Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
ACLU of Massachusetts RFI Response: Biometric Technologies

Police use of machine learning-enabled biometric technologies like facial recognition poses unprecedented threats to basic civil rights and civil liberties, impedes racial justice, and undermines open, free, democratic society. These technologies can be used to identify and track people and groups, using their facial, iris, voice, and other features, turning fast-growing surveillance camera networks into inescapable dragnets enabling the mass tracking of people's movements, habits, associations, and political and religious activities.

The regulatory landscape pertaining to biometrics has changed dramatically in the past few years. But despite significant progress in parts of the country, most states—and the federal government—have not imposed democratic guardrails on police use of facial recognition or other remote biometric surveillance technologies.

Importantly, facial recognition is not one thing. Police can use facial recognition technology in at least three distinct ways, each raising different problems for civil rights and civil liberties: (I) identification and image matching, (II) surveillance, and (III) affect recognition. Short of banning the technology entirely, some states—like Maine and Massachusetts—have opted to regulate police use of image matching in limited situations, subject to law requiring centralization, privacy protections, and democratic controls. But for reasons described below, it is not possible to meaningfully regulate the use of facial recognition technology for surveillance or affect recognition. Indeed, the grave threats to privacy, freedom of speech and association, and racial justice posed by police use of these technologies can only be averted by prohibiting their use entirely.¹

I – Police use of facial recognition for identification and image matching

Law enforcement in the United States has used facial recognition for identification and image matching purposes for at least twenty years. Facial recognition for image matching and identification is the most common police use of the technology in the United States. Police use image matching to confirm the identity of a person in an image, or to put a name to a face. Typically, this is done by using a facial recognition algorithm to compare a still image (e.g. from human review of surveillance camera footage, a social media account, a police surveillance photograph, or other source) to a database of identified faceprints (e.g. a driver’s license or state identification database).

The first decade of the 21st century saw a quiet but massive expansion of law enforcement use of the technology for this purpose, thanks to National Highway and Traffic Safety Administration grants to state motor vehicle and licensing agencies to acquire facial recognition systems. While these systems were purchased to help registries identify fraud in the licensing process, their use was subsequently expanded to include police investigations.

According to records obtained by the ACLU, for example, the Massachusetts Registry of Motor Vehicles obtained a facial recognition system in 2006 and only months later sent a memo to state and local police offering to perform facial recognition searches on their behalf. The registry went on

¹ Below we provide the ACLU of Massachusetts’ (“ACLUM”) views on police use of biometrics technology, focusing specifically on facial recognition. This submission reflects the views of the ACLUM, and not necessarily the National ACLU or other ACLU affiliates.
to perform hundreds of facial recognition searches for police and federal agencies per year, subject to no regulation or privacy protections.\(^2\)

The FBI likewise maintains its own facial recognition program and database, containing at least 640 million images of American adults, taken from both criminal and civil government processes across the country.\(^3\) The FBI ran 157,000 searches between fiscal year 2017 and April 2019.\(^4\)

In most states and at the federal level, police use of facial recognition for image matching and identification remains entirely unregulated. The following are important considerations for policymakers evaluating how to regulate police use of facial recognition for image matching and identification purposes: (A) databases; (B) algorithmic bias; (C) accountability and oversight; and (D) privacy protections.

### A. Databases

Not all databases are created equal. When police or federal agents use image matching facial recognition technology to try to confirm the identity of a person, or to identify an unknown person in an image, they can use any number of databases. Lawmakers and policymakers must consider two important factors when evaluating which data sets ought to be accessible to police for image matching searches: image quality and racial justice.

**First**, the quality of images in these databases matters. In recent years, images taken for official purposes like passports, mug shots, and drivers licenses are typically standardized, making them more appropriate for facial recognition image searching. Image subjects are advised to take off hats, glasses, and other things that obstruct a full view of the face; the images are taken from the front with high-quality digital cameras; the images are taken in full light, with no shadows on the face; and the images are stored in hi-resolution format. None of these things are consistently true of images scraped from social media sites, like those that populate privately-owned and controlled databases like the one maintained by Clearview AI.\(^5\) Instead, the image quality in these data sets varies widely, raising the likelihood of misidentification and wrongful arrest. Policymakers should therefore prohibit police use of images “taken from the wild” as comparison data when performing image matching searches.

**Second**, different data sets raise different racial justice and equity concerns. For many years, data has consistently shown that Black and Latino people have faced higher arrest rates than white people for various crimes, like drug offenses, despite engaging in criminal activity at similar rates.\(^6\) As a result, Black and brown people are more likely than white people to populate mug shot databases, even if they have never been found guilty of a crime—let alone a serious crime. Historic and ongoing racial disparities in arrest rates across the country have resulted in mug shot databases that are unjustifiably Blacker and browner than the general population. Allowing police to use mug shot databases for facial recognition searches would therefore exacerbate historical and existing racial disparities in policing by extending that bias into the future, unfairly subjecting people of color to enhanced

---


3 Michael Balsamo, “Watchdog says FBI has access to about 640m photographs,” June 4, 2019, AP. [https://apnews.com/article/technology-ap-top-news-politics-6a45659e3c084e5eac82edc145d6882](https://apnews.com/article/technology-ap-top-news-politics-6a45659e3c084e5e5eac82edc145d6882)


scrutiny and surveillance, in effect supercharging and automating inequality. Additionally, mug shot databases contain images of people suspected—not convicted—of criminal activity. The unfair racial makeup of these databases and the presumption of innocence both counsel in favor of prohibiting police use of mug shot databases for facial recognition purposes.

B. Algorithmic bias

Not all facial recognition algorithms are created equal, and many systems are not ready for primetime. As has been extensively documented by researchers and the federal government, facial recognition algorithms can exhibit race, gender, and age bias. These biases were initially discovered by the groundbreaking research of world-renowned scientists Joy Buolamwini and Timnit Gebru, and they are now widely acknowledged by the scientific community.

In 2019, the non-partisan federal government National Institute of Standards and Technology ("NIST") published a landmark study presenting further evidence that facial recognition algorithms across the board are biased against certain groups. NIST found that most of the nearly 200 algorithms tested performed worse on Black, Asian, and Native American faces, as well as women, the elderly, and children. In addition, when evaluating nationality, faces from West Africa, the Caribbean, East Africa, and East Asia resulted in more uncertainty and more false matches. Across the board, facial verification and identification scans performed best on middle-aged white men and worse on everyone else.

Face recognition technology works best when using front-facing, clear, high-resolution, high-light images. NIST uses these high-quality probe images to test bias and accuracy in facial recognition systems. But in criminal investigations, police often do not use high-quality probe images—the images are often of poor quality, showing people in bad lighting, at strange angles, or with objects obstructing their faces. Consequently, NIST’s survey results are misleading; the algorithms NIST studied likely perform much more poorly under real world conditions.

Police frequently argue that lawmakers and the public shouldn’t concern themselves too much with these problems, because facial recognition is just one tool in the law enforcement officer’s toolbox, and human review of facial recognition search results accounts for any bias and inaccuracy issues. But studies show people are more likely to believe the results of a facial recognition search than their own eyes.

Thus far in the United States, errors resulting from biased algorithms have tended to have the gravest impact on Black people. Police secrecy surrounding the use of facial recognition means we do not know how many people have been wrongfully arrested due to facial recognition errors. But thanks to increased public debate and press scrutiny about the technology, we now know of three such cases in recent years—all of whom are Black men.

---

11 Id.
These problems counsel in favor of regulation and law that, short of banning police use of facial recognition entirely, imposes rigorous oversight and accountability of police use of facial recognition for image matching. For the reasons described below, this oversight can only be achieved by centralizing police facial recognition technology.

C. Accountability and oversight

Oversight and accountability of police use of facial recognition technology for image matching in serious criminal investigations poses a substantial regulatory challenge. But as Maine and Massachusetts have demonstrated, it is possible to devise and implement regulatory frameworks wherein police use of facial recognition for image matching technology is centralized at one government agency per state, requiring all police use of the technology to flow through those central entities, limited to very serious criminal investigations, and subject to privacy and due process protections. The federal government could likewise require all law enforcement image matching to run through one centralized service and impose stringent checks and balances on its use. Doing so would mitigate threats to civil rights and civil liberties, facilitate meaningful oversight and accountability, and reduce the threat of wrongful arrests, while also protecting the integrity of the criminal legal system, by ensuring consistent technologies, standards, procedures, training, and techniques are applied across the board.

Centralization addresses the following key problems, described below in detail: I. Scale and police misconduct; II. Consistent technology and training.

I. Scale and police misconduct

There are roughly 18,000 law enforcement agencies in the United States, governed by a patchwork of local, state, and federal laws imposed and overseen by city councils, mayors, county governments, legislatures, and courts. There is no uniform, consistent, national method by which law enforcement agencies are subject to democratic control, transparency, oversight, or accountability.

Police accountability is a real challenge in the United States, in part because of the distributed nature of the power structure. Local control can yield positive results in jurisdictions with courageous local elected officials backed by organized residents. But local control just as often means there is effectively no meaningful oversight or accountability over policing—a problem that grows worse with the accelerating demise of local newsrooms. If a local mayor doesn’t want to risk political suicide by challenging a corrupt police department, residents rely on the FBI to step in. But the FBI—an institution with its own significant civil rights and civil liberties problems—cannot police all police; if it tried, it would do nothing else and still fail.

It is extremely difficult to hold police accountable in the United States, and to ensure they uphold the law. As a result, in police departments large and small, across the United States, police officers and departments routinely violate the law. According to an AP report published in 2016, police officers across the United States regularly abuse their access to surveillance databases. A Massachusetts State Trooper issued a rare reprimand for misusing his access to criminal record offender data (a crime in Massachusetts) told a reporter “it was a common practice for troopers to run someone’s name through the CORI system for reasons besides law enforcement.”

---

trooper appeared shocked to be punished for what he perceived to be routine violations of the law by police in Massachusetts.

Facial recognition image matching gives police unprecedented power to identify people in sensitive situations: seeking substance use treatment, attending political demonstrations and meetings, visiting politicians and elected officials, speaking with journalists, and getting treatment for serious health conditions like cancer. Police could use facial recognition image matching to identify who is speaking to a reporter working on a police corruption story, or to identify everyone who goes in and out of the mayor’s office while she is working on heated police union contract negotiations. Police could use facial recognition technology to get the name and address of a beautiful woman they see walking down the street. A police officer friendly to the January 6 insurrectionists could use the technology to identify even low-level staffers photographed in the West Wing or in Congress. In short, police can use the technology to violate people’s rights in ways previously impossible, for political and personal purposes.

It is particularly easy for police to use face recognition technology to violate people’s rights when the technology is 100 percent under the control of the police themselves, subject to no meaningful outside scrutiny. The app Clearview AI, for example, gives police officers the ability to use facial recognition for image matching on their personal cell phones.

For the reasons described above, it is impossible to ensure widely distributed police use of facial recognition technology would comport with even the strictest law meant to regulate its use. If 18,000 policing entities in the United States of America are lawfully allowed to possess facial recognition technology, the technology will be abused by close to 18,000 policing entities every year. We do not maintain the oversight and accountability architecture we would need to ensure the technology will not be abused and misused in the hands of so many police departments. Centralizing the technology in the hands of one entity per state, and one at the federal level, will help enable courts, legislators, journalists, and civil rights advocates to provide meaningful oversight and accountability of its use.

II. **Consistent technology and training**

The facial recognition market is crowded with hundreds if not thousands of different technologies sold by as many companies, based here in the United States and around the world. Each system’s algorithm performs differently, and each user interface offers different options to end users like police officers and forensic analysts. The wide variety of facial recognition technology available to policing entities could, left unregulated, lead to chaos in the criminal legal system. If each of the 18,000 policing entities in the United States is allowed to purchase or lease access to its own facial recognition system, each of them could end up using systems that operate with different levels of accuracy and reliability, using different training and operating procedures as suggested or required by the manufacturers. Such a widely distributed technology field poses insurmountable challenges to government entities responsible for overseeing policing agencies, as well as to courts and criminal defense attorneys. This is not a hypothetical problem; in the United States policing entities too often don’t even know what facial recognition systems their employees are using—or that they are used at all.

A June 2021 U.S. Government Accountability Office ("GAO") report illustrates the point.18 The GAO surveyed 42 federal agencies that employ law enforcement officers, asking questions about their use of facial recognition technology. The survey results reveal a chaotic and disorganized

---

situation. For example, while 14 agencies said they use non-federally owned facial recognition technology to support criminal investigations, only one agency could name that system.

Similar problems have unfolded across the country at the state and local level, as companies like Clearview AI have aggressively and directly marketed their technologies to even lower-level police officers. In many cases, police have used facial recognition technology without the knowledge—let alone approval—of their own superiors. ¹⁹

When police use facial recognition for image matching in criminal investigations, the stakes are extremely high. Consistent standards and technologies must be applied across policing entities, to protect against wrongful arrests and to ensure the integrity of the criminal legal process. Centralization is the only way to achieve consistency and enable oversight and accountability.

D. Privacy protections

Centralization of police use of facial recognition for image matching is necessary, but it is not enough to protect the public interest. The following privacy protections must also be enshrined in law: I. Limitation to serious crimes; II. Warrant requirement; III. Due process protections.

I. Limitation to serious crimes

Law enforcement agencies should not use facial recognition in all types of criminal investigations. The more police use the technique, the more likely they will make mistakes, leading to wrongful arrests and other harms. Loose rules enabling the police to use facial recognition for any type of criminal investigation also provide cover for misuse and abuse. For example, a police officer who wants to know the name of a person or group of people at a protest could justify a search using their images by alleging that they were trespassing or committing disorderly conduct when the photo was taken. This kind of intrusion cannot be tolerated in a free society. But unfortunately, these kinds of abuses are not hypothetical. ²⁰

Police should not be able to use facial recognition to identify people suspected of minor crimes. Instead, this invasive and controversial technique should be limited to the most serious types of crimes, such as murder, attempted murder, arson, rape, and kidnapping.

II. Warrant requirement

Facial recognition gives the government the power to put a name to any face, an unprecedented privacy invasion akin to forcing every person to wear a police-scannable barcode tattooed on their face. People have a reasonable expectation that the government will not invade their privacy in this manner without good reason and court approval. ²¹ Just like with cell phone location searches, which similarly allow the government to perform surveillance of people in public in a manner never before possible, the standard to obtain evidence derived from facial recognition should be the probable cause warrant.

Facial recognition searches ought to be limited to those cases where law enforcement agencies can show a judge probable cause that an unidentified individual in an image has committed a violent

---


²⁰ For example, in June, reporters disclosed that South Florida police used facial recognition technology to identify peaceful protestors in the aftermath of George Floyd's murder. Public records obtained by journalists "revealed that 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." On several occasions, the documents revealed, law enforcement agencies tried to identify people using terms like “Possible protest organizer ‘leaders of liberty’” and "associate of protest organizer ‘leaders of liberty’" and then used facial recognition scans to identify Peaceful Protestors Is That Legal?, The South Florida Sun Sentinel, June 26, 2021, https://www.sun-sentinel.com/local/broward/fl-ns-facial-recognition-protests-20210626-7tl5iuatqthba32n4xldvlw1htmlstory.html

felony, that the probe image is of sufficient quality to be subjected to facial recognition and has not been altered, and that the facial recognition search will reveal evidence of the crime. The standard exceptions to warrant requirements ought to apply, in emergencies and where an immediate threat to human life makes obtaining a warrant impractical.

III. Due process protections

The law must provide due process protections for persons arrested pursuant to criminal investigations involving the use of facial recognition technology.

Public defenders report that too often, police in the United States have not disclosed the use of facial recognition technology to criminal defendants. Without mandatory disclosure requirements, law enforcement appears to be shielding information about their use of facial recognition technology from courts and defendants. This practice threatens defendants' basic due process rights and the integrity of our criminal legal system. Criminal defendants must be able to interrogate any digital witness used against them, no matter whether police call it a “tip” or themselves consider it evidence.

If police investigate and then ultimately charge people with crimes after using facial recognition in a criminal investigation, defendants must be able to access critical details about those searches. It is essential that defendants have access to: information about the algorithm used to perform the search (including, if available, the results of accuracy and bias tests); depositions of technicians who perform the searches to find out what investigatory steps were taken after the search; the full results of the search, including images of other people if these were returned; information about the technical "confidence level" at which the system identified the defendant; and other information critical to mount a defense.

The law must additionally state that any result of a facial recognition search does not, without other evidence, establish probable cause justifying arrest, search, or seizure. Finally, the law must require agencies responsible for conducting facial recognition image searches to report the following information to the public on at least an annual basis, for each facial recognition search: the type of technology used, the agency requesting the search, the type of crime(s) under investigation, the race and other demographics of the person depicted in probe images searched, whether an arrest resulted from the search, and whether the search was undertaken subject to a warrant or in an emergency or exigent circumstance.

Part II – Mass Surveillance of Individuals

Machine learning enabled biometric technologies like facial recognition technology are dangerous when they work and when they don’t. When they work, these technologies allow the government to track every person’s public movements, habits, and associations, not on one day, but on all days—merely with the push of a button. When the technologies fail, racial and gender biases disproportionately harm women and people of color, putting them at risk of wrongful arrest and worse.

Unlike facial recognition for image matching, face surveillance analysis applied to video networks is not commonly deployed by police in the United States. The time is ripe to insist, through law and regulation, that we never build these systems in our communities. The extremely high costs imposed on our communities by face recognition surveillance do not outweigh its marginal benefits. For this and the reasons below, government agencies including police should be permanently prohibited from analyzing video data with face recognition and other machine learning enabled remote biometric surveillance technology.

1. Oversight and accountability are impossible
Unlike facial recognition for image matching, using face recognition for surveillance necessitates a distributed approach. As we describe above, it is possible and relatively simple to standardize and centralize police use of facial recognition for image matching. No such standardization or centralization is possible with face surveillance, because of the physical architecture of the technology.

Facial recognition surveillance works by applying automated analysis technology to video data produced by networked surveillance cameras, like those that exist in most major cities today. That means to use the technology, each city’s police department would by necessity operate its own facial surveillance network. The distributed nature of the surveillance makes effective oversight and accountability impossible—particularly given the heightened risks of this kind of surveillance.

II. B. Facial Recognition is the Perfect Tool for Oppression

People in free and open societies should be able to walk around their communities, visit friends and family, seek medical treatment, go to church, and attend political events without worrying that the government is secretly keeping tabs on their every movement, habit, and association. A jealous police officer should not have the capacity to monitor the activities of his girlfriend as she moves about a city; a star-struck officer should not be able to use advanced technology to track the movements of her favorite celebrity; and an officer with a political grudge should not be able to monitor the movements, habits, or associations of a political candidate he opposes.

Today, most cities maintain video surveillance networks across large geographic areas. Each year, governments add more cameras to these networks. The systems can be useful when serious crimes and car accidents occur, because officers can query video from a specific camera at a specific location, on a specific time and date, to look for evidence. The use of face surveillance and other biometric algorithms to automate the analysis of a city’s video data qualitatively changes the network, effectively allowing the government to query stored and real-time video images as if each frame were catalogued using the names of each person captured in each frame.

Today, video data is dumb, waiting for police to look at it when something goes wrong. Tomorrow, police could use face surveillance and other biometric analysis algorithms to apply a Google-like search feature to all video data, enabling officials to track and catalogue the movements, habits, and associations of any person, or of all people, merely with the click of a button. This kind of surveillance will not impact all people equally. Like other forms of surveillance, police use of face surveillance applied to video data will harm Black, brown, immigrant, and poor people first and worst.22

It is not an accident that the regimes making quick use of the technology for this purpose are authoritarian governments, like those in China and Russia.23 As scholars have written, face recognition surveillance is "the perfect tool for oppression."24

---


23 The Chinese government’s use of the technology is instructive. According to several reports, the Chinese government uses its network of surveillance cameras integrated with facial recognition technology to monitor millions of Uighurs in Xinjiang. “The facial recognition technology,” the New York Times reports, "looks exclusively for Uighurs based on their appearance and keeps records of their comings and goings for search and review. The practice makes China a pioneer in applying next-generation technology to watch its people, potentially ushering in a new era of automated racism." See: Paul Mozur, One Month, 50,000 Face Scans: How China is Using A.I. to Profil e a Minority, April 14, 2019, New York Times. According to these reports, the PRC has used face surveillance to track how many people of certain ethnic backgrounds are in a location at once, to monitor individual people’s movements and activities—including their religious worship habits—and even to flag that someone entered their house from the rear, instead of the front door. Recent reports indicate that police in China’s largest provinces are developing a surveillance system they say they want to use to track journalists and international students, among other “suspicious people.” See: "Exclusive: Chinese province targets journalists, foreign students with planned new surveillance system,” November 29, 2021, Reuters. https://www.reuters.com/technology/exclusive-chinese-province-targets-journalists-foreign-students-with-planned-new-2021-11-29/

24 Woodrow Hartzog and Evan Selinger, Facial Recognition is the Perfect Tool for Oppression, August 2, 2018, Medium. https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66
Our own experience with surveillance mission creep in the United States cautions against allowing government agencies to build surveillance technology that gives officials these powers. Initially, police might say they will only use the technology for terrorism or other extreme events. But time and time again, technologies and powers granted to US government agencies for terrorism are later expanded and used for routine policing, for example in the war on drugs. Surveillance technology implementation and policy only move in one direction; once technologies are implemented, they are not withdrawn. The only way to protect the public interest from the kinds of abuses described above is to enact laws forbidding government agencies from building the architecture of face surveillance.

III. Face surveillance doesn’t work very well

Facial recognition technology can be inaccurate and racially discriminatory. But the problems researchers have identified with facial recognition image matching systems are magnified when the technology is used to surveil people in public. For example, in 2017, police in London attempted to identify people on a hotlist at a carnival, by using face surveillance algorithms to analyze real time video data. The system wrongfully identified people 98 percent of the time. Nearby, police in Wales reported similarly bad outcomes in a similar test: 91 percent failure. "On 31 occasions police followed up the system saying it had spotted people of concern," the Guardian reports of the test, "only to find they had in fact stopped innocent people and the identifications were false."

IV. Facial Recognition Poses Grave Constitutional Concerns

The use of facial recognition for surveillance raises grave constitutional concerns that can only be addressed by prohibiting its use.

First, dragnet biometric monitoring of individuals while they are exercising rights protected by the First Amendment would chill freedom of expression, freedom of speech, and exercise of religion.

Second, the technology poses a fundamental threat to our basic Fourth Amendment privacy rights and right to be left alone.

Law enforcement officials have argued that we have no privacy in public spaces, but the Supreme Court disagrees. In a historic ruling in Carpenter v. U.S., Chief Justice John Roberts held that new technologies enabling retroactive and real-time mass surveillance fundamentally change the balance of power between the government and the people. In that case, the Court ruled that law enforcement officials must get a warrant to obtain historical cell-site location data from phone companies. Eventually, courts may very well apply Carpenter’s reasoning to ubiquitous face tracking in public space. But that case was not decided until 2018, decades after Americans began to use cell phones. We cannot wait decades for the courts to rule on the constitutionality of facial recognition technology or other machine learning enabled remote biometric surveillance technologies. We must ban the use of this technology for this purpose now, before police buy and install dragnet surveillance infrastructure.

Third, we must distinguish facial recognition from even the most invasive tracking technologies that the courts have considered to date. Cell phone tracking is fundamentally different from facial recognition in at least two significant ways. First, you do not have to bring your phone with you if


27 Ibid.

28 Ibid.

you want to go somewhere anonymously—a political demonstration, a clinic, a bar, or a motel. But you cannot leave your face at home. Second, for a government official to access information from your phone, they must in most cases either possess the device itself or request access from a third-party service provider. In either case, they must obtain a warrant. But judicial authorization and oversight become substantially less effective tools to prevent misuse and abuse if a government agency acquires facial recognition technology and can use it in-house without going through any other gatekeeper. For this reason, legislative or executive intervention is imperative—before government acquisition and use of the technology becomes endemic.

For these reasons, legislatures and executive branch officials should prohibit police use of facial recognition for surveillance, and intervene to ensure the physical architecture for this kind of dragnet monitoring is never built.

**Part III – Affect recognition and other remote biometric monitoring tools**

Facial recognition is not the only machine learning enabled biometric technology that allows the government to use our features to monitor us without our knowledge or consent. Very limited studies exist to show how these technologies work. And none of them are promising.

*First*, automatic gender recognition, a subfield of face surveillance technology, regularly misgenders transgender and gender-nonconforming people.  

*Second*, algorithms that claim to identify how someone is feeling based on their facial expressions are unreliable and based on pseudoscience. For example, one study used so-called "affect recognition" software to analyze images of NBA players’ official portraits and found it more likely to classify Black players as angry and contemptuous despite smiling like their white counterparts. Moreover, research from leading scholar Dr. Lisa Barrett at Northeastern University has shown that it is simply not possible to reliably discern how someone feels based on the physical characteristics of their face.

Without law prohibiting its use, it is only a matter of time before companies try to sell this kind of snake-oil technology to police to use in interrogations, on our streets, and even in our schools. The government should prohibit police use of these untested, dangerous technologies.

**Conclusion**

Machine learning enabled biometric technologies pose grave risks to free and open societies, racial justice, and core civil rights and civil liberties. Short of banning its use entirely in policing, governments should tightly regulate police use of image matching, by centralizing its use and subject it to strict limitations and court oversight. But effective regulation is not applicable to face surveillance or affect recognition. These latter forms of facial recognition ought to be permanently prohibited in government.

---

30 Matthew Gault, Facial Recognition Software Regularly Misgenders Trans People, February 19, 2019, Vice.  

31 Lauren Rhue, Emotion-Reading Tech Fails The Racial Bias Test, The Conversation, January 3, 2019,  