CENTER FOR DEMOCRACY & TECHNOLOGY

Transparency and Policy Recommendations for Federal Law Enforcement Use of Facial Recognition

Friday, January 19, 2024

The Center for Democracy & Technology (CDT) welcomes the opportunity to provide input to the Departments of Justice and Homeland Security pursuant to their October 13 request for written submissions. CDT is a leading nonpartisan, nonprofit organization fighting to advance civil rights and civil liberties in the digital age. We shape technology policy, governance, and design with a focus on equity and democratic values. Established in 1994, CDT has been a trusted advocate for digital rights since the earliest days of the internet.

While guidance was also sought regarding use of other biometric technologies, this comment focuses on law enforcement use of facial recognition technology. Facial recognition is a powerful surveillance technology, and absent strong rules and safeguards it can significantly harm individuals. This risk is acute because facial recognition is a double-edged sword: It is dangerous when it works poorly, and can be dangerous in an entirely different way when it works well. There are numerous documented cases of facial recognition causing Americans to be improperly arrested and jailed,[1] as well as several recorded instances of facial recognition being abused to identify and catalog individuals engaged in First Amendment-protected activities.[2] Because of the range of risks it presents, law enforcement use of facial recognition requires a comprehensive set of policies and limits.

States and cities have begun to respond, with over a dozen enacting meaningful limits, and some jurisdictions banning the technology entirely.[3] Unfortunately, the federal government has fallen behind. Neither Congress nor federal agencies have enacted regulations or policies that are critical to protect civil rights and civil liberties. Below, we describe a set of recommended best practices divided into five categories: procurement, transparency, deployment, redress, and accountability. We urge the Department of Justice (DOJ) and Department of Homeland Security (DHS) to promptly adopt these policies.

---

[1] See, Khari Johnson, "How Wrongful Arrests Based on AI Derailed 3 Men's Lives", *Wired*, Mar. 7, 2022, https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/; see also, Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match", *The New York Times*, Dec. 29, 2020, https://perma.cc/CHM4-QAZ3; see also, Kashmir Hill and Ryan Mac, "'Thousands of Dollars for Something I Didn't Do,'" *New York Times*, Mar. 31, 2023, https://perma.cc/CNK3-926N.

[2] See, Joanne Cavanaugh Simpson and Marc Freeman, "South Florida police quietly ran facial recognition scans to identify peaceful protestors. Is that legal?", *Sun Sentinel*, June 26, 2021, https://perma.cc/V6PT-S2JB; see also, Kevin Rector and Alison Knezevich, "Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest," *Baltimore Sun*, Oct. 11, 2016, https://perma.cc/3AC8-6J9X.

[3] Jake Laperruque, "Limiting Face Recognition Surveillance: Progress and Paths Forward", Center for Democracy & Technology, Aug. 23, 2022, https://perma.cc/R473-PJMY.

CENTER FOR DEMOCRACY & TECHNOLOGY

I. Definitions and Use of Terms

Because examination of facial recognition involves use of various terms that often are given different meanings, at the outset we would like to clarify how certain terms will be used throughout this comment:

Facial Recognition, Face Identification, and Face Matching: We use the term "facial recognition" to mean using computers to engage in an automated process of scanning facial features to *identify* a previously unidentified person. This process is sometimes referred to as "face identification" or a "one-to-many" matching process, because it compares a single, unidentified face to numerous possible matches. We treat facial recognition as distinct from using computers to engage in an automated process of scanning facial features to *confirm* a person's identity, a process sometimes referred to as "face matching" or a "one-to-one" matching process (e.g., to confirm that a person's face matches a picture on an identification document). We draw this distinction because face identification presents far more serious civil rights and civil liberties risks than face matching, and because face matching tends to be less prone to error.

Limiting our discussion of facial recognition to an identification process is an important limitation on the scope of our recommendations. Our recommendations do not apply to the use of face matching to confirm identity when logging in to a device or service, such as for unlocking phones. Similarly, our recommendations do not implicate a range of potential law enforcement uses of face matching. For example, a recommended policy that prevents law enforcement personnel from running a *facial recognition* scan during a car stop would not prevent personnel from conducting a *face match* scan between the driver's face and their photo ID to confirm its authenticity.[4]

Targeted and Untargeted Facial Recognition: We refer to "targeted facial recognition" as the practice of selecting a particular person in a photo or video feed, and running a facial recognition scan on that discrete individual's face. Targeted scans are the most common law enforcement use of facial recognition; they encompass applications ranging from cross-checking an individual's identity during booking to attempting to discern the identity of a suspect from a crime scene video.

In contrast, we refer to "untargeted facial recognition" as the practice of using a facial recognition system to scan *groups* of individuals in a video feed, and either to catalog identities en masse or flag

[4] Other examples include verification of identity as a check in tool or for application of benefits by migrants, and airport security. Transportation Security Administration practices are generally built around face matching, and the Customs and Border Protection Biometric Entry-Exit program could be formatted as a face match system as well. These applications do raise legitimate concerns regarding civil rights, civil liberties, and accuracy, and should be subject to rigorous review and sensible guidelines for deployment. However, they are meaningfully distinct from face identification and should be evaluated in a separate manner.

whenever a person in the crowd matches against a watchlist of pre-identified and flagged faces. This process is sometimes referred to as "real-time" facial recognition because it is often performed on live video feeds. We do not use this label, however, because untargeted facial recognition scans could occur on tape delay, or even several hours or days after a video is recorded, and still create near identical risks. Untargeted facial recognition is frequently used in China as part of its government's pervasive surveillance network,[5] and has been deployed in pilot programs in United Kingdom cities.[6] As discussed below, similar use in the United States should be prohibited.

II. Procurement

Law enforcement agencies should only procure facial recognition systems that will ensure accuracy to the highest degree possible, protect civil rights and equity, and conform to ethical standards. We recommend three policies that will support these goals:

1) Require independent testing and high accuracy standards (both in terms of overall accuracy and avoiding demographic variance);
2) Prohibit any purchase of untargeted facial recognition; and
3) Prohibit any purchase of facial recognition systems built from photos that were acquired illegally, fraudulently, or in violation of terms of service.

Low accuracy and propensity for misidentifications has been a persistent problem for facial recognition systems. To address this, law enforcement agencies should not procure facial recognition systems unless they have been subject to testing by independent experts such as the National Institute of Standards and Technology, and consistently attained high overall accuracy levels in such tests. To provide transparency and enable oversight, law enforcement agencies should publicly report procurement information including vendors they use, the systems they employ, the dates and duration of contracts for such use, and the cost of each purchase or license.

For testing to be useful, it should be conducted under conditions as similar as is practicable to the conditions in which law enforcement will deploy facial recognition systems. Notably, relevant testing should focus on one-to-many matching, and should examine the accuracy of systems using photos taken "in the wild," meaning in real-world settings with variable conditions for lighting, angle, photo resolutions, and other factors that impact clarity of photos, similar to the crime scene photos police often use for scans.[7] Additionally, law enforcement agencies should test a system at all confidence

[5] Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *New York Times*, July 8, 2018, https://perma.cc/27U7-S365.
[6] Big Brother Watch, Face Off: The Lawless Growth of Facial Recognition in UK Policing (May 2018), https://perma.cc/PHW5-T57Z.
[7] See, Jake Laperruque, "POGO Proposes Strong Limits on Face Recognition to White House Office of Science and Technology Policy," Project On Government Oversight, January 18, 2022, https://perma.cc/578G-ZVYY ("Bad lighting, indirect angles, distance, poor camera

thresholds — meaning the required level of certainty to list an individual as a possible match — at which they plan to use it.

In addition to overall accuracy, it is important to address demographic variance. Many facial recognition systems have shown major variance in accuracy across categories such as race and gender.[8] This has caused real-world harms, and there is growing evidence that Black persons are being improperly arrested and jailed due to facial recognition errors more often than their white peers.[9] Even when these mistakes are corrected, they leave a lasting impact of serious harms, including loss of employment, enormous legal bills, and mental health issues.[10] It is unacceptable for police to rely on systems that will cause disparate and inequitable treatment, especially for matters as important as designation of suspects, arrests, and criminal charges. Law enforcement agencies should not procure or use facial recognition systems unless independent testing confirms such systems display no demographic variance in accuracy in all relevant circumstances of use.

Untargeted facial recognition has proven to be especially fraught in terms of accuracy. In several pilot programs conducted in cities in the United Kingdom, untargeted facial recognition systems produced false positive rates of 81 to 96 percent.[11] This means that, in as many as 19 of 20 cases, when a system flagged an individual in a crowd as matching an individual on a watch list, it did so erroneously. This degree of inaccuracy is unacceptable, especially given the risks that can naturally accompany law enforcement encounters. Law enforcement agencies should not procure untargeted facial recognition systems so long as pilots and testing result in such high levels of error.[12]

Beyond restrictions centered on accuracy, law enforcement should not procure facial recognition systems built on unethical practices. Specifically, law enforcement should not procure facial recognition

---

quality, and low image resolution all make misidentifications more likely. These poor image conditions are more common when photos and videos are taken in public, such as with a CCTV camera. But these low-quality images often serve as probe images for face recognition scans, without proper consideration for their diminished utility").

[8] Joy Buolamwini and Timnit Gebru (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Fairness, Accountability and Transparency, Proceedings of Machine Learning Research 81:77-91. https://perma.cc/7CPA-Y6NZ; Patrick Grother, Mei Ngan, and Kayee Hanaoka (Dec. 2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, National Institute Of Science and Technology. https://perma.cc/A86F-NVT9.

[9] See, fn 1; see also, Christina Swarns, "When Artificial Intelligence Gets It Wrong," The Innocence Project, September 19, 2023. https://perma.cc/5DH4-L4EX ("To date, six people that we know of have reported being falsely accused of a crime following a facial recognition match — all six were Black").

[10] See, fn 1.

[11] Lizzie Dearden, "Facial recognition wrongly identifies public as potential criminals 96% of time, figures reveal", *The Independent*, May 7, 2019, https://perma.cc/YZ36-RC6A; Rachel England, "UK police's facial recognition system has an 81 percent error rate", *Engadget*, July 4, 2019, https://perma.cc/88ER-PREX.

[12] While high rates of error are a sufficient reason to avoid any use of untargeted facial recognition, CDT also believes this form of face recognition constitutes unacceptable dragnet surveillance that should not be deployed, even if accuracy improves in the future. See, Artificial Intelligence and Human Rights: Hearing before the U.S. Senate Committee on the Judiciary Subcommittee on Human Rights and the Law, 118th Cong. (June 13, 2023) (statement by Alexandra Reeve Givens President & CEO, Center for Democracy & Technology), https://perma.cc/Q6BK-X39P.

systems built from photos that were acquired illegally, fraudulently, or in violation of terms of service. Such purchases encourage, finance, and enable such conduct.

The Department of Justice has not just treated scraping in violation of websites' terms of service as unethical; it has gone so far as to prosecute such activity as an act of malicious hacking in violation of the Computer Fraud and Abuse Act.[13] It would be hypocritical to treat such an action as criminal in some cases and in others pay vendors to engage in that very same practice. Yet that is precisely what the government does when it uses facial recognition systems such as Clearview AI, which build their photo databases by scraping billions of user photos from social media websites,[14] in violation of terms of service and explicit demands of those social media services.[15] Law enforcement should not procure facial recognition systems derived from such a dubious practice.

III. Transparency

Despite the range of dangers it poses, law enforcement use of facial recognition is often shrouded in secrecy. Transparency is critical to protect civil rights and civil liberties, enable oversight, incentivize responsible use, and guard against abuse. We recommend that federal law enforcement publicly report the following information:

1) The full set of crimes for which facial recognition is used to investigate and respond, and how often it is used in relation to each crime;
2) The number of instances where facial recognition is used to identify individuals who are not criminal suspects, and circumstances of such use;
3) The number of instances where facial recognition is used to identify individuals who are engaging in First Amendment-protected activities — including when used to identify those allegedly engaged in criminal conduct during a protest — and circumstances of such use; and
4) How often — both in general and in comparison to overall use — use of facial recognition is disclosed to defendants.[16]

[13] CDT has for over a decade maintained that mere violation of terms of service is not sufficient to constitute a Computer Fraud and Abuse Act violation. But, while not criminal, violating terms of service to pull biometric data on a mass scale raises serious ethical concerns. And it is undeniably at odds with how DOJ has for years treated scraping in violation of terms of service.

[14] Clearview AI is used by numerous federal law enforcement entities, including hundreds of personnel within DOJ and DHS. See, Government Accountability Office, "Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties," September 2023, https://perma.cc/WSX8-74AD. Hereinafter, *2023 GAO Report on Facial Recognition*.

[15] Alfred Ng and Steven Musil, "Clearview AI hit with cease-and-desist from Google, Facebook over facial recognition collection," *CNet*, February 5, 2020, https://perma.cc/Y76G-HSWA.

[16] This will require publishing not only the number of instances in which use of facial recognition is disclosed to defendants, but also how often facial recognition is used overall, and how often facial recognition is used in investigations that lead to criminal charges. being filed. The FBI previously published the number of facial recognition scans it conducted on a monthly and annual basis as part of its "Next Generation Identification (NGI) System Fact Sheet," but ceased doing so several years ago. Federal law enforcement agencies have never publicly reported on how facial recognition is used in investigations that lead to charges.

5) How often and in what manner facial recognition is used for immigration enforcement purposes, particularly for identification, detainment, and deportation of undocumented individuals.

In order to evaluate the efficacy of facial recognition and weigh value against risks, it is necessary to understand how the technology is used. In particular, it is important to know the full set of crimes facial recognition is used to investigate and respond to.[17] All law enforcement agencies that use facial recognition should track and publicly report this, as well as the frequency with which it is used in relation to each crime.

It is vital that the public is informed of the circumstances in which law enforcement uses facial recognition, and in particular if there are instances where facial recognition is used to identify individuals who are not criminal suspects. Current Immigration and Customs Enforcement (ICE) policies permit use of face recognition "in furtherance of ongoing investigations,"[18] allowing broad use of facial recognition to identify individuals beyond just criminal suspects and individuals believed to have violated immigration law, while general DHS policy permits use of facial recognition that is "for use for DHS missions, in accordance with DHS' lawful authorities, applicable statutes, regulations, and DHS policies."[19] Federal Bureau of Investigation (FBI) policies are even more permissive, permitting facial recognition in general support of investigations or assessments.[20] This means that not only are FBI personnel allowed to conduct facial recognition scans of individuals who are not designated criminal suspects, they can conduct scans as part of assessments when there is not even a factual predicate for criminal wrongdoing.[21] Using facial recognition in this manner creates serious risk of fishing investigations, disparate treatment, and outright abuse. To guard against this, law enforcement agencies should publicly report on how often they use facial recognition to identify individuals other than suspects, and if so, under what circumstances.

[17] Despite Congressional inquiry requesting the full set of crimes the FBI uses facial recognition to investigate over three years ago, this information remains unknown. See, Oversight of the Federal Bureau of Investigations: Hearing before the House Committee on the Judiciary, 117th Cong. (February 5, 2019).
[18] Department of Homeland Security, U.S. Immigration and Customs Enforcement, "Privacy Impact Assessment for the ICE Use of Facial Recognition Services," (May 13, 2020), https://perma.cc/JXS4-3EM6, hereinafter, *ICE Facial Recognition Privacy Impact Assessment*.
[19] Department of Homeland Security, "Use of Face Recognition and Face Capture Technologies," (Sept. 11, 2023), https://perma.cc/BTG6-BTQN, hereinafter, *DHS Facial Recognition Policy Directive*.
[20] See, Facial Recognition Technology (Part II): Ensuring Transparency in Government Use: Hearing before the House Committee on Oversight, 116th Cong. (June 4, 2019) (statement by Kimberly Del Greco, Deputy Assistant Director, FBI Criminal Justice Information Services Division), https://perma.cc/7NEW-RRW9, hereinafter, *Deputy Assistant Director Kimberly Del Greco Statement*; see also, *FBI Facial Recognition Privacy Impact Assessment*; see also, Erin M. Priest, Privacy and Civil Liberties Officer, FBI, "Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Phase II System," (2019). https://perma.cc/FR82-SFPB, hereinafter, *FBI Facial Recognition Privacy Impact Assessment*.
[21] "Just What Is An FBI Investigation? A Fact Sheet," The Brennan Center for Justice, May 20, 2013, https://perma.cc/9QXZ-UNJJ.

The most acute danger of using facial recognition to identify non-suspects is by scanning and seeking to identify faces of individuals engaged in First Amendment-protected activities, such as protesters, people attending political demonstrations and rallies, and individuals going to or from a house of worship. Such scanning can discourage conduct that the Constitution protects. Unfortunately, facial recognition has already been abused in precisely this manner: There are documented cases of numerous police departments using facial recognition to identify peaceful civil rights protesters.[22] While there are no known instances of such activity by federal law enforcement, relevant policies are disturbingly lax: FBI personnel are authorized to use facial recognition to identify individuals engaged in First Amendment-protect activities, so long as doing so is "pertinent to and within the scope of an authorized law enforcement activity," giving latitude to scan individuals at locations such as a protest or church if they are marginally connected to an investigation.[23,24] Any instances when federal law enforcement used facial recognition to identify individuals in such sensitive situations should be publicly disclosed.

Despite its potential for inaccuracy, use of facial recognition is often hidden from criminal defendants.[25] This practice undermines basic constitutional rights — specifically due process rights to disclosure of potentially exculpatory information — and increases the likelihood that the technology will be improperly used.[26] To better understand the scope of this problem, federal law enforcement agencies should disclose how frequent use of facial recognition as part of an investigation is disclosed to or withheld from defendants. Specifically, the government should publicly report how often facial recognition is used overall, how often such use leads to criminal charges, and how often it is disclosed to defendants.

Finally, use of facial recognition in the immigration context is problematically opaque. While some select programs, such as Customs and Border Protection's Biometric Entry-Exit, have been publicized and subject to input and oversight, we lack basic information on how facial recognition is used in other forms of immigration enforcement, in particular identification and detainment of undocumented individuals. DHS should release general information on which of its subcomponent agencies use facial

[22] See, fn 2.

[23] *FBI Facial Recognition Privacy Impact Assessment*. In terms of DHS policy, while Homeland Security Investigations contains the laudable policy that "photos from individuals actively exercising rights protected by the First Amendment" may not be subject to facial recognition scans, overall policies for ICE or DHS regarding use of facial recognition on individuals engaged in First Amendment-protect activities are unknown. See, *ICE Facial Recognition Privacy Impact Assessment*.

[24] DHS rules do not mention any special protections or rules for using the technology to identify individuals engaged in First Amendment-protect activities. See, *DHS Facial Recognition Policy Directive*. Published ICE rules only relevant restriction is that "HSI will not collect probe photos from individuals actively exercising rights protected by the First Amendment to the United States Constitution," but there is known limit on any other components of the agency from doing so. See, *ICE Facial Recognition Privacy Impact Assessment*.

[25] Khari Johnson, "The Hidden Role of Facial Recognition Tech in Many Arrests", *WIRED*, Mar. 7, 2022, https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests/; Jennifer Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short", *New York Times*, Jan. 12, 2020, https://perma.cc/6DAY-WFBM.

[26] For these reasons, discussed in detail in Section V, we believe disclosure to defendants should be required as a matter of policy.

recognition for general immigration enforcement and for what purposes, such as whether Border Patrol and ICE deploy it when stopping and questioning individuals inside the United States. It should also release statistics on how often its subcomponent agencies use the technology for immigration enforcement, and how often its use contributes to detainments and deportations.

IV. Deployment

Deployment of facial recognition absent strong rules and safeguards endangers civil rights and civil liberties. In order to prevent abuse, improper monitoring of sensitive activities, and disparate policing that harms civil rights and equity, we recommend federal law enforcement enact the following policy rules for any use of facial recognition:

1) Require probable cause that any individual who is the subject of a facial recognition scan committed a crime;
2) Limit use of facial recognition to prevention, investigation, and prosecution of serious crimes.

Additionally, we recommend DHS apply these policy rules to both immigration enforcement and law enforcement activities.

a) Probable Cause Standard

One of the greatest threats facial recognition poses is that it will be used to monitor and catalog public activities fundamental to democratic society, such as demonstrations, protests, political rallies, and religious activities. Using facial recognition in such situations threatens to chill participation, and enables targeting and harassment.

Unfortunately, facial recognition has already been misused in this manner. In 2015, following the death of Freddie Grey in police custody, Baltimore police used facial recognition to disrupt and selectively punish protesters by identifying and arresting individuals with outstanding warrants for unrelated offenses.[27] In 2020, several Florida cities used facial recognition to identify and catalog activists engaging in peaceful protests and community activities supporting the Black Lives Matter movement.[28]

Current federal law enforcement standards for use of facial recognition are far too lax to prevent this type of surveillance. Because FBI guidelines permit use of facial recognition even for assessments when there is no factual predicate of criminal activity[29] — and overall DHS policy contains no restrictions on

[27] See, fn 2.
[28] See, fn 2.
[29] See, *FBI Facial Recognition Privacy Impact Assessment*.

identification[30] — facial recognition could be used to identify protesters based on broadly defined "intelligence" efforts, as was the pretext when misused against protesters in Florida.[31] The breadth of surveillance of Black Lives Matter activists over the past decade and Muslim communities following the September 11 attacks reflect how dangerous facial recognition could be if permitted for general reconnaissance purposes.[32]

Even if use of facial recognition were limited to predicated criminal investigations, it could easily be abused through tangential connections between investigations and marginalized communities that are often subjected to improper surveillance. Applying low standards such as "relevance to an investigation," use of the technology would open the door to cataloging individuals en masse at a protest, mosque, church, political event, or community center simply due to proximity to a suspect.

To effectively prevent abuse, a strong standard is needed. Specifically, we recommend that federal law enforcement officers investigating a crime limit use of facial recognition to situations in which there is probable cause to believe that an unidentified individual to be scanned has committed the crime. This is a tried and tested model, first adopted as a law in Maine several years ago, with Montana following suit last year.[33,34]

While this standard would effectively guard against abuse in the criminal context, it should have relatively little impact on legitimate law enforcement activities. The most common genuine investigative use of facial recognition is to identify unknown individuals from crime scene photos and video. Because such photos show individuals in commission of a crime (or at a crime scene with their

[30] See, *DHS Facial Recognition Policy Directive*. According to published ICE policies, its Homeland Security Investigation unit limits facial recognition identification to suspects and victims ("HSI will only create probe photos from individuals suspected of participating in or being victimized by a crime under its legal authority"), but there is no such policy for ICE or DHS more broadly. See, *ICE Facial Recognition Privacy Impact Assessment*.

[31] Joanne Cavanaugh Simpson and Marc Freeman, "South Florida police quietly ran facial recognition scans to identify peaceful protestors. Is that legal?", *Sun Sentinel*, June 26, 2021, https://perma.cc/V6PT-S2JB ("at least three agencies — the Broward Sheriff's Office and the Boca Raton and Fort Lauderdale police departments — submitted more than a dozen images that referenced protests or protesters, but no crimes …. police ran nearly 20 searches linked to 'Intelligence,' a controversial use of the technology before a crime has even been committed").

[32]See, Maggie Miller, "FBI misused surveillance authorities to investigate Black Lives Matter protesters," *Politico*, June 19, 2023, https://perma.cc/3LPP-7E8S; see also, Diala Shamas and Nermeen Arastu, Creating Law Enforcement Accountability & Responsibility Project, Asian American Legal Defense and Education Fund, and Muslim American Civil Liberties Coalition, *Mapping Muslims: NYPD Spying and its Impact on American Muslims* (June 28, 2012). https://perma.cc/K9HS-9CMQ.

[33] Specifically, the Maine model creates an internal requirement for law enforcement that police may only use facial recognition "when there is probable cause to believe that an unidentified individual in an image has committed the serious crime." MRS Title 25, §6001. The Montana law goes further, requiring police obtain a warrant to conduct a scan based on probable cause. CDT supports a full warrant requirement, but as a matter of internal agency policies believes it would be highly effective for federal law enforcement to adopt the Maine model. SB 0397 (2023)

[34] Beyond their general probable cause requirement for scans of suspects, both states' laws also include exceptions for identifying victims, missing persons, and incapacitated or deceased individuals. CDT supports these exceptions, and believes they should be applied to the probable cause rule we recommend federal law enforcement adopt. CDT also supports an exception from the probable cause rule for post-arrest booking.

role as perpetrator confirmed by witnesses), meeting the probable cause standard should not be an onerous burden that would prevent use of facial recognition. It would be in cases of fishing investigations and unsubstantiated uses where the probable cause standard would have the greatest impact.

b) Serious Crime Limit

Facial recognition should not be used in a draconian manner, or to facilitate disparate policing practices that undermine civil rights and equity. In autocratic regimes, facial recognition is commonly employed on an overbearing scale to undermine individual autonomy. For example, in China, facial recognition is deployed for mass enforcement of minor offenses such as jaywalking, a tactic for promoting social control and turning entire cities into panopticons.[35] It is also weaponized for selective maltreatment of China's Uyghur minority.[36] In Iran, facial recognition is used to detect and identify women who do not wear a hijab "correctly," as well as to threateningly inform individuals they have been cataloged participating in unlawful demonstrations.[37]

Ensuring facial recognition cannot be weaponized to create an overbearing "Big Brother Is Always Watching" mentality or for selective policing of marginalized communities requires limiting its use to combating serious crimes. The danger of using facial recognition for selective prosecution of minor offenses is especially pronounced when combined with the problem of municipalities stockpiling bench warrants for low-level offenses, such as unpaid traffic tickets.[38]

The concept of limiting powerful surveillance tools to serious crime investigations is a longstanding principle in American law and policy: For over 50 years, U.S. law has limited real time electronic

[35] Alfred Ng, "How China uses facial recognition to control human behavior", *CNET*, Aug. 11, 2020, https://perma.cc/P6Y3-U7XV ("The punishing of these minor offenses is by design, surveillance experts said. The threat of public humiliation through facial recognition helps Chinese officials direct over a billion people toward what it considers acceptable behavior, from what you wear to how you cross the street").

[36] Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", *New York Times*, Apr. 14, 2019, https://perma.cc/2X8B-JUT3.

[37] Sam Biddle and Murtaza Hussain, "Hacked Documents: How Iran Can Track And Control Protesters' Phones", *Intercept*, Oct. 28, 2022, https://perma.cc/EA56-9Q2Q; Khari Johnson, "Iran to use facial recognition to identify women without hijabs", *Ars Technica*, Jan. 11, 2023, https://perma.cc/HGR4-6BCB.

[38] For example, a 2015 DOJ investigation revealed that Ferguson, Missouri, had active bench warrants — mostly for minor offenses such as unpaid fines for traffic violations — for 16,000 people in a 21,000 person municipality. Ability to freely use facial recognition in relation to minor offenses under such circumstances would effectively create an "scan and arrest at will" authority to be wielded against over three-quarters of the community. See, Department of Justice Civil Rights Division, *Investigation of the Ferguson Police Department*, (March 4, 2015) 3-6, 55. https://perma.cc/YVW5-JLGP; see also, Duda-Banwar, J., & Burt, J. M. (2022), "Living with Warrants: Life Under the Sword of Damocles," *CrimRxiv*. https://perma.cc/Q672-5T8F ("The majority of arrests are for low-level offenses, including misdemeanor crimes and violations …. In many jurisdictions, non-criminal offenses, such as unpaid traffic tickets, frequently escalate into criminal offenses … These traffic violations, which carry no jail time, are the most common original offense for bench warrants … Even federal law enforcement has been impacted by these low-level warrants").

surveillance to a set of serious crimes enumerated in the Wiretap Act.[39] Given its power and potential to facilitate unfettered surveillance, facial recognition should be bound by this same principle. We recommend that federal law enforcement limit use of facial recognition to prevention, investigation, and prosecution of a specific set of serious offenses. Specifically, we recommend limiting use to responding to a "Serious Violent Felony" as defined in 18 USC 3559(c)(2)(F), or the Wiretap Act set of offenses listed in 18 USC 2516.[40] While doing much to alleviate risk of abuse and selective policing of marginalized communities, this policy would focus the use of facial recognition on public safety priorities.

c) Application to Immigration Enforcement Activities

DHS should apply these rules not only to its activities conducted for law enforcement purposes, but also for those which involve immigration enforcement, as immigration enforcement involves the same risks that prompt the need for a probable cause rule and serious crime limit in the law enforcement context. Without such rules, the risk of selective enforcement aimed at harming and chilling marginalized communities is acute. Despite longrunning policies on protected areas, ICE has repeatedly targeted essential social services such as hospitals, courts, schools, and churches.[41] Use of facial recognition in combination with such activities would dramatically amplify their harm. Even outside these especially fraught locations, potential for general use of the technology at residential areas and workplaces suspected of mere visa overstays risks opening the door to fishing efforts, pervasive monitoring, and selective enforcement being weaponized for abuse. Finally, using facial recognition for immigration during field work without probable cause of wrongdoing, such as by Border Patrol during a standard stop inside the border zone, also creates serious risk of misidentification. In such variable conditions, and absent review and confirming evidence, such use could lead to citizens and lawful residents being improperly detained and forced to demonstrate their status. Of course, if there were probable cause that an immigrant had committed a serious crime, use of facial recognition for immigration enforcement regarding that individual would be permissible.

V. Redress

[39] Such surveillance is also permitted for foreign intelligence purposes, although use of information collected via such surveillance as evidence in criminal court proceedings is limited to a set of serious crimes as well. See, 50 USC 1881a(j)(3)(D).

[40] CDT believes that of these two options, the "Serious Violent Felony" limit more effectively pairs with the range of crimes facial recognition would be most useful in responding to. However, enacting a serious crime limit based on either option would be a significant policy improvement for federal law enforcement.

[41] See e.g., Katie Shepherd "ICE Arrested an Undocumented Immigrant Just Outside a Portland Hospital," *Willamette Weekly*, October 31, 2017. https://perma.cc/QH4Y-P6NL; Trevor Hughes, "Immigration agents accused of targeting parents taking their kids to school," *USA Today*, February 27, 2020, https://perma.cc/M6SX-79FJ; "String of ICE arrests at Philadelphia courthouse denounced, community seeking investigation" *Fox29 Philadelphia*, December 4, 2023, https://perma.cc/639G-Z8HN; Julie Carey, "ICE Agents Arrest Men Leaving Fairfax County Church Shelter," *NBC Washington*, February 19, 2017, https://perma.cc/K2D8-HELM; Ted Sherman, "AG criticizes ICE arrests of immigrants as kids were going to school," *NJ.com*, January 26, 2018, https://perma.cc/6QYF-8CJ3; Abené Clayton, "Courts must be safe spaces: Ice arrests undo long-held migrant protections, lawyers warn," *Guardian*, March 13, 2020, https://perma.cc/7CL6-7HTT.

Proper redress for improper use of facial recognition has been severely hampered by the persistent practice of failing to disclose its use in court proceedings and to defendants, which occurs in spite of significant reliance on the technology.[42,43] This secrecy both undermines the basic constitutional rights of defendants, and disincentivizes responsible law enforcement practices. The basic threshold for redress is awareness of when and under what circumstances the technology is used, giving affected individuals the potential to pursue appropriate remedies.

Disclosure is critical given the potential for error in facial recognition systems. Even the most accurate systems can make errors leading to misidentification.[44] Situational factors such as lighting, camera angle, distance, photo resolution, and obstructions can significantly impact accuracy, and will vary in quality across different situations.[45]

Questionable practices in facial recognition software settings and image treatment impact accuracy as well. One common issue is the confidence threshold that is deemed acceptable to return matches. Many law enforcement agencies, including the FBI, set their systems to *always* return a set of potential matches for facial recognition scans, no matter how low the confidence level for those matches is.[46] Such a practice will inevitably pull innocent individuals into investigations based on unreliable pretenses.

Even more troublingly, law enforcement entities regularly employ irresponsible methods to alter or replace images they are scanning, ranging from using computer-generated imagery (CGI) to artificially fill in uncaptured portions of a face, to scanning a composite sketch rather than a photo.[47] In one

[42] Jennifer Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short," *New York Times*, January 12, 2020. https://perma.cc/6DAY-WFBM. ("[Facial recognition] results still can play a significant role in investigations, though, without the judicial scrutiny applied to more proven forensic technologies …. In some of the Florida cases The Times reviewed, the technology was not mentioned in initial warrants or affidavits. Instead, detectives noted "investigative mean" or an "attempt to identify" in court documents, while logging the matters as facial recognition wins in the Pinellas County records").

[43] While failure to disclose use of facial recognition may simply be due to lack of understanding about the technology and its importance, there is some evidence of malicious motives, with one major police department deliberately instructing officers to avoid disclosure, instructing them "Do not let the software become exculpatory evidence" in a training presentation. See, Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Center on Privacy & Technology at Georgetown Law (2022), fn. 326, https://perma.cc/PA7H-62N4.

[44] See, Section II.

[45] See, fn 7.

[46] According to then-FBI Deputy Assistant Director Kimberly Del Greco, its system is set up so that it "returns a gallery of 'candidate' photos [reference photos] of 2-50 individuals (the default is 20).",*Deputy Assistant Director Kimberly Del Greco Statement*; see also, *FBI Facial Recognition Privacy Impact Assessment* ("A gallery of two to fifty photos will be returned, with the law enforcement agency choosing the size of the gallery. If no choice is made, a default of twenty photos is returned.").

[47] These activities include using CGI built into facial recognition software or even basic Google images searches to alter images in ways such as: "'Removal of Facial Expression'—such as replacing an open mouth with a closed mouth …. 'Insertion of Eyes'—the practice of "graphically replacing closed eyes with a set of open eyes in a probe image …. 'Mirrored effect on a partial face'—copying and mirroring a partial face …. 'Creating a virtual probe'—combining two face photographs of different people whom detectives think look similar to

documented case, police went so far as to replace a low-quality crime scene photo with a celebrity lookalike.[48] In the absence of the oversight and accountability that disclosure would provide, instead of being fringe cases, these dubious methods have become common practices.[49]

Law enforcement will often argue that corrective oversight is unnecessary because facial recognition "is just used for leads," implying that erroneous matches will be uncovered during the course of an investigation.[50] However, as previously described, faulty facial recognition matches have served as the sole basis for arrests and jail time for numerous individuals.[51] In order to prevent this, many law enforcement agencies, including the FBI and DHS, employ guidelines that facial recognition matches may not be the sole basis for arrests.[52] This is a laudable policy, and CDT has recommended it be enshrined into law.[53]

However, that measure is far from sufficient to prevent the harm misidentifications cause. Even in providing lead value rather than serving as the sole basis for arrest, facial recognition matches can shape investigations, and in the case of errors, lead them astray. According to a report from the Center on Law & Technology at Georgetown Law, "In multiple other investigations, the face recognition match was paired with highly suggestive, legally impermissible or otherwise deficient evidence to meet the probable cause threshold."[54] The value that leads provide varies significantly, and overreliance can be highly detrimental. This has proven true even for forensic science methods — such as bite mark analysis, footwear analysis, and lie detector tests — that were treated as objective and highly reliable,

---

generate a single image to be searched …. using 3D modeling software to complete partial faces and to 'normalize' or rotate faces that are turned away from the camera. After generating a 3D model, the software will fill in the missing facial data with an approximation of what it should look like, based on the visible part of what the subject's face looks like as well as the measurements of an 'average' face." See, Clare Garvie, "Garbage In, Garbage Out | Face Recognition on Flawed Data," Georgetown Law Center on Privacy & Technology, May 16, 2019, https://perma.cc/49K8-GEYV.

[48] Clare Garvie, "Garbage In, Garbage Out | Face Recognition on Flawed Data," Georgetown Law Center on Privacy & Technology, May 16, 2019, https://perma.cc/49K8-GEYV ("One detective from the Facial Identification Section (FIS), responsible for conducting face recognition searches for the NYPD, noted that the suspect looked like the actor Woody Harrelson …. A Google image search for the actor predictably returned high-quality images, which detectives then submitted to the face recognition algorithm in place of the suspect's photo").

[49] For example, then-Commissioner of the New York Police Department James O'Neill in a 2019 op-ed actively highlighted that the department used computer imaging to model half of a face artificially before running a scan of it. But because faces are not genuinely symmetrical and facial recognition systems evaluate full facial contours, this is not a reliable use. See, James O'Neill, "How Facial Recognition Makes You Safer," *New York Times*, June 9, 2019, https://perma.cc/HL98-AFK3 ("The system can also create a mirror image of the right side of a face if we have only the left side, for example, to produce a 3-D model").

[50] For example, FBI Director Christopher Wray responded to inquiries on face recognition during a Congressional hearing by stating "We use it for lead value. We don't use facial recognition as a basis to arrest or convict." House Judiciary Committee. Oversight of the Federal Bureau of Investigation: Hearing before the House Judiciary Committee, 116th Cong. (February 5, 2020).

[51] See, fn 1.

[52] See, *FBI Facial Recognition Privacy Impact Assessment;* see also, *DHS Facial Recognition Policy Directive*.

[53] See, Artificial Intelligence and Human Rights: Hearing before the U.S. Senate Committee on the Judiciary Subcommittee on Human Rights and the Law, 118th Cong. (June 13, 2023) (statement by Alexandra Reeve Givens President & CEO, Center for Democracy & Technology), https://perma.cc/Q6BK-X39P.

[54] Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Center on Privacy & Technology at Georgetown Law (2022), https://perma.cc/PA7H-62N4.

but in reality were subjective and prone to error.[55] It is critical that the same overreliance not occur with facial recognition, but masking its use from courts and defendants makes this goal far more difficult to achieve.

Disclosing use of facial recognition is critical to protecting constitutional rights. A long-established component of individuals' Fifth Amendment due process rights is ensuring defendants have the ability to examine all evidence that may be of an exculpatory nature or help challenge the credibility of government witnesses.[56] Reliance on facial recognition in a problematic manner (such as conducting a scan of a CGI created image) creates concerns that could be vital to an individuals' defense. But even more standard uses of the technology leave a litany of questions that a defendant should be entitled to evaluate: What software was used, and how accurate is it? What confidence threshold was employed? Were other potential matches returned and investigated? What was the quality of the photo scanned? Was the photo altered, and if so, in what ways?[57] A state appellate court last year recognized the importance of disclosure, concluding that facial recognition was "novel and untested, and the possibility that errors in the technology may exculpate [the] defendant," and that information on its use "is vital to impeach the witnesses' identification, challenge the State's investigation, create reasonable doubt, and demonstrate third-party guilt."[58]

Disclosure of facial recognition's use is also an important means of ensuring efficacy. Disclosure rules, and the threat that evidence will be excluded or deemed uncredible if courts and defendants discover deficiencies, is a basic means of ensuring responsible law enforcement conduct. Disclosing use of facial recognition will aid not only defendants, but also improve law enforcement practices and public safety by discouraging improper, unvetted, and sloppy use of the technology.

For these reasons, CDT recommends that federal law enforcement develop policies to ensure that defendants receive notification whenever facial recognition was used during an investigation, as well as all pertinent information about its use.

VI. Accountability: Ensuring Oversight of Personnel Using Facial Recognition

[55] See, President's Council of Advisors on Science and Technology, *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods* (September 2016), https://perma.cc/L73U-53WX; see also, Joseph Stromberg, "Lie detectors: Why they don't work, and why police use them anyway," *Vox*, December 15, 2014, https://perma.cc/SM4L-BMSY.
[56] *Brady v. Maryland*, 373 U.S. 83 (1963).
[57] The National Association of Criminal Defense Lawyers highlights these forms of information as useful for defendants in providing exculpatory evidence or suppression remedies that may be vital to their cases. See, Kaitlin Jackson "Challenging Facial Recognition Software in Criminal Court," National Association of Criminal Defense Lawyers, https://perma.cc/V4VN-NKUY.
[58] *State of N.J. v. Arteaga*, 476 N.J. Super. 36 (App. Div 2023).

Effective rules for use of facial recognition will provide little value unless there are effective procedures to ensure compliance. In order to achieve this, we recommend:

1) That use of facial recognition is limited to specialized staff members who receive training and are subject to careful oversight; and
2) Rules for use of facial recognition are also applied when the FBI conducts facial recognition scans on behalf of state and local law enforcement, with oversight mechanisms to ensure compliance.

In recent years there have been widespread problems of law enforcement officials — including those within federal law enforcement — using facial recognition systems in a manner inconsistent with agency guidelines, or in situations in which agencies do not have policies at all.[59] This creates an array of dangers, ranging from haphazard uses to outright abuse. To ensure compliance with rules, it is necessary to limit the use of the technology to specifically authorized individuals, who not only receive proper training, but are also subject to rigorous auditing and oversight in their use of the technology.

We recommend that federal law enforcement limit use of facial recognition to staff within specialized units, with broader use prohibited. Personnel in these specialized units should receive training in agency rules and guidelines for the technology's use. These officials should also be trained to have technical expertise, such as knowledge of image factors affecting match accuracy, appropriate confidence thresholds to employ, what types of alterations to images are permissible or reckless, and how to evaluate the value of potential match results.

Forensic examinations are often conducted separately from the investigations to which they contribute. This not only allows for review by experts, it prevents confirmation bias and other forms of contamination. Facial recognition should be treated the same way as these isolated forms of forensic review, another reason for limiting use to specialized units.

It is important to also recognize and account for how facial recognition flows from federal law enforcement to state and local police. In particular, the FBI Next Generation Identification-Interstate Photo System (NGI-IPS) is used to run facial recognition scans for state and local law enforcement entities across the country.[60] Yet there is disturbingly little public knowledge on how the results of this system are used: What range of crimes do local police use FBI facial recognition scans to investigate? Are requested scans always of criminal suspects, or conducted for more broad surveillance purposes? Are they ever conducted to identify individuals in conjunction with protests, or other First

[59] See, *2023 GAO Report on Facial Recognition*.
[60] The Perpetual Line-Up: Unregulated Police Face Recognition in America, Georgetown Law Center on Privacy and Technology, Oct. 18, 2016, https://perma.cc/NJ37-KJ2D; see also, *FBI Facial Recognition Privacy Impact Assessment*.

Amendment-protected activities? Are FBI facial recognition scans conducted for police departments that the DOJ is investigating or suing for civil rights violations? Are scans themselves ever used in support of policing practices that violate civil rights? Is the technology's use hidden from defendants?

Accountability requires ensuring responsible use not only by federal law enforcement itself, but also by state and local law enforcement on whose behalf the FBI uses facial recognition. To achieve this, we recommend that NGI-IPS and any other federal law enforcement use of facial recognition on behalf of state or local law enforcement be subject to the same type of rules and policies we propose above, specifically:

1) Requests can only be made when there is probable cause that the individual to be scanned committed a crime;[61]
2) Requests can only be made to support investigation of serious crimes; and
3) Requests can only be made if the requesting agency maintains a policy of disclosing use of facial recognition to defendants.

Federal law enforcement should ensure compliance with these rules with rigorous reporting requirements and auditing procedures. Any department that fails to comply with rules for use should be prohibited from receiving further support.

***

We thank DOJ and DHS for soliciting comments from stakeholders and affected communities on this important issue, and its ongoing work to develop effective guidelines and limits on law enforcement's use of facial recognition that protect civil rights and civil liberties, as well as improve efficacy. CDT is eager to serve as a resource in the ongoing evaluation of this important issue. For additional information, or any inquiries, please contact Jake Laperruque (jlaperruque@cdt.org), Deputy Director of CDT's Security and Surveillance Project.

[61] Such a rule should be subject to the same exceptions described above, see fn 34.