



April 8, 2024

Commission Chair Rochelle Garza
U.S. Commission on Civil Rights
1331 Pennsylvania Ave., NW, Suite 1150
Washington, DC 20425

Subject: Request for Comment on the Civil Rights Implications of Facial Recognition Technology

Dear Chair Garza and Commissioners:

The Project On Government Oversight (POGO) submits the following comment to the U.S. Commission on Civil Rights as you seek to complete a forthcoming report on the civil rights implications of facial recognition technology (FRT).

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 the Commission is aware of a recent public comment submitted by POGO, which in part addressed the challenges related to FRT in the federal law enforcement context within the U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS). This comment, submitted to DOJ and DHS to ensure full implementation of 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," included recommendations on specific limitations that federal law enforcement should adopt to protect rights as it collects and uses biometric data.

Given the Commission's interest in analyzing "how FRT is developed, how it is being utilized by federal agencies, emerging civil rights concerns, and safeguards the federal government is implementing to mitigate potential civil rights issues," we believe the information and recommendations we shared with DOJ and DHS may also be useful to the Commission.¹

Biometric Data — Including FRT — and its Use by the Justice Department

As we noted in our earlier comment, POGO has engaged in extensive work monitoring the operations of the Justice Department, as well as DHS and its relevant components, advocating

¹ U.S. Commission on Civil Rights, "Public Briefing: Civil Rights Implications of the Federal Use of Facial Recognition Technology," Press Release, February 29, 2024, <https://www.usccr.gov/files/2024-03/usccr-frt-briefing-media-advisory.pdf>.

for reforms that would curtail law enforcement abuses caused by overly intrusive and unaccountable surveillance.² 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.³ 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.

Facial recognition presents several threats to privacy and other civil rights. The technology is prone to inaccuracy, which has led to false arrests.⁴ 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.⁵ Facial recognition's reliability is highly variable, dependent upon lighting, angles, and resolution, as well as the "confidence thresholds" set by law enforcement.⁶ It has been used by state and federal law enforcement to chill constitutionally protected activities, like protesting.⁷

Law enforcement often state that the technology is only used for "investigative leads," but this use can have several downstream negative consequences as well.⁸ 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 United States Court of Appeals for the Seventh Circuit found,

² "Protecting Civil and Human Rights," Project On Government Oversight, accessed January 10, 2024, <https://www.pogo.org/issue/protecting-civil-and-human-rights>.

³ 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>.

⁴ 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>.

⁵ 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>.

⁶ 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>.

⁷ 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/>.

⁸ *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>.

fundamentally “alter the relationship between citizen and government in a way that is inimical to democratic society” as its use becomes more pervasive.⁹

This year, we recommended to the DOJ that components within the department engaged in biometric data collection should be rigorously examined by the forthcoming review. 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.¹⁰ As POGO has written on the FBI’s system:

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.¹¹

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, such as U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE), the deployment and use of these technologies has permeated into fundamental law enforcement operations, including conducting facial recognition searches to create investigative leads for Homeland Security Investigations.¹² DHS law enforcement use these technologies within the interior of the country, particularly — but not only — on migrants.¹³

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

⁹ 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>.

¹⁰ 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>.

¹¹ 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>.

¹² 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>.

¹³ 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>.

criminal investigations.¹⁴ 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.

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.¹⁵ CBP uses facial recognition technology at many airports, seaports, and land ports of entry.¹⁶ 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.¹⁷ At airports, the technology is widely deployed, based in 238 locations.¹⁸ CBP estimates that it has processed a staggering 300 million travelers using biometric facial comparison technology.¹⁹ 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."²⁰ ICE is also increasingly relying on facial recognition to track migrants in its "alternative to detention" program.²¹

The Border Patrol routinely collects fingerprints, iris images, photographs, and facial scans of detained migrants and enters them into multiple government databases.²² Border Patrol agents also collect biometric information from individuals and search it against several government databases.²³ As of July 2023, 163 land border checkpoints used "Biometric Facial Comparison Technology" for pedestrian entry points.²⁴ It should be noted that two of these crossings

¹⁴ Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training*, 13-14 [see note 12].

¹⁵ 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>.

¹⁶ "Where is it Deployed?" Department of Homeland Security, last modified January 4, 2024, <https://www.cbp.gov/travel/biometrics>.

¹⁷ "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/>.

¹⁸ "Airports | CBP Biometrics," Department of Homeland Security, last modified November 29, 2023, <https://www.cbp.gov/travel/biometrics/airports>.

¹⁹ "Where is it Deployed?" Department of Homeland Security [see note 16].

²⁰ "CBP One: An Overview," American Immigration Council, December 9, 2021, <https://www.americanimmigrationcouncil.org/research/cbp-one-overview>.

²¹ 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>.

²² 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>.

²³ Government Accountability Office, *Border Patrol: Actions Needed to Improve Checkpoint Oversight and Data*, 13 [see note 22].

²⁴ "Land Crossings," Department of Homeland Security, last modified July 13, 2023, <https://www.cbp.gov/travel/biometrics/land-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.²⁵

CBP, ICE, and the Secret Service reported that they used federal, state, local, and privately owned facial recognition systems.²⁶ Within ICE, Homeland Security Investigations agents used these systems to generate investigative leads and support criminal investigations.²⁷ From October 2019 through March 2022, the entity conducted over 15,000 searches.²⁸ CBP also stated that it used face recognition searches to develop and share information in support of other agencies' criminal investigations.²⁹ 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.³⁰ 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."³¹ 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.³² 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.³³ 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.³⁴ 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.³⁵ 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.³⁶ In April 2020, the Secret Service halted the technology's use,

²⁵ "Land Crossings," Department of Homeland Security [see note 24].

²⁶ Government Accountability Office, *Facial Recognition Technology: ... Privacy and Other Risks*, 12 [see note 10]; Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training*, 47 [see note 12].

²⁷ Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training*, 13 [see note 12].

²⁸ Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training*, 15 [see note 12].

²⁹ Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training*, 14 [see note 12].

³⁰ Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training*, 15 [see note 12].

³¹ Government Accountability Office, *Facial Recognition Technology: ... Privacy and Other Risks*, 17-18 [see note 10].

³² Government Accountability Office, *Facial Recognition Technology: ... Privacy and Other Risks*, 18 [see note 10].

³³ Government Accountability Office, *Facial Recognition Technology: ... Privacy and Other Risks*, 19 [see note 10].

³⁴ 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 10].

³⁵ Guardian staff and agency, "Clearview AI agrees to restrict use of face database" [see note 34]; Laperruque, "Face Recognition Is Far from the Sci-Fi Super-Tool Its Sellers Claim" [see note 34].

³⁶ Laperruque, "Face Recognition Is Far from the Sci-Fi Super-Tool Its Sellers Claim" [see note 34].

after it was discovered that employees had been using free trials of Clearview AI to utilize facial recognition technology without authorization or training.³⁷

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.³⁸ 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.³⁹ 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.

Recommendations

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;
- 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.⁴⁰

It is imperative that any 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 committed 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;

³⁷ Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training*, 56 [see note 12].

³⁸ Government Accountability Office, *Facial Recognition Technology: ... Privacy and Other Risks*, 16 [see note 10].

³⁹ Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training*, 40-43 [see note 12].

⁴⁰ Laperruque, *Law Enforcement Use of Facial Recognition* [see note 8].

- 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.⁴¹

POGO appreciates the opportunity to provide a comment on the civil rights implications of using facial recognition technology. We are hopeful that your report is a meaningful step forward in addressing the proliferation of this technology within the federal government.

Thank you,

Don Bell
Policy Counsel, The Constitution Project

⁴¹ 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>.