particularly dangerous surveillance technology and DHS should immediately suspend its use

As DHS noted in the NPRM, the agency has collected facial photographs for some time now.[82] Of course, most of this collecting took place well before individuals even considered that their photographs would be used as a biometric modality for facial recognition. These photographs have traditionally been used to create secure identity documents (e.g. permanent resident card). DHS now proposes to unilaterally decide to use all the facial photographs previously collected and future facial photographs for a "facial recognition system."[83] This decision will effectively create a digital ID controlled by the government. This along with the ease in which facial images can be obtained and facial recognition technology can be expanded poses serious threats to privacy and civil liberties.

Facial recognition can be deployed covertly, remotely, and on a mass scale. There is a lack of well-defined regulations controlling the collection, use, dissemination, and retention of biometric identifiers, particularly for face recognition. Ubiquitous identification via facial recognition by the government eliminates the individual's ability to control the disclosure of their identities, creates new opportunities for tracking and monitoring, and increases the security risks from data breaches.

[82] NPRM at 56356.
[83] *See* NPRM at 56356.

An individual's ability to control disclosure of his or her identity is an essential aspect of personal freedom and autonomy. The use of facial recognition erodes these freedoms.

There is little a person in the United States could do to prevent the capture of their image by the government if face surveillance is deployed. Participation in society necessarily requires participation in public spaces. But ubiquitous and near effortless identification eliminates the individual's ability to control the disclosure of their identities to others. Strangers will know our identities as readily as our friends and family members.

In addition to the serious privacy and civil liberties implications, facial recognition systems have shown gender and racial bias. A recent National Institute of Standards and Technology (NIST) study on Facial Recognition Software generally found false positives and/or false negatives to be higher for people of color, females, children, and the elderly.[84] The NIST study aligns with previous studies that have demonstrated racial and gender bias in facial recognition algorithms.[85]

There is a growing movement across the United States to ban the use of facial recognition by government entities as the dangers of the technology are recognized. A growing list of cities have already banned its use, including Portland, Boston, Oakland, and San Francisco. DHS should heed these warnings and suspend the agency's use of facial recognition technology.

IV. Conclusion

DHS's proposed rule to expand the collection and use of biometric modalities and information is ill-advised. DHS should immediately rescind the proposed rule and commit to

[84] 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.
[85] *See, e.g.*, Joy Buolamwini, Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* (Feb. 2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; C.M. Cook, J.J. Howard, et al., Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems, in *IEEE Transactions on Biometrics, Behavior, and Identity Science* (Jan. 2019), https://ieeexplore.ieee.org/document/8636231.

narrowing the use of biometrics to the bare minimal needed to affect its mission. Additionally, DHS should immediately suspend the use of facial recognition technology—the technology is too fraught with privacy and civil liberties risks to even consider government use without comprehensive and strict regulation in place.

Respectfully Submitted,

Jeramie Scott
Jeramie Scott
Senior Counsel

Jake Wiener
Jake Wiener
EPIC Kennedy Fellow