January 15, 2022

Office of Science and Technology Policy
Executive Office of the President, Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, DC 20504

Via email: BiometricRFI@ostp.eop.gov

Subject: Comment in Response to Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

To the Office of Science and Technology Policy:

Thank you for the opportunity to submit comments to the White House Office of Science and Technology Policy regarding use of biometric technologies for the purposes of identity verification, identification of individuals, and inference of attributes. Law enforcement use of face recognition involves the risk of misidentification as well as misuse — each of which causes serious harm to civil rights, civil liberties, and public welfare.

Our comment will focus on one biometric identification technology — face recognition — that is already used on a large scale by local, state, and federal law enforcement. Our comment describes the multitude of dangers face recognition, as currently deployed, poses to civil rights and civil liberties, examines how current federal government policies contribute to this danger, and recommends a series of White House policies to reduce the harm face recognition causes.

Founded in 1981, the Project On Government Oversight (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.

The Constitution Project at POGO centers its work on issues such as guarding against improper and overbroad surveillance, including unchecked face recognition. In 2019, The Constitution Project at POGO convened a face recognition task force of expert stakeholders to examine the impact of face recognition surveillance.¹ The task force included academics, tech experts, civil rights and civil liberties advocates, and law enforcement officials. Our group concluded that any law enforcement use of face recognition should be subject to strong limits, and provided a set of policy recommendations to support legislatures in the creation of reasonable but necessary limits.

Law Enforcement’s Use of Face Recognition Is Already Significant

At least one in four state and local police departments have the capacity to run face recognition searches, either directly or through a partnering agency. According to a BuzzFeed News investigative report, over 1,800 publicly funded agencies have used Clearview AI — a face recognition system that is especially problematic for developing a photo database built on scraping social media without users’ consent.

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.

Federal use of face recognition extends beyond the FBI. Sixteen federal agencies use face recognition, including half a dozen that employ it in criminal investigations. Notably, Immigration and Customs Enforcement has in recent years run thousands of face recognition searches of state drivers’ license databases, sometimes without oversight and approval of state officials. ICE’s access to face recognition appears to be a driving factor in the detention of immigrants.

Face Recognition Misidentifications Cause Serious Harm to Civil Rights, Civil Liberties, and Public Welfare

One of the most acute risks of face recognition is its potential to misidentify individuals. In terms of law enforcement use, this could lead to incorrect identification of suspects, as well as wrongful arrest and incarceration.

---

Face Recognition Misidentifications Stem from a Variety of Causes, Many of Which Cannot Be Prevented

First, the quality of face recognition algorithms can vary significantly, causing acute harms to civil liberties. Notably, many algorithms misidentify women and people of color at a higher rate than other people. Studies by the National Institute of Standards and Technology; the Massachusetts Institute of Technology, Microsoft, and AI Now Institute researchers; the American Civil Liberties Union; and an FBI expert all concluded that face recognition systems misidentify women and people of color more frequently. Most recently, the National Institute of Standards and Technology found that some systems were 100 times more likely to misidentify people of East Asian and African descent than white people. Failure to recognize the significance of this problem — and account for it in selection and review of software, training, and auditing — will undermine investigations, seriously endanger civil rights, and undermine efforts to reduce systemic bias in policing and the criminal justice system.

Second, image quality can also significantly impact the accuracy of matches. Sets of reference images — databases containing previously identified faces — in face recognition systems are typically high-resolution photos of a person directly facing a camera at close range, such as for a mug shot photo. But probe images — from which law enforcement seeks to identify individuals — are derived from a wide range of situations, which creates the potential for low image quality and erroneous results. Bad lighting, indirect angles, distance, poor camera 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.

Third, even when using more effective software and higher quality images, system settings can make face recognition matches prone to misidentification. For example, the way law enforcement sets confidence thresholds — a metric used to compare which proposed matches within a system are more likely to be accurate — can undermine the reliability of results. The lower the confidence threshold, the more likely the “match” is actually a false positive. So, if law enforcement entities set face recognition systems to always return potential matches — no matter how low confidence the


threshold — they will receive untrustworthy data. Troublingly, some law enforcement entities, including the FBI, do just that.  

In the absence of safeguards to address this range of misidentification risks, face recognition will continue to provoke errors, harm innocent individuals, and exacerbate inequalities in how different communities are policed.

**Using Face Recognition to Generate Leads Does Not Avoid Harms Such as Wrongful Arrests**

Law enforcement officials supporting the use of face recognition, such as FBI Director Christopher Wray, downplay the dangers of misidentification by arguing that face recognition is just used for leads. But this ignores a basic fact: Leads can vary immensely in how reliable or delusive they are, as well as how much or how little they might impact the course of an investigation. Law enforcement has previously relied heavily on certain “scientific” forensic evidence techniques — techniques that have been touted as presumptively objective, consistent, and reliable — that were, in fact, highly misleading. As is the case with bite-mark analysis or lie detector tests, the fact that face recognition is merely used as a lead does not prevent it from producing errors that cause the arrest or incarceration of innocent individuals.

Individuals could be — and in numerous recorded cases have been — charged in part based on how a face recognition match affects the direction of an investigation early on. Law enforcement overconfidence in the accuracy of matches can promote confirmation bias and sloppy follow-up, limiting the ability to identify face recognition errors.

It is also important to recognize that even if errors in face recognition systems are eventually discovered and accounted for, face recognition mismatches can form the basis of individuals becoming investigative targets. A variety of disruptive and potentially traumatic police actions can

---


16 For example, during a 2020 Congressional hearing, FBI Director Christopher Wray responded to inquiries on face recognition 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), https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=2780.


19 For example, in one incident, New York City Police Department officers allegedly took a face recognition match, and then rather than try to legitimately confirm or disconfirm its accuracy, instead texted a witness, “Is this the guy…?” along with a single photo, rather than following proper procedure to use a photo array. Clare Garvie, “Garbage In, Garbage Out: Face Recognition on Flawed Data,” Georgetown Law Center on Privacy & Technology, May 16, 2019, https://www.flawedfacedata.com/.
flow from such errors, such as being stopped, searched, monitored for prolonged periods of time, or detained and questioned. These harms will be disproportionately borne by people of color so long as algorithmic bias is present in face recognition systems, and more generally so long as systemic bias impacts policing and our criminal justice system.

It is critical when evaluating these harms to consider the real-world human cost. Take for example the impact that a faulty face recognition match had on Robert Williams, who was arrested at his home and subsequently held in custody for 30 hours:

During the time that I was in custody, my wife was dealing with the emotional and practical immediate fall out. My daughters were scared, wondering why their father had been arrested and whether he would come home. My wife had to comfort them. While I was away, our oldest daughter turned over a family photo that was sitting out on the family furniture because she couldn’t bear looking at a picture of her Daddy under the circumstances. My wife also had to call my employer and explain to them where I was and why I wouldn’t be coming to work that day. They could have fired me right then …. My daughters can’t unsee me being handcuffed and put into a police car. They continue to suffer that trauma. For example, after I returned from Jail, they started playing cops and robbers games where they tell me that I’m in jail for stealing. And even today, when my daughters encounter the coverage about what happened to me, they are reduced to tears by their memory of those awful days.20

Despite this traumatic experience, Williams describes himself as “lucky” that the harm he and his family unjustly experienced was not more severe.21

Finally, the notion that face recognition matches are merely leads that serve as one of many components of an investigation is often simply untrue. There are already three documented cases where individuals were wrongfully arrested — with two spending time in jail — based entirely on bad face recognition matches.22 According to a 2020 New York Times investigation of face recognition systems in Florida, “Although officials said investigators could not rely on facial recognition results to make an arrest, documents suggested that on occasion officers gathered no other evidence.”23 And because use of face recognition in investigations is often hidden from arrestees and defendants, there are likely many similar instances of face recognition being the sole basis for an arrest that remain hidden from the public.

Lack of Disclosure Augments Misidentification Risks and Undermines Due Process Rights

The risks of misidentification causing serious harm are increased by the fact that use of face recognition is often hidden from defendants. Given the wide range of technical factors that can impact face recognition’s effectiveness, it is critical that defendants are notified and given the opportunity to examine face recognition technology whenever it is used in an investigation, as they would with any other complex forensic tool.

Despite the importance of disclosure, it rarely occurs. In some jurisdictions, law enforcement uses facial recognition thousands of times per month, and defendants almost never receive notice of its use in investigations. Yet even as law enforcement relies on the technology for investigations, they obscure it from examination in court by defendants and judges.

Defendants have a vested interest in reviewing a variety of factors, such as algorithm quality, the software settings police used, and whether any other potential matches were discovered or investigated that could provide exculpatory or mitigating evidence. This is key not only to protecting innocent individuals, but also to preserving constitutionally guaranteed due process rights of all defendants and promoting genuine public safety.

Furthermore, guaranteeing access to this information is not only critical for due process rights, but also acts as an important safeguard to deter corner cutting and inappropriate use of face recognition during investigations.

**Face Recognition Also Creates Risks of Pervasive Surveillance that is Fundamentally Incompatible with Democratic Society**

One of the most important aspects of face recognition is that even if the government could mitigate the dangers of misidentification, doing so would not lessen the dangers of the technology as a whole. Simply put, face recognition surveillance is dangerous when it does not work, but also dangerous in a different — yet equally important — way when it does.

In the digital age, privacy rights do not just protect the inside of our homes from improper intrusion; they are also critical safeguards from overbearing government power. As Justice Sonia Sotomayor warned about emerging surveillance technologies when the Supreme Court first examined the issue of electronic location tracking, “making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track … may ‘alter the relationship between citizen and government in a way that is inimical to democratic society.’”

---

If unrestrained in its use, face recognition surveillance offers so much information and power to government that it could upend basic rights and foundations of democracy. In authoritarian regimes such as China, face recognition is used as a means of social control, with the technology serving as a means of mass cataloging of activities and draconian enforcement of minor offenses. It has been weaponized for continuous surveillance and brutal oppression of its Uighur minority. It is used to identify, discourage, and detain pro-democracy protesters.

The frightening abuse of face recognition technology is not limited to China. Officials in the U.S. have already used the technology to undermine fundamental features of democracy here.

According to a South Florida Sun Sentinel investigation, in 2020, law enforcement repeatedly used face recognition to identify and catalog peaceful protesters. Fort Lauderdale police ran numerous face recognition searches to identify people who might be a “possible protest organizer” or an “associate of protest organizer” at a peaceful Juneteenth event to promote defunding the police. Boca Raton police also ran face recognition scans on half a dozen occasions throughout May 2020 targeting protesters during peaceful events. And the Broward Sheriff’s Office ran nearly 20 face recognition searches during this same time period for the purpose of “intelligence” collection, rather than to investigate any criminal offense.

Face recognition has also been used to selectively target individuals who are protesting, with law enforcement using the technology to rapidly scan protests for individuals with active bench warrants for unrelated offenses. Several years ago, Baltimore police used face recognition amid protests to find individuals with “outstanding warrants and arrest[ed] them directly from the crowd,” in a selective effort that appeared to be aimed at disrupting, punishing, and discouraging demonstrators from protesting.

**Federal Use of Face Recognition Should be Seriously Curtailed to Protect Civil Rights and Civil Liberties**

Federal use of face recognition contains serious flaws, creating potential for both overreliance on misidentifications as well as misuse. The FBI systems guarantee that match results are returned for any scan, amplifying the risk of errors, as does the lack of oversight that stems from failure to disclose the use of face recognition to courts and defendants. FBI officials can conduct face recognition searches during this same time period for the purpose of “intelligence” collection, rather than to investigate any criminal offense.

---

recognition searches pursuant to both criminal investigations or mere open assessments, meaning that searches do not require probable cause, or even suspicion of wrongdoing.\(^{33}\)

ICE face recognition systems can similarly be used for photos that are “in furtherance of ongoing investigations,” and can be used to support immigration detention and deportation so long as the scan is not conducted “solely in furtherance of civil immigration enforcement.”\(^{34}\)

The risks of face recognition being misused should be taken especially seriously in light of how federal law enforcement has used surveillance to target protesters\(^{35}\) and the press in recent years,\(^{36}\) as well as lawmakers, their staff, and their families.\(^{37}\)

Currently, the only meaningful restriction on federal law enforcement use of face recognition is the FBI requirement that matches cannot serve as the sole basis for arrests or other law enforcement action.\(^{38}\) But for the reasons previously described, requiring that face recognition is only used for leads does not eliminate the risk of error. And lack of disclosure to defendants removes a key safeguard in ensuring that even this rule is effectively applied.

In order to effectively reduce the dangers posed by face recognition surveillance, we recommend the White House establish the following policy requirements for all federal law enforcement use of the technology:

- **Probable cause rule:** Require that all scans be predicated on probable cause that the individual to be identified has committed, is committing, or is planning to commit the offense being investigated.
- **Serious crime limit:** Limit use of face recognition to the investigation of violent felonies.
- **Disclosure requirements:** Require that any use of face recognition during an investigation is disclosed to defendants.

---


Federal Assistance to State and Local Law Enforcement for Face Recognition Use is Dangerously Unregulated and Must be Reformed

In addition to its direct use by federal law enforcement, the federal government provides significant support for face recognition surveillance by state and local law enforcement, with inadequate safeguards.

The FBI Next Generation Identification-Interstate Photo System (NGI-IPS) provides state and local law enforcement across the country with the ability to run face recognition searches on a mass scale. Searches can be run through NGI-IPS so long as the relevant photos are “obtained pursuant to an authorized criminal investigation,” but does not require probable cause or even suspicion of wrongdoing. FBI policy authorizes use of its system to identify exercising First Amendment-protected activities (such as lawful assembly and protests) so long as the scanned photo is “pertinent to and within the scope of an authorized law enforcement activity.”\(^39\)

These rules are insufficient to protect against pervasive surveillance and selective targeting, including the type of selective targeting that has previously been directed at peaceful protesters.

Further, FBI rules contain no known restrictions on which law enforcement entities are authorized to run scans through its systems, including those that may be under investigation by the Justice Department for systemic violation of constitutional rights — investigations the White House describes as “critical tools to promote constitutional policing in jurisdictions where reform is warranted.”\(^40\) This raises the important question of why the department would provide access to a powerful technology such as face recognition — which is susceptible to abuse and undermining constitutional rights — to police departments even as it acts to curtail systemic abuse within those departments.

Similar to its own policy rules, the FBI provides no meaningful restrictions on how state and local law enforcement use NGI-IPS for face recognition searches, other than to require that matches cannot serve as the sole basis for law enforcement actions such as arrests,\(^41\) an inadequate measure to guard against both overreliance on misidentifications as well as misuse. Even when NGI-IPS is used in a proper manner for legitimate law enforcement needs, the consistent pattern of leaving defendants uninformed undermines critical due process rights to review investigative evidence and techniques.

Further, the federal government should examine and act on its role in promoting inadequately restricted face recognition systems that are operated at the state and local level. Federal grant

---


funding for local policing has directly been used to create face recognition systems.\textsuperscript{42} Federal funds are also used to develop mass video surveillance networks that power the collection of images run through local face recognition systems.\textsuperscript{43}

The federal government bears responsibility if it — either by providing direct access to scans or funding for locally managed systems — enables state and local law enforcement to use face recognition in a manner that endangers civil rights and civil liberties, and should act to prevent such use. We recommend the White House establish the following policy requirements regarding assistance to state and local law enforcement involving face recognition:

- **Probable cause rule:** Only allow state and local law enforcement entities to run searches through NGI-IPS or other federal face recognition systems if scans are predicated on probable cause that the individual to be identified has committed, is committing, or is planning to commit the offense being investigated.

- **Serious crime limit:** Only allow state and local law enforcement entities to run searches through NGI-IPS or other federal face recognition systems if scans are for the investigation of violent felonies.

- **Prohibit use to bad actors:** Prohibit use of NGI-IPS or other federal face recognition systems by law enforcement entities under pattern and practice investigations for biased policing and other unconstitutional practices.

- **Disclosure requirements:** Require that any state and local law enforcement entity that uses NGI-IPS or other federal face recognition systems disclose such use to defendants.

- **Funding contingent on reasonable regulations:** Require that any state or local law enforcement entity that uses federal funding for face recognition or video surveillance that could be used for face recognition scans be conditioned on that entity abiding by these probable cause rules, serious crime limits, and disclosure requirements for its own use of face recognition.

Thank you for the opportunity to provide this comment in response to the White House Office of Science and Technology Policy’s request for information. We strongly hope the White House will adopt the recommended policies in support of its ongoing commitment to civil rights, civil liberties, and improving racial equity in criminal justice and policing.

Sincerely,

Jake Laperruque
Senior Policy Counsel
The Constitution Project at the Project On Government Oversight
