PROJECT ON GOVERNMENT OVERSIGHT

The Honorable Saeed Mody
Deputy Associate Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

January 19, 2024

Re: Request for Comment on Law Enforcement Agency Use of Facial Recognition Technology and Other Biometric Data Collection Technologies

Dear Deputy Associate Attorney General Mody:

The Project On Government Oversight (POGO) submits the following comment to the Department of Homeland Security, the Department of Justice, and the White House Office of Science and Technology Policy as they seek to fully implement President Joe Biden's May 2022 Executive Order 14074, on "Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety."[1] This executive order charged the attorney general, secretary of Homeland Security, and director of the Office of Science and Technology Policy to jointly develop a report assessing "use by LEAs [law enforcement agencies] of facial recognition technology, other technologies using biometric information, and predictive algorithms, as well as data storage, and access regarding such technologies."[2]

Founded in 1981, POGO is a nonpartisan, independent watchdog that investigates and exposes waste, corruption, abuse of power, and when the government fails to serve the public or silences those who report wrongdoing. We champion reforms to achieve a more effective, ethical, and accountable federal government that safeguards constitutional principles.

We offer this commentary to ensure that President Biden's executive order is fully implemented, which means that any report must examine all facets of federal law enforcement within the Department of Homeland Security (DHS). We also provide recommendations on specific limitations that federal law enforcement should adopt to protect rights as it collects and uses biometric data.

Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE), for example, represent two of the largest federal law enforcement agencies in the country and are already engaged in extensive activities that affect privacy and other civil rights of those with

[1] Executive Order No. 14074, 87 Fed. Reg. 32945 (May 25, 2022), https://www.federalregister.gov/documents/2022/05/31/2022-11810/advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and.
[2] Executive Order No. 14074 [see note 1].

whom the agencies' officers interact.[3] We believe that this interagency process cannot meet the requirements of Section 13(e) of Executive Order 14074 without a full and comprehensive examination of the deployment, use, and impact of facial recognition technology and biometric information collection within all components of DHS law enforcement.

POGO has engaged in extensive work monitoring the operations of the Justice Department and DHS and its relevant components, advocating for reforms that would curtail law enforcement abuses caused by overly intrusive and unaccountable surveillance.[4] We have long sought safeguards that would protect rights and promote accountability among federal law enforcement and the intelligence community, especially with regard to its surveillance activities.[5] POGO has been a leading expert on the impact of government surveillance technologies, including the proliferation of facial recognition at the federal, state, and local levels, as well as the potential abuses of the use of such technology and other biometric technologies such as DNA collection.[6]

In identifying best practices to protect privacy, civil rights, and civil liberties, the forthcoming report must grapple with the largely unaccountable and opaque components of DHS operations to understand the extent of facial recognition technology data sharing, deployment of other biometric technology, and their harms. In addition to analyzing the use of biometric collection technology by specific DHS law enforcement and quasi-law enforcement entities, it is essential for the report to analyze and develop best practices for other components within the agency that

---

[3] Department of Justice Bureau of Justice Statistics, "Federal Law Enforcement Officers, 2020 – Statistical Tables," Revised September 29, 2023, 4, https://bjs.ojp.gov/document/fleo20st.pdf; Laperruque, Jake, "ICE Backs Down on 'Extreme Vetting' Automated Social Media Scanning," Project On Government Oversight, May 23, 2018, https://www.pogo.org/analysis/ice-backs-down-on-extreme-vetting-automated-social-media-scanning; Hawkins, Katherine, *The Border Zone Next Door, and Its Out-of-Control Police Force*, Project On Government Oversight, January 10, 2023, https://www.pogo.org/reports/the-border-zone-next-door-and-its-out-of-control-police-force.

[4] "Protecting Civil and Human Rights," Project On Government Oversight, accessed January 10, 2024, https://www.pogo.org/issue/protecting-civil-and-human-rights.

[5] Laperruque, Jake, "A Proposed Agenda for a New PCLOB," Project On Government Oversight, August 29, 2018, https://www.pogo.org/analysis/a-proposed-agenda-for-a-new-pclob.

[6] The Constitution Project's Task Force on Facial Recognition Surveillance and Jake Laperruque, *Facing the Future of Surveillance*, Project On Government Oversight, March 4, 2019, https://www.pogo.org/reports/facing-the-future-of-surveillance; *Law Enforcement Use of Facial Recognition: The Presidential Commission on Law Enforcement and Administration Technology Working Group* (April 22, 2020) (testimony of Jake Laperruque, senior counsel, The Constitution Project at the Project On Government Oversight), https://www.pogo.org/testimonies/facial-recognition-technology-strong-limits-are-necessary-to-protect-public-safety-civil-liberties; Letter from Danielle Brian, executive director of the Project On Government Oversight and Jake Laperruque, policy counsel at The Constitution Project at The Project On Government Oversight, to Merrick Garland, U.S. attorney general, about Justice Department safeguards against surveillance, March 10, 2021, https://www.pogo.org/policy-letters/pogo-calls-on-justice-department-to-enact-safeguards-against-surveillance; Laperruque, Jake, "Geofence Warrants: The Last Piece of the Location Privacy Puzzle," Project On Government Oversight, August 25, 2021, https://www.pogo.org/analysis/geofence-warrants-the-last-piece-of-the-location-privacy-puzzle; Laperruque, Jake, and David Janovsky, "These Police Drones are Watching You," Project On Government Oversight, September 25, 2018, https://www.pogo.org/analysis/these-police-drones-are-watching-you; Laperruque, Jake, "Key Facts About Face Recognition for Policymaking," Project On Government Oversight, August 24, 2021, https://www.pogo.org/analysis/key-facts-about-face-recognition-for-policymaking; Jake Laperruque, senior counsel, The Constitution Project at The Project On Government Oversight, and Katherine Hawkins, senior legal analyst, The Constitution Project at The Project On Government Oversight, to Office of Legal Policy, Department of Justice, about DNA collection from immigration detainees, November 12, 2019, https://www.pogo.org/public-comments/pogo-comment-on-dna-collection-from-immigration-detainees.

potentially use facial recognition and biometric collection technologies to support law enforcement operations inside and outside of DHS.

While we confine our comments to the conduct of DHS law enforcement activities, components within the Department of Justice (DOJ) engaged in biometric data collection should also be rigorously examined by the forthcoming review. Within DOJ, the FBI, Federal Bureau of Prisons; U.S. Marshals Service; Bureau of Alcohol, Tobacco, Firearms and Explosives; and Drug Enforcement Administration have used facial recognition technology, and the FBI and Federal Bureau of Prisons operate their own face identification systems.[7] POGO has written on the FBI's system in the past:

> The FBI oversees a massive face recognition system through its Facial Analysis, Comparison, and Evaluation Services Unit, with capacity to scan hundreds of millions of photos, including nearly one out of every three drivers' license photos. In addition to conducting face recognition scans for its own investigations, the FBI also employs its Next Generation Identification-Interstate Photo System to process requests for scans largely from state and local law enforcement. The FBI no longer discloses how many face recognition searches it runs, but it previously processed as many as 8,000 searches per month on average.[8]

The FBI, using the Combined DNA Index System (CODIS), also holds the DNA profiles of millions of individuals.[9] The very same limits that are needed to ensure DHS protects constitutional rights as it collects biometric data must apply to *any* federal law enforcement entity.

Unrestricted Biometric Collection Technologies Reinforce Discriminatory Policing Practices

The U.S. government has increased its biometric surveillance capability — from facial recognition to iris scans to DNA collection — too broadly, too quickly, and with too much secrecy.[10] While the government has a legitimate interest in protecting public safety, it has deployed biometric technology in the name of security without due consideration of the extraordinary threat that massive collection of such sensitive data presents to the functioning of a free society.[11]

---

[7] Government Accountability Office, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, GAO-21-518 (2021), 9, https://www.gao.gov/assets/gao-21-518.pdf.
[8] Laperruque, Jake, Comment in Response to Request for Information on Public and Private sector Uses of Biometric Technologies (January 18, 2022), https://www.pogo.org/resources/pogo-proposes-strong-limits-on-face-recognition-to-white-house-office-of-science-and-technology-policy.
[9] CODIS-NDIS Statistics," Federal Bureau of Investigation, last modified August 2023, https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis/codis-ndis-statistics.
[10] The Constitution Project's Task Force on Facial Recognition Surveillance and Jake Laperruque, *Facing the Future of Surveillance* [see note 6].
[11] Laperruque, Jake, "A Day Without the Fourth Amendment," Project On Government Oversight, September 20, 2018, https://www.pogo.org/analysis/a-day-without-the-fourth-amendment; Hussain, Saira and Matthew Guariglia, "The U.S. Government's Database of Immigrant DNA Has Hit Scary, Astronomical Proportions," Electronic Frontier Foundation, September 25, 2023, https://www.eff.org/deeplinks/2023/09/us-governments-database-immigrant-dna-has-hit-scary-astronomical-proportions.

There is a long and shameful history of illegal and overbroad government surveillance of historically marginalized communities and groups, often a result of members of those communities exercising constitutionally protected rights. Ga number of dangers. These are extraordinarily powerful tools and their use must be heavily scrutinized to prevent misidentification, technology creep that eviscerates privacy rights, and deployment that reinforces discriminatory policing practices.

Facial recognition, in particular, presents several threats to privacy and other civil rights. The technology is prone to inaccuracy, which has led to false arrests.[12] Many algorithms used by these technologies misidentify women and people of color at a higher rate than other people, undermining investigations and endangering civil rights.[13] Facial recognition's reliability is highly variable, dependent upon lighting, angles, and resolution, as well as the "confidence thresholds" set by law enforcement.[14] It has been used by state and federal law enforcement to chill constitutionally protected activities, like protesting.[15]

Law enforcement often state that the technology is only used for "investigative leads," but this use can have several downstream negative consequences as well.[16] Defendants are often not informed that facial recognition formed the basis of their arrest, depriving them of an opportunity to examine its reliability. Without any limits on how law enforcement can use facial recognition, the technology can, as the seventh circuit found, fundamentally "alter the relationship between citizen and government in a way that is inimical to democratic society" as its use becomes more pervasive.[17]

---

[12] Hill, Kashmir, "Eight Months Pregnant and Arrested After False Facial Recognition Match," *New York Times*, August 6, 2023, https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.

[13] Grother, Patrick, Mei Ngan, and Kayee Hanaoka, National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280 (December 19, 2019), 2, https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf; Buolamwini, Joy, and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 81 (2018), 8, https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Snow, Jacob, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots," American Civil Liberties Union, July 26, 2018, https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28; Klare, Brandan et al., "Face Recognition Performance: Role of Demographic Information," *IEEE Transactions on Information Forensics and Security* 7, no. 6 (December 2012), 13, http://openbiometrics.org/publications/klare2012demographics.pdf.

[14] Laperruque, Jake, "About-Face: Examining Amazon's Shifting Story on Facial Recognition Accuracy," Project On Government Oversight, April 10, 2019, https://www.pogo.org/analysis/about-face-examining-amazon-shifting-story-on-facial-recognition-accuracy.

[15] Garvie, Clare and Neema Singh Guliani, "Lawmakers Need to Curb Face Recognition Searches by Police," American Civil Liberties Union, October 26, 2016, https://www.aclu.org/news/privacy-technology/lawmakers-need-curb-face-recognition-searches.; Turner Lee, Nicol, and Caitlin Chin-Rothmann, "Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color," Brookings, April 12, 2022, https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

[16] Laperruque, *Law Enforcement Use of Facial Recognition* [see note 6].

[17] Mak, Aaron, "Facing Facts: A case in Florida demonstrates the problems with using facial recognition to identify suspects in low-stakes crimes," *Slate*, January 25, 2019, https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html; United States v. Cuevas-Perez, 640 F. 3d 272, 285 (CA7 2011) (Flaum, J., concurring).

Mass collection of DNA presents dangers that are equally concerning, if not more. DNA contains some of the most sensitive information about an individual, and law enforcement's possession of it opens the door to government revealing important connections between people through genetic identification.[18] Mass collection of DNA could chill engagement in constitutionally protected activities. For example, DNA collection could allow the government to catalogue participants in a protest by simply testing the remnants of trash or debris found at the protest site. The involuntary collection of DNA from millions of people could become the basis for denying public benefits, medical treatments, or immigration status, which is of particular concern given the troubling history of eugenics policies in this country. As we wrote in 2019:

> Researchers have theorized that DNA could be used to identify personality traits, intelligence, sexual orientation, political affiliations, and inclination to commit crimes. And the ability to identify these or other sensitive traits does not need to be fully developed or accurate, just simply convincing enough, to be applied.[19]

Large-scale DNA collection from those disconnected from criminal activity, such as migrants, also circumvents due process systems established for use of DNA in a law enforcement context, where individuals can typically have their DNA sample expunged absent a criminal conviction.[20]

As we explain below, DHS components' access to biometric collection technology is particularly concerning given the size of the agency, in addition to its documented lack of accountability for abuses when they do occur.[21] The expanse of DHS law enforcement activities makes scrutiny of this agency's policies and practices in the collection and use of biometric data urgent.

DHS Law Enforcement Components Fall Under the Executive Order's Purview

The U.S. Department of Homeland Security has a sprawling mandate across nine agencies and offices, several of which engage in law enforcement activities, such as conducting criminal investigations and making arrests on a frequent basis.[22] Two of DHS's largest components — CBP and ICE — conduct traditional law enforcement activities within the interior of the U.S. and along the border. These two law enforcement entities possess extraordinary resources and expansive enforcement powers and jurisdiction, making scrutiny of their use of biometric data fundamental to developing appropriate best practices that address privacy, civil rights, civil liberties, and equity.

---

[18] Jake Laperruque and Katherine Hawkins, to Office of Legal Policy, Department of Justice, about DNA collection from immigration detainees [see note 6].
[19] Jake Laperruque and Katherine Hawkins, to Office of Legal Policy, Department of Justice, about DNA collection from immigration detainees [see note 6].
[20] Jake Laperruque and Katherine Hawkins, to Office of Legal Policy, Department of Justice, about DNA collection from immigration detainees [see note 6].
[21] Turberville, Sarah and Chris Rickerd, *An Oversight Agenda for Customs and Border Protection: America's Largest, Least Accountable Law Enforcement Agency,* Project On Government Oversight, October 12, 2021, https://www.pogo.org/reports/an-oversight-agenda-for-customs-and-border-protection-americas-largest-least-accountable-law-enforcement-agency.
[22] Law Enforcement," Department of Homeland Security, last modified January 5, 2024, https://www.dhs.gov/ohss/topics/law-enforcement.

The forthcoming report will be woefully inadequate if it does not collect information regarding the policies and guidelines that govern the deployment, use, and facilitation of biometric collection technology and data in the law enforcement components of DHS.

By CBP's own estimation, it is the largest federal law enforcement agency in the country, employing 25,836 law enforcement officers in the Office of Field Operations, which is responsible for overseeing the operations at ports of entry, and 19,357 law enforcement officers in the U.S. Border Patrol, which is responsible for patrolling the border between ports of entry.[23] CBP has continuous and far-reaching engagement with the public. In fiscal year 2023, CBP had over 3 million enforcement encounters and conducted over 40,000 electronic device searches.[24]

ICE employs over 20,000 law enforcement and support personnel.[25] More than 13,000 law enforcement personnel are housed in Enforcement and Removal Operations, which is charged with arrests and removals of people from the interior of the United States, and Homeland Security Investigations, which engages in federal investigations of terrorist and transnational criminal organization activity.[26] These law enforcement personnel are based across the country in field offices — 25 for Enforcement and Removal Operations and 31 for Homeland Security Investigations.[27] In fiscal year 2023, Enforcement and Removal Operations made 170,590 arrests and conducted 142,580 removals while Homeland Security Investigations made 33,108 criminal arrests.[28]

It is well known that ICE operates within the interior of the U.S., but CBP also possesses broad authority to set up checkpoints and stop, search, and arrest people without probable cause within the country. Federal law provides that "immigration officers" (in practice, usually CBP employees, though the term also encompasses ICE officers) can conduct stops and searches without a warrant "within a reasonable distance from any external boundary" of the United States.[29] Decades-old federal regulations, issued without public comment or debate, define that

---

[23] Department of Homeland Security, "U.S. Customs and Border Protection Snapshot: A Summary of CBP Facts and Figures, May 2023, 1, https://www.cbp.gov/sites/default/files/assets/documents/2023-May/cbp-snapshot-fy2022-stats.pdf; "Executive Assistant Commissioners' Offices," Department of Homeland Security, last modified November 27, 2023, https://www.cbp.gov/about/leadership-organization/executive-assistant-commissioners-offices; "Border Patrol Overview," Department of Homeland Security, last modified May 17, 2023, https://www.cbp.gov/border-security/along-us-borders/overview.

[24] "Nationwide Encounters," Department of Homeland Security, last modified December 22, 2023, https://www.cbp.gov/newsroom/stats/nationwide-encounters; "CBP Enforcement Statistics," Department of Homeland Security, last modified December 22, 2023, https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics.

[25] "U.S. Immigration and Customs Enforcement," Department of Homeland Security, last modified January 2, 2024, https://www.ice.gov/about-ice.

[26] "Enforcement and Removal Operations," Department of Homeland Security, last modified June 27, 2023, https://www.ice.gov/about-ice/ero; "Homeland Security Investigations," Department of Homeland Security, last modified April 14, 2023, https://www.ice.gov/about-ice/homeland-security-investigations.

[27] "ICE Field Offices," Department of Homeland Security, last modified October 2, 2023, https://www.ice.gov/contact/field-offices.

[28] Department of Homeland Security U.S. Immigration and Customs Enforcement, "ICE Releases Fiscal Year 2023 Annual Report," Press Release, December 29, 2023, https://www.ice.gov/news/releases/ice-releases-fiscal-year-2023-annual-report.

[29] 8 U.S.C. § 1357(a)(3) (2022), https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title8-section1357&num=0&edition=prelim.

reasonable distance as "100 air miles" from any external boundary, including the Atlantic and Pacific Oceans and the Gulf of Mexico, in addition to the land borders with Mexico and Canada.[30] Almost two thirds of the U.S. population live in this border enforcement zone, which includes virtually the entire states of Connecticut, Delaware, Florida, Hawaii, Maine, Maryland, Massachusetts, Michigan, New Hampshire, New Jersey, New York, Rhode Island, and Vermont, as well as most of the largest cities in the country.[31]

Within this vast enforcement zone, Border Patrol can set up checkpoints to stop and question every driver based on no suspicion whatsoever.[32] These checkpoints are a daily fact of life for many residents of Southern border communities spanning from Southern California to the Rio Grande Valley.[33] For non-citizens and citizens alike, they can lead to inconvenience, racial profiling, and surveillance.[34] Most citizens are waved through, but some have been subjected to detention and serious human rights violations, and the risks to non-citizens are much greater.[35] Collection of biometric data by CBP has become a part of these interactions.

CBP agents can also board buses and trains and check the immigration status of the people on board if the company's owner or an employee consents.[36] Agents can set up roving patrols to stop cars if they have a "reasonable suspicion" of anyone committing an immigration violation on board.[37]

Furthermore, the pernicious practice of racial profiling is widespread by CBP.[38] Unlike CBP, ICE is not permitted to use racial profiling within the interior of the United States — but it can stop, arrest, and search people based on "reasonable suspicion." A "reasonable suspicion" in

---

[30] 8 C.F.R. § 287.1 (2022), https://www.ecfr.gov/current/title-8/chapter-I/subchapter-B/part-287/section-287.1.
[31] Misra, Tanvi, "Inside the Massive U.S. 'Border Zone,'" *Bloomberg CityLab*, May 14, 2018, https://www.bloomberg.com/news/articles/2018-05-14/mapping-who-lives-in-border-patrol-s-100-mile-zone.
[32] U.S. v. Martinez-Fuerte, 428 US 543 (1976), Jones, Reece, "The long, deep reach of the U.S. Border Patrol," *Los Angeles Times*, July 17, 2022, https://www.latimes.com/opinion/story/2022-07-17/border-patrol-border-zone-supreme-court-search-checkpoint.
[33] Government Accountability Office, *Border Patrol: Actions Needed to Improve Checkpoint Oversight and Data*, GAO-22-104568 (June 2022), 10, https://www.gao.gov/assets/730/720899.pdf#page=16.
[34] Burnett, John, "Fearing Checkpoints, Undocumented Immigrants Cut Off From Medical Care," NPR, November 3, 2017, https://www.npr.org/2017/11/03/561883665/fearing-checkpoints-undocumented-immigrants-cut-off-from-medical-care; Mejía Lutz, Elena, "At Border Patrol Checkpoints, an Impossible Choice Between Health Care and Deportation," *Texas Observer*, February 13, 2018, https://www.texasobserver.org/border-patrol-checkpoints-impossible-choice-health-care-deportation/; Eltagouri, Marwa, "A 10-year-old immigrant was rushed to the hospital in an ambulance. She was detained on the way," *Washington Post*, October 27, 2017, https://www.washingtonpost.com/news/post-nation/wp/2017/10/26/a-10-year-old-immigrant-was-rushed-to-the-hospital-in-an-ambulance-she-was-detained-on-the-way/; Romero, Dennis "U.S. citizen says he lost 26 pounds while wrongfully held in 'inhumane' conditions," NBC News, July 27, 2019, https://www.nbcnews.com/storyline/immigration-border-crisis/u-s-citizen-says-he-lost-26-pounds-while-wrongfully-n1035321.
[35] Flynn, Meagan, "U.S. citizen freed after nearly a month in immigration custody, family says," *Washington Post*, July 24, 2019, https://www.washingtonpost.com/nation/2019/07/23/francisco-erwin-galicia-ice-cpb-us-citizen-detained-texas/.
[36] Smith, Hillel R. and Kelsey Y. Santamaria, Congressional Research Service, *Searches and Seizures at the Border and the Fourth Amendment*, R46601 (March 30, 2021), CRS-65, https://sgp.fas.org/crs/homesec/R46601.pdf.
[37] Hillel R. Smith and Kelsey Y. Santamaria, *Searches and Seizures at the Border* [see note 36].
[38] United States v. Brignoni-Ponce, 422 U.S. 873 (1975); United States v. Martinez-Fuerte, 428 U.S. 543 (1976).

theory should be based on specific facts about a person or their actions, but in practice can be almost anything.[39]

Given the scope of CBP and ICE's authority — coupled with the lack of accountability for the agencies' abuses of citizens and non-citizens — the interagency working group must scrutinize the collection and use of biometrics by these entities. While their law enforcement activities may be conducted under the auspices of immigration enforcement and border security, fundamentally these are law enforcement entities that engage extensively with the public within the interior of the United States.

How Biometric Data Is Collected By DHS's Quasi-Law Enforcement Entities

In addition to CBP and ICE, other law enforcement and quasi-law enforcement entities within DHS interact with the public, collect and use biometric data, or facilitate use of biometric data by law enforcement. Careful scrutiny is required to assess the threat that current practices pose to civil rights and civil liberties.

These other entities within DHS using biometric data include the U.S. Secret Service, charged with investigations of threats to U.S. heads of states and certain financial crimes, which made 893 arrests in fiscal year 2022, and the Federal Protective Service, a police force responsible for protecting the more than 9,000 federal buildings around the nation.[40] In fiscal year 2020, the Federal Protective Service supported more than 534,000 calls for service and had over 1,600 arrests and citations issued.[41] The broad authority granted to this entity has led to abuses. One such example took place in 2020, when Federal Protective Service officers, along with the several other federal law enforcement agents, tear gassed and engaged in physical altercations with protesters during racial justice protests in Portland, Oregon.[42]

Another DHS component is the Transportation Security Administration (TSA). While there is only a fraction of sworn law enforcement officers within the TSA relative to agencies like CBP and ICE, the quasi-law enforcement aspects of this agency have a dramatic impact on the public through the agency's widespread use of biometric collection technology. Originally deployed to

[39] Surana, Kavitha, "How Racial Profiling Goes Unchecked in Immigration Enforcement," *ProPublica*, June 8, 2018, https://www.propublica.org/article/racial-profiling-ice-immigration-enforcement-pennsylvania; ACLU of Michigan, *The Border's Long Shadow*, (March 25, 2021), 32-33, https://www.aclumich.org/sites/default/files/field_documents/100_mile_zone_report-updated.pdf.

[40] 18 U.S.C. § 3056, https://uscode.house.gov/view.xhtml?req=(title:18%20section:3056; U.S. Department of Homeland Security, United States Secret Service, *FY 2022 Annual Report*, 48, https://www.secretservice.gov/sites/default/files/reports/2023-02/fy-2022-annual-report-final.pdf; "Operations," Department of Homeland Security, last modified June 2, 2023, https://www.dhs.gov/fps-operations.

[41] Department of Homeland Security Federal Protective Service, "Federal Protective Service At A Glance," 3-4, https://www.dhs.gov/sites/default/files/publications/fps_at_a_glance.pdf.

[42] Wilson, Conrad, "DHS sent more than 750 federal officers, spent millions responding to Portland protests," *Oregon Public Broadcasting*, updated April 22, 2021, https://www.opb.org/article/2021/04/21/dhsreport-says-750-federal-officers-sent-to-2020-protests-in-portland/.

30 airports, facial recognition technology was planned to dramatically expand to more than 400 federalized airports across the country.[43]

DHS's Office of Biometric Identity Management greatly affects law enforcement operations as a coordinating entity. The office is responsible for providing biometric matching, sharing, and analysis for DHS components and interagency partners.[44] It manages the biometric system of record.[45] This biometric data is housed in the Automated Biometric Identification System, or "IDENT." The Office of Biometric Identity Management is actively engaged in transitioning the system to the Homeland Advanced Recognition Technology system, or "HART," a system that will, according to DHS, "store and process biometric data (digital fingerprints, iris scans, facial images (including a photo)"— and link biometrics with biographic information to facilitate the establishment and verification of identities.[46] It will become a massive repository for biometric data once completed with data providers including DHS, DOJ, the intelligence community, the Department of Defense, and TSA, among others.[47] Through this DHS office, approximately 16 million facial recognition searches were conducted in 2019.[48]

Finally, there are intelligence gathering and analysis entities within DHS, for which little is known concerning their collection or use of biometric data. These entities include the Office of Intelligence and Analysis, which shares vast amounts of data with DHS components, as well as with state and local law enforcement agencies.[49] The approximately 700 employees in this office collect, analyze, and disseminate information by engaging with data from varying sources, interacting with law enforcement agencies around the country through their intelligence reports, and working within fusion centers.[50]

During the 2020 protests in Portland, Oregon, the Brennan Center reported that the Office of Intelligence and Analysis authored dossiers of people cited or arrested during that period.[51] In creating the dossiers, the office searched protester names "through government travel and immigration systems, commercial data sets, and some systems the government would not publicly reveal."[52] The dossiers were provided to DHS political leadership and the Federal

---

[43] Department of Justice Bureau of Justice Statistics, "Federal Law Enforcement Officers, 2020 – Statistical Tables," [see note 3]. Transportation Security Administration, "Facial Recognition Technology," accessed January 12, 2024, https://www.tsa.gov/news/press/factsheets/facial-recognition-technology.
[44] "Office of Biometric Identity Management," Department of Homeland Security, last modified November 20, 2023, https://www.dhs.gov/obim.
[45] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART) Increment 1 PIA*, DHS/OBIM/PIA-004, (February 24, 2020), 2, https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf.
[46] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Homeland Advanced Recognition Technology System*, 2 [see note 45].
[47] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Homeland Advanced Recognition Technology System*, 5 [see note 45].
[48] Government Accountability Office, *Facial Recognition Technology:… Privacy and Other Risks*, 65 [see note 7]
[49] Reynolds, Spencer and Faiza Patel, Brennan Center for Justice, *A New Vision for Domestic Intelligence: Fixing Overbroad Mandates and Flimsy Safeguards* (March 30, 2023), 2, https://www.brennancenter.org/our-work/policy-solutions/new-vision-domestic-intelligence.
[50] Reynolds and Patel, *A New Vision for Domestic Intelligence,* 2 [see note 49].
[51] Reynolds and Patel, *A New Vision for Domestic Intelligence,* 3 [see note 49].
[52] Reynolds and Patel, *A New Vision for Domestic Intelligence,* 3 [see note 49].

Protective Service, and led to the revelation that this practice occurred "thousands" of times before.[53]

Given the alarming scope of intelligence collection within the Office of Intelligence and Analysis and the secrecy surrounding what government databases are being used, it is critical to review the extent to which quasi-law enforcement components like that office are seeking out biometric information and engaging with data received from other agencies that utilize facial recognition technology. Additionally, it is important to examine how other components plan to use facial recognition technology in the future.

DHS's Increasing Use of Biometric Data

Across DHS, law enforcement and quasi-law enforcement agencies have dramatically expanded the use of biometric data collection technology. Among law enforcement agencies, the deployment and use of these technologies has permeated into fundamental law enforcement operations, from collecting DNA after an arrest of a noncitizen within CBP and ICE to conducting facial recognition searches to create investigative leads for Homeland Security Investigations.[54] DHS law enforcement use these technologies within the interior of the country, particularly — but not only — on migrants.[55]

For example, 52 Border Patrol checkpoints located within the interior of the U.S. are equipped with fingerprint readers.[56] ICE used mobile fingerprinting technology to assist in deportations, including during traffic stops and against bystanders swept up in immigration raids.[57] Given the lack of publicly available data, it is unclear if this technology is still being utilized today, and if so at what scale. DHS law enforcement's most prolific collection of biometric data, however, takes three forms: facial recognition, iris scanning, and DNA collection.

Facial Recognition

By far, the most widespread use of biometric data collection comes from facial recognition platforms. DHS law enforcement states that it uses facial recognition technology to identify travelers entering and exiting the country, to "develop investigative leads," and to assist in criminal investigations.[58] This data collection persists despite a lack of clear congressional authorization to collect such data from U.S. citizens. And even seemingly mundane daily interactions that incorporate the use of facial recognition technology and other biometric surveillance technologies can have a dramatic impact on citizens and non-citizens alike.

---

[53] Reynolds and Patel, *A New Vision for Domestic Intelligence,* 3 [see note 49].
[54] Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties,* GAO-23-105607 (2023) 13-14, https://www.gao.gov/assets/gao-23-105607.pdf.
[55] Hawkins, *The Border Zone Next Door* [see note 3].
[56] Hawkins, *The Border Zone Next Door* [see note 3].
[57] Bajak, Frank, "Report: Mobile fingerprinting a core tool in US deportations," Associated Press, November 23, 2020, https://apnews.com/article/donald-trump-freedom-of-information-freedom-of-information-act-lawsuits-immigration-0fac264dc20da65c3e5924174f9db5aa.
[58] Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training,* 13-14 [see note 54].

After examining several biometric collection pilot programs, DHS decided that facial recognition was the preferred method of widespread biometric collection for the purpose of identifying travelers.[59] CBP uses facial recognition technology at many airports, seaports, and land ports of entry.[60] U.S. citizens are permitted to request alternative means of verifying identity, but very few non-citizens are allowed to do so, and in practice agents do not always respect a U.S. citizen's attempt to opt out.[61] At airports, the technology is widely deployed, based in 238 locations.[62] CBP estimates that it has processed a staggering 300 million travelers using biometric facial comparison technology.[63] Although CBP purports not to use facial recognition on the new CBP One app, for users to schedule appointments at a port of entry or seek travel authorization for parole processes, they must submit a photo for a "liveness check."[64] ICE is also increasingly relying on facial recognition to track migrants in its "alternative to detention" program.[65]

The Border Patrol routinely collects fingerprints, iris images, photographs, and facial scans of detained migrants and enters them into multiple government databases.[66] Border Patrol agents also collect biometric information from individuals and search it against several government databases.[67] As of July 2023, 163 land border checkpoints used "Biometric Facial Comparison Technology" for pedestrian entry points.[68] It should be noted that two of these crossings deployed the technology for vehicle crossings — in Buffalo, New York, and Brownsville, Texas — potentially highlighting an expansion of the technology being applied to vehicle crossings.[69]

---

[59] Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States, 85 Fed. Reg. 74,163, (November 19, 2020), https://www.govinfo.gov/content/pkg/FR-2020-11-19/pdf/2020-24707.pdf.
[60] "Where is it Deployed?" Department of Homeland Security, last modified January 4, 2024, https://www.cbp.gov/travel/biometrics.
[61] "TSA PreCheck: Touchless Identity Solution," Department of Homeland Security, accessed January 12, 2024, https://www.tsa.gov/biometrics-technology/evaluating-facial-identification-technology; Ovide, Shira, "You can say no to a TSA face scan. But even a senator had trouble." *Washington Post*, July 11, 2023, https://www.washingtonpost.com/technology/2023/07/11/tsa-airport-security-facial-recognition/.
[62] "Airports | CBP Biometrics", Department of Homeland Security, last modified November 29, 2023, https://www.cbp.gov/travel/biometrics/airports.
[63] "Where is it Deployed?", Department of Homeland Security [see note 60].
[64] "CBP One: An Overview," American Immigration Council, December 9, 2021, https://www.americanimmigrationcouncil.org/research/cbp-one-overview.
[65] Debusmann, Bernd Jr., "At US border, tech issues plague new migrant applications," BBC, March 9, 2023, https://www.bbc.com/news/world-us-canada-64814095; "Alternatives to Immigration Detention: An Overview," American Immigration Council, July 11, 2023, https://www.americanimmigrationcouncil.org/research/alternatives-immigration-detention-overview.
[66] Government Accountability Office, *Border Patrol: Actions Needed to Improve Checkpoint Oversight and Data*, [see note 33].
[67] Government Accountability Office, *Border Patrol: Actions Needed to Improve Checkpoint Oversight and Data*, 13 [see note 33].
[68] "Land Crossings," Department of Homeland Security, last modified July 13, 2023, https://www.cbp.gov/travel/biometrics/land-crossings.
[69] "Land Crossings," Department of Homeland Security [see note 68].

CBP, ICE, and the Secret Service reported that they used federal, state, local, and privately owned facial recognition systems.[70] Within ICE, Homeland Security Investigations agents used these systems to generate investigative leads and support criminal investigations.[71] From October 2019 through March 2022, the entity conducted over 15,000 searches.[72] CBP also stated that it used face recognition searches to develop and share information in support of other agencies' criminal investigations.[73] CBP was unable to provide information on the number of searches conducted because the agency did not track this information within the two services it used.[74] In the wake of the murder of George Floyd, the GAO found that six agencies used facial recognition on images of "individuals suspected of violating the law."[75] The description of what the alleged criminal offense was is all the more problematic, as three of the six agencies could not specify what the activity was.[76] CBP also used its Automated Targeting System in the wake of the January 6, 2021, insurrection to conduct facial recognition searches at the request of another agency.[77] Without an accountability structure and clear guidelines on when this technology can be used, the risk for misuse and abuse is high.

CBP, ICE, and the Secret Service have also used Clearview AI, a controversial facial recognition technology company.[78] Clearview AI's practices are particularly problematic because they routinely violated social media companies' terms of use by scraping billions of photos from their sites without the consent of users.[79] In addition, Clearview AI suffers from the same inaccuracies that plague facial recognition technology as a whole, and the company has overinflated the accuracy of its identifications.[80] In April 2020, the Secret Service halted the technology's use, after it was discovered that employees had been using free trials of Clearview AI to utilize facial recognition technology without authorization or training.[81]

---

[70] Government Accountability Office, *Facial Recognition Technology:… Privacy and Other Risks*, 12 [see note 7]; Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training,* 47 [see note 54].
[71] Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training,* 13 [see note 54].
[72] Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training,* 15 [see note 54].
[73] Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training,* 14 [see note 54].
[74] Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training,* 15 [see note 54].
[75] Government Accountability Office, *Facial Recognition Technology:… Privacy and Other Risks*, 17-18 [see note 7].
[76] Government Accountability Office, *Facial Recognition Technology:… Privacy and Other Risks*, 18 [see note 7].
[77] Government Accountability Office, *Facial Recognition Technology:… Privacy and Other Risks*, 19 [see note 7].
[78] Guardian staff and agency, "Clearview AI agrees to restrict use of face database," *Guardian*, May 9, 2022, https://www.theguardian.com/us-news/2022/may/09/clearview-chicago-settlement-aclu; Laperruque, Jake, "Face Recognition Is Far from the Sci-Fi Super-Tool Its Sellers Claim," *Project On Government Oversight,* April 16, 2021, https://www.pogo.org/analysis/face-recognition-is-far-from-the-sci-fi-super-tool-its-sellers-claim; Government Accountability Office, *Facial Recognition Technology:… Privacy and Other Risks*, 12 [see note 7].
[79] Guardian staff and agency, "Clearview AI agrees to restrict use of face database" [see note 78]; Laperruque, "Face Recognition Is Far from the Sci-Fi Super-Tool Its Sellers Claim" [see note 78].
[80] Laperruque, "Face Recognition Is Far from the Sci-Fi Super-Tool Its Sellers Claim" [see note 79].
[81] Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training,* 56 [see note 54].

Iris Scanning

DHS law enforcement entities also engaged in iris scanning. Within CBP, iris scanning began with a pilot program at a pedestrian crossing at Otay Mesa, California, in 2015.[82] The data was sent to the Office of Biometric Identity Management to identify non-citizens entering the country.[83] Since then, the collection of iris data has expanded. Today, CBP uses iris scanning at four checkpoints.[84] TSA also uses CLEAR, a private sector biometric company, to collect and verify face, iris, and fingerprint biometric data at over 50 airports.[85]

While CLEAR states that it does not share the information with other companies, biometric data for its 16 million users is held indefinitely.[86] According to U.S. Border Patrol official Jason Thompson, the Border Patrol began collecting iris images in 2014 and has collected over 1 million since then.[87] According to biometric data firm Iris ID, "the US Border Patrol collects up to one hundred thousand iris records per month."[88] In a law enforcement context, while iris records are checked by the Office of Biometric Identity Management for entry, there are no reports on how, if at all, these records are used in criminal investigations. DHS law enforcement can also search the FBI's Next Generation Identification Iris Service, which has over two million sets of iris records, with more added monthly.[89]

DNA Collection

Since 2020, CBP and ICE have begun to collect DNA samples from an ever-growing number of migrants, including children as young as 14 as well as asylum seekers, and sending them to CODIS, the FBI's coordinated national database, which holds DNA profiles from convicted

---

[82] Mason, Marcy, "Biometric Breakthrough: How CBP is Meeting its Mandate and Keeping America Safe," *Frontline*, U.S. Customs and Border Protection, accessed January 11, 2024, https://www.cbp.gov/frontline/cbp-biometric-testing.

[83] Iris ID, "Iris ID products implemented at US-Mexico border crossing," Press Release, January 19, 2016, https://www.irisid.com/iris-id-products-implemented-at-us-mexico-border-crossing/.

[84] Hawkins, *The Border Zone Next Door* [see note 3].

[85] Customs and Border Protection, "CBP to Meet Legal Requirement to Collect DNA Samples from Certain Populations of Individuals in Custody," Press Release, December 3, 2020, https://www.cbp.gov/newsroom/national-media-release/cbp-meet-legal-requirement-collect-dna-samples-certain-populations; Prokop, Danielle, "U.S. continues to take DNA samples from asylum seekers at Border," *Missouri Independent,* June 9, 2023, https://missouriindependent.com/2023/06/09/u-s-continues-to-take-dna-samples-from-asylum-seekers-at-the-border/; "Privacy & Trust: Which biometrics does CLEAR capture?" CLEAR, accessed January 11, 2024, https://www.clearme.com/support/which-biometrics-does-clear-capture; Zipper, David, "Important People Are Noticing How Terrible CLEAR Is for Airports," *Slate*, December 5, 2023, https://slate.com/business/2023/12/clear-lines-airports-tsa-congress.html.

[86] Hunter, Tatum, "Clear vs. TSA PreCheck: What's better for price and privacy?" *Washington Post,* July 20, 2023, updated July 27, 2023, https://www.washingtonpost.com/technology/2023/07/20/clear-tsa-precheck-cost-privacy-airport-security/.

[87] "Iris recognition on the border: Interview with Jason Thompson Assistant Chief with the United States Border Patrol," *Iris ID Radio*, audio interview, January 24, 2022, 7:54, https://www.irisid.com/iris-recognition-at-the-border/.

[88] Meyerhoff, Tim, "Iris Recognition Delivers a Positive ID for Law Enforcement," Iris ID, February 2, 2023, https://www.irisid.com/iris-recognition-delivers-a-positive-id-for-law-enforcement/.

[89] Meyerhoff, Tim, "Iris Recognition Delivers a Positive ID for Law Enforcement," [see note 88].

individuals, crime scenes, and missing persons.[90] According to FBI budget documents, this has led to a tenfold increase in the number of DNA profiles added to CODIS every year: Last April, the bureau's director estimated it would collect well over 1 million samples by the end of the year .[91] A GAO report found that CBP alone collected nearly 1 million DNA samples from detained or arrested individuals from fiscal years 2020-22.[92]

With the expansion in collecting DNA through DHS law enforcement components, CODIS now holds DNA information of approximately 21 million people.[93] In 2020, ICE also piloted a program out of an Enforcement and Removal Operations facility to send DNA samples to CODIS.[94] Before the expansion of DNA collection to other components within DHS, Homeland Security Investigations was already engaged in the practice of collecting and sending DNA samples to CODIS, including those of U.S. persons arrested under their criminal authority.[95]

Recommendations

The unbridled law enforcement power of DHS — particularly of CBP and ICE — demands that the agency employ safeguards to protect against rights abuses. DHS uses a number of federal, state, local, and private biometric collection platforms in the area of facial recognition, and these platforms collectively hold billions of images.[96] GAO reports highlight a lack of training and transparency in the deployment and use of this technology, as well as a lack of privacy policies and controls.[97] Absent significant guardrails regarding the use of powerful and rapidly evolving biometric collection technologies, the law enforcement power of DHS will only expand, becoming an even greater threat to the rights of all.

As you examine the extensive collection and use of biometric data by law enforcement, we recommend that you consider the following principles and adopt policy recommendations consistent with them:

- Biometric data collection must be viewed as a technology that fundamentally alters police power, and it should not be brought into use without public debate;

---

[90] "Government Accountability Office, *DNA Collections: CBP is Collecting Samples from Individuals in Custody, but Needs Better Data for Program Oversight [Reissued with revisions on Jun. 5, 2023],* GAO-23-106252 (2023), 8, 10, https://www.gao.gov/assets/gao-23-106252.pdf; "Glossary: CODIS," Bureau of Justice Statistics, accessed January 11, 2024, https://bjs.ojp.gov/glossary/codis.

[91] Klippenstein, Ken, "FBI Hoovering Up DNA at a Pace That Rivals China, Holds 21 Million Samples and Counting," *The Intercept*, August 29, 2023, https://theintercept.com/2023/08/29/fbi-dna-collection-surveillance/.

[92] Government Accountability Office, *DNA Collections: CBP is Collecting Samples from Individuals in Custody, but Needs Better Data for Program Oversight [Reissued with revisions on Jun. 5, 2023],* GAO-23-106252 (2023), 8, https://www.gao.gov/assets/gao-23-106252.pdf.

[93] Hussain and Guariglia, "The U.S. Government's Database of Immigrant DNA Has Hit Scary, Astronomical Proportions" [see note 11].

[94] Department of Homeland Security, *Privacy Impact Assessment for CBP and ICE DNA Collection,* DHS/ALL/PIA-080, 8, https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs080-detaineedna-october2020.pdf.

[95] Department of Homeland Security, *Privacy Impact Assessment for CBP and ICE DNA Collection,* 8 [see note 94].

[96] Government Accountability Office, *Facial Recognition Technology:… Privacy and Other Risks*, 16 [see note 7].

[97] Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training,* 40-43 [see note 54].

- Biometric data collection must be treated as a forensic tool that requires careful use and precise application; and
- Biometric data collection must be checked by limits that will prevent improper applications and abuse.[98]

It is imperative that the forthcoming report address how the use of facial recognition and biometric collection data is shared between both law enforcement and quasi-law enforcement agencies, how surveillance utilizing these tools impacts civil rights and privacy, and how strong accountability structures, coupled with routine assessment and strong policies narrowing the scope of deployment, will ensure that the use of these technologies does not reinforce discriminatory policing practices.

Guiding the interagency review and recommendations, the report should consider limitations to the deployment and use of biometric collection technologies and data. With respect to the deployment of facial recognition, we recommend the following key safeguards:

- Use of federal face recognition systems must be predicated on a probable cause finding that a person has or is committing the offense being investigated;
- Limit use of face recognition to the investigation of violent felonies;
- Prohibit use of face recognition for untargeted surveillance;
- Require disclosure of the use of facial recognition to defendants; and
- Prohibit law enforcement agencies from purchasing facial recognition technology from companies that fail to meet basic thresholds for protecting data and privacy rights.[99]

Given the sensitive nature of DNA collection and its potential for invasive government surveillance and creation of discriminatory practices, we recommend the following safeguards concerning collection of DNA:

- End the collection and retention of biometric data from immigration detainees who are not charged with a qualifying offense for DNA collection under federal law; and
- Create a process for promptly expunging DNA information.

These recommendations should also apply to state and local law enforcement that seek to use federal biometric data. Additionally, we recommend the following:

- The federal government should prohibit use of its biometric data collection systems by state or local law enforcement entities under pattern and practice investigations for biased policing and other unconstitutional practices; and
- The federal government should create an external and independent audit program on the collection of biometric data.

Executive Order 14074 provides a unique opportunity to review the policies and procedures that proport to protect civil liberties and privacy rights and examine how they match up against the increasing deployment of facial recognition and biometric collection technologies by law

[98] Laperruque, *Law Enforcement Use of Facial Recognition* [see note 6].
[99] Laperruque, Jake, "No, Clearview AI's creepy plan to spy on us is not 'free speech,'" Project on Government Oversight, February 14, 2020, https://www.pogo.org/analysis/no-clearview-ais-creepy-plan-to-spy-on-us-is-not-free-speech.

enforcement agencies within DOJ and DHS. It is essential to meeting the mandate of the executive order that any report include an analysis of the deployment and use of these technologies within the largest law enforcement components of DHS, including CBP and ICE, in alignment with the principles we outlined above.

POGO appreciates the opportunity to provide a comment on this important issue. We are ready to work with you to provide a civil society perspective on how best to achieve the goals of the executive order.

Sincerely,

Sarah Turberville
Director, The Constitution Project

Don Bell
Policy Counsel, The Constitution Project