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 U.S. COMMISSION ON CIVIL RIGHTS

Call for Public Comments: Civil Rights Implications of the Federal Use
of Facial Recognition Technology

April 8, 2024

---

The Electronic Privacy Information Center (EPIC) submit these comments to the U.S. Commission on Civil Rights to inform the Commission's report on the civil rights implications of the federal use of facial recognition technology. EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[1] EPIC has a particular interest in accountability, fairness, privacy, civil rights, and civil liberties in the context of surveillance and algorithm-powered technologies, particularly with the respect to the use of facial recognition technology.[2]

## I. Federal law enforcement should not use facial recognition technology

Facial recognition is a dangerous and privacy-invasive surveillance technology that law enforcement should not use. As a law enforcement investigative tool, facial recognition has not been proven to be reliable and the typical steps involved in law enforcement's use of facial recognition—from the selection of probe photos to the human review of the search results—can all contribute to its unreliability. Furthermore, facial recognition has been shown to be biased and will likely continue to be disproportionately focused on marginalized communities and will only exacerbate the historical inequalities in the criminal justice system. On a broader scale, the widespread use of facial recognition technology by federal law enforcement agencies will undermine democratic values and

[1] EPIC, *About Us* (2023), https://epic.org/about/.

[2] *See* EPIC Comments to DOJ and DHS on Section 13(e) of EO 14074 (Jan. 19, 2024), https://epic.org/wp-content/uploads/2024/01/EPIC-DOJDHS-Comment-LE-Tech-011924.pdf; *Assessing CBP's Use of Facial Recognition Technology: Hearing Before the Subcomm. on Border Security, Facilitation & Operations of the House Comm. on Homeland Security* 114th Cong. (2022) (statement of Jeramie D. Scott, Director of EPIC's Project on Surveillance Oversight), https://epic.org/wp-content/uploads/2022/07/Testimony-Scott-CBP-FRT-Use-2022.07.27.pdf; EPIC Comments to OSTP on Public and Private Sector Uses of Biometric Technologies (Jan. 15, 2022), https://epic.org/documents/epic-comments-to-ostp-on-public-and-private-sector-uses-of-biometric-technologies/; EPIC Comments to DHS: Advance Collection of Photos at the Border (Nov. 29, 2021), https://epic.org/documents/epic-comments-to-dhs-advance-collection-of-photos-at-the-border/; EPIC Comments to DHS on Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States (Dec. 21,2023), https://epic.org/documents/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states/.

Constitutional rights. It is a perfect tool of oppression and poses far too great a risk to our democracy to become a ubiquitous tool of police surveillance. This is true even with regulations in place but particularly true given the current lack of federal regulations to protect against the potentially worst outcomes.

### a. *Facial recognition is inaccurate and bias and has not been established as a reliable investigative tool*

Several studies have shown that many facial recognition algorithms have accuracy issues. Furthermore, these accuracy issues tend to be most prominent among people of color, creating a racial bias issue in the accuracy of facial recognition algorithms. A well-known study in 2019 conducted by National Institute of Standards and Technology (NIST) evaluated several facial recognition algorithms and found "empirical evidence for the existence of demographic differentials in the majority of contemporary face recognition algorithms."[3] NIST's 2019 study found that Black people were typically 100x more likely to be misidentified than white people, though results varied somewhat across algorithms.[4] The same study found that women were 2-5x more likely to be misidentified (a false positive) than men.[5]

The latest NIST reports use a variety of datasets to assess the accuracy of facial recognition algorithms, including both high quality images like passport photos, and lower quality images drawn from immigration lane cameras.[6] The NIST testing reveals a broad variance in accuracy of the facial recognition algorithms that are available to law enforcement—finding false negative rates ranging from 0.12 to 50 percent of searches against a mugshot database.[7] A 50 percent false negative error rate will return all wrong results in a disturbing half of its searches. While the best algorithms performed very well on controlled mugshot images, the same algorithms had error rates above 20 percent "for side-view images, poorer quality webcam images, and, particularly, for newly introduced ATM-style kiosk photos that were not originally intended for automated face recognition."[8]

NIST's testing reveals that even the best algorithms are only as good as the reference image. And even though more recent NIST tests contain a broader range of image variability, the NIST tests still do not regularly test algorithms against the types of photos that police are likely to encounter in investigations, such as surveillance cameras images where the subject is blurry, looking away, obscured in some way, or in poor light. While setting high thresholds for accuracy may prevent some misidentifications, the low-quality target images used by police continue to pose a substantial threat of wrongful identification, arrest, and in the worst cases, wrongful conviction—particularly for

[3] Patrick Grother, Mei Ngan, & Kayee Hanaoka, *Face Recognition Vender Test Part 3: Demographic Effects*, NIST (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [hereinafter "NIST FRT Demographic Effects Test"].

[4] *Id.*

[5] *Id.* at 7.

[6] Patrick Grother, Mei Ngan, & Kayee Hanaoka, *Face Recognition Technology Evaluation (FRTE) Part 2: Identification*, NIST 5 (Feb. 2022), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf [hereinafter "NIST FRT Identification Evaluation"].

[7] *Id.*

[8] *Id.*

people of color. It unfortunately should come as no surprise that, for the publicly reported cases, every single person wrongfully arrested due to the use of facial recognition has been Black.[9]

The lack of reliability in facial recognition technology does not only stem from the algorithms themselves, indeed, there is plenty of evidence that suggests law enforcement procedures compound the potential for misidentifications and biased outcomes. As one facial recognition expert has explained:

> No study has comprehensively examined the reliability of face recognition as actually used by a representative sample of U.S. law enforcement officers, taking into account the full range of possible variabilities generated by unconstrained probe photo qualities, probe photo manipulation, variably trained human analysis, and the contextual and other biases that may be present in many searches conducted in police departments across the country today.[10]

Despite the lack of comprehensive review of facial recognition as deployed by law enforcement, there is plenty of evidence that speaks to its unreliability. The unreliability of facial recognition as a law enforcement investigative tool does not merely stem from potential misidentifications by the facial recognition algorithm itself, but also stem from the various steps police typically take in the use of facial recognition for identification, including: 1) the selection of a probe photo, 2) the choice of database to use for the search, 3) the preprocessing of the probe photo, 4) the algorithm used for the search, and 5) the human review conducted of the results of the search.[11]

The probe photo is the photograph chosen of the unknown subject used to run the facial recognition search. The quality of the photo affects the accuracy of the search results.[12] The photos of an unknown subject police have to work with vary in quality. The angle of the photo, the lighting, and the sharpness of the photo, among other things, can all have an impact on the accuracy of the search results, so much so that oversight and scientific bodies have issued standards for photos and vendors have made minimum photo quality recommendations.[13]

The database a probe image is run against affects the reliability of the results. If a subject is not in the database against which a facial recognition search is run, all the results returned will necessarily be false positives. The quality of the images in the chosen database will affect reliability. Databases with older and/or lower quality images will increase the potential for errors. Additionally, the size of the database has an impact on reliability. Larger databases are more likely to contain people who look similar, which can lead to misidentification.[14]

[9] Katie Hawkinson, *In every reported case where police mistakenly arrested someone using facial recognition, that person has been Black*, Bus. Insider (Aug. 6, 2023), https://www.businessinsider.com/in-every-reported-false-arrests-based-on-facial-recognition-that-person-has-been-black-2023-8.

[10] Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Geo. L. Ctr. on Priv. & Tech. 16 (2022), https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf.

[11] *Id.* at 9.

[12] *Id.* at 9–10.

[13] *Id.* at 10.

[14] *Id.*

Preprocessing of a probe photo involves some type of editing of the photo itself, which can impact the reliability of the facial recognition search. Law enforcement have used software to edit probe photos in several different ways, including "using the blur tool to add pixels into a low-quality image; cutting and pasting new features into the subject photograph; combining photographs of two different people to generate a single image; and using 3D modeling to recreate an approximation of facial features not visible in the original image."[15] These changes to the probe photos may make it more likely that the facial recognition search returns results, but it also is likely to increase the unreliability of the returned results.

The algorithm used in a facial recognition search can also impact the reliability of the results. The accuracy of algorithms can vary widely and is impacted by, among other things, the data used to train the algorithm. For example, algorithms trained on images of predominately white males will likely be relatively accurate with facial recognition searches of white males but tend to be less accurate when performing a search of a person of color.[16] Additionally, older algorithms tend to be less accurate than newer algorithms.

The issues created by photo selection, choice of database, preprocessing of photos, and the algorithms used are not necessarily mitigated by the human review of the search results. On the contrary, the human review can create its own reliability issues due to variance in people's ability to identify unfamiliar faces, training issues, and various bias issues.

Facial recognition searches generally return a candidate list of possible matches with each candidate associated with a confidence score. A human is then responsible for sorting through the list of possible matches to identify the correct one. The general assumption is that with a human in the loop, they can mitigate the potential misidentifications. Of course, this assumes that humans are good at face comparisons.

Research shows that people are generally not great at identifying unfamiliar faces.[17] This is true even when dealing with high-quality photos, which is rarely the case with law enforcement probe photos. The unfamiliarity of the subject, low-quality images, the different angles of photos, the obfuscation of facial features, among other things, all contribute to the difficulty of identifying whether a probe photo and one of the photos from the candidate list are indeed a match.

### b. *Law enforcement's use of facial recognition is disproportionately directed at communities of color and exacerbates the historical racial inequalities in the criminal justice system*

There is plenty of evidence that police surveillance is disproportionately directed at communities of color, particularly Black communities. There are no shortage of examples through history including the lantern laws during colonial times, the FBI's COINTELPRO program, the war on drugs, and the surveillance of Black Lives Matter activist just to name a few—police surveillance

[15] *Id*. at 11.

[16] NIST FRT Demographic Effects Test, *supra* note 40, at 2.

[17] Garvie, *supra* note 10, at 22.

has a long history of targeting Black people.[18] The targeting of Black people for police surveillance has contributed to the historic inequalities in the criminal justice system. Unfortunately, this trend of disproportionately directing surveillance technologies towards communities of color has already started with facial recognition and will only increase if federal law enforcement continues to expand its use.

Despite the research showing that facial recognition algorithms often have the highest error rate on people of color, the technology is most often directed towards communities of color. In New Orleans, the city council voted to lift a ban on police's use of facial recognition after a violent crime rose in the city.[19] The technology was touted as "effective, fair tool for identifying criminals quickly."[20] Roughly a year after New Orleans police began using facial recognition again, the reality was the technology "had low effectiveness, was rarely associated with arrests and was disproportionately used on Black people."[21]

In Detroit, the Project Green Light surveillance program has connected high definition cameras at over 700 locations that send a live feed to Detroit Police's real time crime center (RTCC).[22] These live video feeds can be used to pull images for facial recognition searches against a database that contains "mug shots, sex offender registry photographs, driver's license photos and state ID photos[.]"[23] Almost every Michigan resident is in the database, but the Project Green Light cameras are concentrated in majority-Black areas.[24] A 2019 critical analysis of Project Green Light reported that "surveillance and data collection was deeply connected to diversion of public benefits, insecure housing, loss of employment opportunities, and the policing and subsequent criminalization of the community members that come into contact with these surveillance systems."[25] Despite claims that Project Green Light reduces crime, there is little evidence so far that it actually does.[26]

[18] *See generally* Simone Browne, *Dark Matters: On the Surveillance of Blackness* (2015).

[19] Alfred Ng, *'Wholly ineffective and pretty obviously racist': Inside New Orleans' struggle with facial-recognition policing*, Politico (Oct. 31, 2023), https://www.politico.com/news/2023/10/31/new-orleans-police-facial-recognition-00121427.

[20] *Id.*

[21] *Id.*

[22] City of Detroit, Crime Intel. Unit, *Project Green Light Detroit Presentation* (Aug. 6, 2020), https://detroitmi.gov/sites/detroitmi.localhost/files/2020-08/Facial%20Recog%20and%20Project%20Green%20Light%20%281%29.pdf.

[23] Detroit Cmty. Tech. Proj., *A Critical Summary of Detroit's Project Green Light and its Greater Context* 5 (June 9, 2019), https://detroitcommunitytech.org/system/tdf/librarypdfs/DCTP_PGL_Report.pdf?file=1&type=node&id=77&force=.

[24] Alex Najibi, *Racial Discrimination in Face Recognition Technology*, Harv. GSAS Sci. Pol'y Grp. Blog (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

[25] Detroit Cmty. Tech. Proj., *supra* note 66, at 5.

[26] Laura Herberg, *Tracked and Traced: Does Project Green Light in Detroit Reduce Crime?*, WDET.org (Feb. 3, 2022), https://wdet.org/2022/02/03/tracked-and-traced-does-project-green-light-in-detroit-reduce-crime/.

There is no shortage of evidence that demonstrates the racial bias in the criminal justice system.[27] Many if not all aspects of the criminal justice system produce racially disparate outcomes. It is instructive to consider traffic stops where there are plenty studies that overwhelmingly show evidence of racial bias in who gets stopped and who gets searched. A 2020 study analyzing nearly 100 million traffic stops from all over the country found racial bias in stop decisions and a lower bar for searching Black and Hispanic drivers compared to their white counterparts.[28] A 2013 Justice Department study found that Black drivers were more likely to get pulled over and more likely to be searched than white drivers.[29]

These broad studies are further supported by numerous analyses of traffic stops in states and cities across the United States. A 2023 statewide analysis of traffic stops in Connecticut found that Black motorists were more likely to be searched yet less likely to be found with contraband from those searches.[30] A study of stops by police in Springfield, Missouri found "substantial disparities in the rate at which African-Americans were stopped, and that the disparities increased, from 2012 to 2016 in Springfield."[31] A study of traffic stops in Kansas City found that Blacks were 2.7 times more likely to be pulled over for an investigatory traffic stop and five times more likely to be searched.[32] Black drivers in Vermont were found to be four times more likely to be searched than a white driver.[33] Similarly, a study of hundreds of thousands of traffic stops in San Diego found that police were more likely to search Black and Latino drivers compared to white drivers—despite the fact that white drivers were more likely to be found with contraband.[34]

The racial inequalities in policing and the criminal justice system are well documented and there is no reason to believe that facial recognition technology will not be applied in a racially bias manner, indeed, as shown in the previous section, facial recognition is already directed in a racially bias manner. Furthermore, a study that analyzed facial recognition deployment by police and arrests

[27] Radley Balko, *There's Overwhelming Evidence That the Criminal Justice System Is Racist. Here's the Proof*, Wash. Post (June 10, 2020), https://www.washingtonpost.com/graphics/2020/opinions/systemic-racism-police-evidence-criminal-justice-system/.

[28] Emma Pierson et al., *A Large-scale Analysis of Racial Disparities in Police Stops Across the United States*, 4 Nature Hum. Behav. 736, 736 (2020), https://www.nature.com/articles/s41562-020-0858-1.pdf.

[29] Lynn Langton & Matthew Durose, *Police Behavior During Traffic and Street Stops*, DOJ (Sept. 2013), https://bjs.ojp.gov/content/pub/pdf/pbtss11.pdf (revised Oct. 27, 2016).

[30] Ken Barone et al., *Connecticut Racial Profiling Prohibition Project, Traffic Stop Data Analysis and Findings 2021*, Univ. Conn. Inst. for Mun. & Reg'l Pol'y 45–58 (Oct. 2023), https://assets-global.website-files.com/6076e3f57e39855392637f16/6525a6b30968fb82c5a80237_2021%20CTRP3%20Traffic%20Stop%20Analysis%20and%20Findings%20Report.pdf.

[31] Mike Stout, *Racial and Ethnic Disparities in Traffic Stops and Stop Outcomes in Springfield, Missouri: 2012-2016* 2 (Aug. 8, 2017), https://www.springfieldmo.gov/DocumentCenter/View/45970/Racial-and-Ethnic-Disparity-in-Traffic-Stops-Report-2012-2016-.

[32] Lisa Rodriguez, *Study of KC Metro Traffic Stops Shows Race Deeply Embedded In Police Practice*, NPR (Mar. 12, 2015) https://www.kcur.org/show/up-to-date/2015-03-12/study-of-kc-metro-traffic-stops-shows-race-deeply-embedded-in-police-practice#stream/0.

[33] Stephanie Seguino & Nancy Brooks, *A Deeper Dive into Racial Disparities in Policing in Vermont* 28 (Mar. 26, 2018), http://mediad.publicbroadcasting.net/p/vpr/files/201803/a_deeper_dive_into_racial_disparities_in_policing_in_vermont_3.26_final.pdf.

[34] Joshua Chanin et al., *Traffic Enforcement in San Diego, California: An Analysis of SDPD Vehicle Stops in 2014 and 2015* ii (Nov. 2016), https://www.sandiego.gov/sites/default/files/sdpdvehiclestopsfinal.pdf.

in over a 1,000 U.S. cities found that it "contributes to greater racial disparity in arrests."[35] It's clear that the continued use and adoption of facial recognition technology by law enforcement will magnify the historic inequalities of the criminal justice system.

### *c. Facial recognition is a dangerous tool of oppression and poses too great a risk to our democracy that is amplified by the lack of strict federal regulation*

The dangers of facial recognition do not begin and end with racial bias. Even if facial recognition was perfectly accurate for and equally applied to all types of people, the dangers of facial recognition would not disappear. In some sense, the danger would be even greater. Facial recognition is a powerful surveillance tool that can destroy any sense of privacy we may have as we go about our daily lives. The technology itself enables comprehensive surveillance which poses a threat to privacy and civil liberties. Face surveillance can be used for real-time tracking and for identification of individuals in crowds. These abilities are nearly unique to facial recognition. Comprehensive real time surveillance will substantially chill freedom of speech and protest as individuals rightfully fear identification and retaliation for engaging in lawful protests. Facial recognition has already been used numerous times by law enforcement agencies to conduct surveillance on people engaged in First Amendment-protected activities.[36] Simply put, facial recognition technology places too much power in the hands of the police.

These dangers are heightened by the fact that the U.S. lacks strict regulation of the use of facial recognition technology. Strict regulation would not eliminate the dangers of facial recognition, but regulation would at least decrease it. Currently, federal law enforcement can generally implement facial recognition with little to no oversight and take advantage of the vast number of images of people that are available online through social media and other websites, in government databases like DMV or Passport photo databases, or that are caught on the millions of CCTV cameras across the country. The ease of implementation of facial recognition makes the technology too tempting to resist and all the more dangerous. The dangers and risk of facial recognition technology to individuals and our democracy are far too great to allow its use by law enforcement.

## II. The use of facial recognition for identity verification poses serious risks

Although the use of facial recognition technology for identity verification may not seem as dangerous as using the technology for law enforcement purposes, face verification creates serious risks for our society. There are of course the potential bias issues that could disproportionately affect people of color and women—leaving them to bear the burden of the negative impact of the

[35] Thaddeus L. Johnson et al., *Facial Recognition Systems in Policing and Racial Disparities in Arrests* 1, 9 (Oct. 2022), https://www.sciencedirect.com/science/article/abs/pii/S0740624X22000892.

[36] *See, e.g.*, U.S. Gov't Accountability Office, GAO-21-518, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks 17 (June 3, 2021), https://www.gao.gov/assets/gao-21-518.pdf (finding that at least six agencies used facial recognition to surveil Black Lives Matter protestors); Benjamin Powers, *Eyes Over Baltimore: How Police Use Military Technology to Secretly Track You*, Rolling Stone (Jan. 6, 2017), https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885/ (reporting that the Baltimore Police Department used facial recognition and social media surveillance to surveil protestors following the death of Freddie Gray).

technologies use. But the issues go beyond potential bias and cannot be corrected by improving the accuracy of the algorithm.

The use of facial recognition for identity verification has long term implications when our face becomes our ID. The federal government's use of face verification acts as an endorsement of the technology regardless of whether the government means it too. Consequently, the government's use of face verification will accelerate the use of our faces as our IDs. No longer will we control our identification as that control will be ceded to the government or possibly a third party, which will have the ability to easily identify us without our consent and even without our knowledge. And using our faces as our ID means the infrastructure for facial recognition will become ubiquitous and centralized and the temptation to expand the use of such an infrastructure will likely be too great to resist, resulting in mission creep. The outcome is a national ID based on our faces and controlled by the government, which will be disastrous for our privacy, civil liberties, and civil rights. It would destroy anonymity and put the control of identification in the hands of the government and further exacerbate the imbalance of power between the government and the people.

Face verification not only builds out the infrastructure for face surveillance but normalizes the use of facial recognition by the government on the govern. Consequently, there will be an enormous amount of temptation, if not pressure, to expand the use of the infrastructure for surveillance. This is particularly true given the lack of federal regulation on the facial recognition technology to provide tight restrictions on its use. At present, we only have agency promises and policies to rely on and that is certainly not good enough to ensure that mission creep does not occur down the line, especially knowing that leadership of these agencies changes on a regular basis.

## III. Agency promises and policies and even federal regulation are not enough to mitigate the risks of facial recognition technology

The lack of strong federal regulation of facial recognition should be the death knell of the federal government's current use of the technology. Facial recognition is too dangerous of a surveillance technology to leave the way it is used up to agency policies. Take TSA's use of face verification at airport security checkpoints. The TSA likes to emphasize how travelers can opt-out of face verification but that is just TSA's currently policy, indeed, the head of TSA, David Pekoske, stated at SXSW this year while talking about the use of facial recognition at airports that "eventually we will get to the point we will require biometrics across the board."[37]

The government has already leveraged its data to expand the use of facial recognition. For example, the CBP currently uses photos from the State Department's passport photo database for CBP's Biometric Entry/Exit program—and there are numerous other agencies that have access to passport photos for facial recognition.[38] When people applied to get a passport, particularly people who did this before Biometric Entry/Exit existed, they did so to get a physical passport. They did not sign up the government to leverage the photos applicants are required to provide for a passport for a

[37] Wilfred Chan, Exclusive: TSA to expand its facial recognition program to over 400 airports, Fast Company (June 6, 2023), https://www.fastcompany.com/90918235/tsa-facial-recognition-program-privacy.

[38] *See* Letter from Sen. Wyden to Secretary of State Blinken (Nov. 3, 2022), https://www.wyden.senate.gov/imo/media/doc/Wyden%20letter%20to%20State%20Department%20on%20protecting%20Americans%20Passport%20Data%2011.3.22.pdf.

government face verification program. It is important to note that Congress never gave CBP authority to use facial recognition on US Persons. The authority granted was for non-US Persons. But as is often the case, ease of implementation—not privacy, civil liberties, or civil rights, was the overwhelming impetus behind how the program was implemented despite the lack of Congressional authority.

Federal regulation is not necessarily the answer that mitigates the risk of facial recognition. Unfortunately, federal agencies like DHS and DOJ have a history of not abiding by legal requirements. This is particularly true when it comes to oversight of the use of surveillance technology. Under the E-government Act of 2002, agencies are required to conduct privacy impact assessment (PIA) when personally identifiable information (PII) will be collected or used.[39] PIAs play an important role in government accountability and determining the privacy risks of systems that use PII. A properly conducted PIA enables an agency to identify privacy risks, determine if and how those risks can be mitigated, and make an informed decision whether the proposed collection or system can be justified in light of its privacy impact. Additionally, a PIA informs the public of data collection or an information system that poses a threat to privacy. PIAs not only help to protect privacy but in doing so inherently help to protect civil rights and civil liberties.

Over the past decade, EPIC has identified numerous instances in which the DHS, FBI, DEA, United States Postal Service, and other agencies have failed to complete required PIAs under the E-Government Act for activities implicating personal data.[40] PIAs, a requirement under the law, have become an optional box checking exercise that largely no longer serves its intended purpose. Facial recognition has already been treated this way as evidence by documents obtained by EPIC through the Freedom of Information Act showing that DHS Privacy was unaware that ICE was using Clearview AI.[41] A PIA to cover the use of Clearview AI was only conducted after media scrutiny of Clearview AI. Facial recognition is too dangerous to hope agencies abide by their policies or follow federal regulation. The safest thing to do is to ban federal law enforcement agencies from using facial recognition technology.

## IV. Conclusion

Facial recognition technology is a growing threat to our privacy, our civil liberties, our civil rights, and to our democratic values. We urge the Commission to consider in its report the risks of facial recognition to society if the technology is allowed to expand as a tool of law enforcement and as a means of identity verification.

Respectfully submitted,

Jeramie D. Scott
Director, EPIC Project on Surveillance Oversight
Senior Counsel

[39] *See* Comments of EPIC to OMB on Privacy Impact Assessments (Apr. 1, 2024), https://epic.org/wp-content/uploads/2024/04/EPIC-Comment-to-OMB-re-PIAs-April-2024-with-Appendix.pdf.
[40] *Id.*
[41] Jeramie D. Scott, *Is ICE Using Facial Recognition to Track People Who Allegedly Threaten Their Agents*, EPIC Blog (Mar. 17, 2022), https://epic.org/is-ice-using-facial-recognition-to-track-people-who-allegedly-threaten-their-agents/.