THE JUSTICE COLLABORATIVE INSTITUTE

THE CASE FOR BANNING LAW ENFORCEMENT FROM USING FACIAL RECOGNITION TECHNOLOGY

Evan Selinger *(Professor of Philosophy, Rochester Institute of Technology)*
Woodrow Hartzog *(Professor of Law and Computer Science at Northeastern University)*

August 2020

EXECUTIVE SUMMARY

Police use of facial recognition technology has become routine in the United States, posing grave risks to privacy and civil liberties, especially for people of color. Despite its ubiquity, there is no comprehensive regulation of the technology and its use by law enforcement.

Thus far, some cities and states have reined in law enforcement use of the technology. Some private companies that have developed facial recognition software have paused their partnerships with police as a response to pressure from critics.

A federal law would be the most powerful step to regulate the use of this invasive and dangerous technology. The Facial Recognition and Biometric Technology Moratorium Act of 2020 was introduced in June in the Senate and House of Representatives by Senators Edward Markey and Jeff Merkeley and Representatives Pramila Jayapal and Ayanna Pressley. It would ban federal agencies' use of facial recognition technology (and other biometric technologies) and create incentives for local and state prohibitions.

INTRODUCTION

Facial recognition technology is the most dangerous surveillance tool ever invented. Law enforcement agencies have the ability to use facial recognition technology to identify, investigate, surveil, and arrest people. Advances in artificial intelligence, widespread video and photo surveillance, diminishing costs of storing big data sets in the cloud, and cheap access to sophisticated data analytics systems together make the use of algorithms to identify people perfectly suited to authoritarian and oppressive ends. Historically, government agencies in the United States have lacked anything close to such a powerful means of keeping tabs on citizens. Despite posing unprecedented threats to civil liberties, free expression, privacy, human rights, and democratic accountability, facial recognition technology is woefully underregulated. But the Black Lives Matter protests against systemic policing problems have become an inflection point for demanding immediate and dramatic change.

In recent years, there has been progress on the regulatory front at the local and state level. Policymakers in cities in California (San Francisco, Oakland, Berkeley, Alameda, and Santa Cruz), Massachusetts (Somerville, Brookline, Cambridge, Northampton, Springfield, Boston, and Easthampton), and Maine (Portland) have banned government agencies from using facial recognition technology. California, Oregon, and New Hampshire have moratoria in place, preventing law enforcement from using facial recognition and other biometric tracking technology in body cameras. This has happened despite claims from some that law enforcement cannot be prohibited since the "genie of facial recognition is not going back in the bottle."

There has been important but insufficient movement among private actors, in response to criticism. The Association for Computing Machinery (which has nearly 100,000 members) is calling for "an immediate suspension of the current and future private and governmental use of facial recognition technologies in all circumstances known or reasonably foreseeable to be prejudicial to established human and legal rights." And big technology companies are making public commitments: IBM is out of the facial recognition technology business; Amazon will not

sell facial recognition technology to the police for a year; and, Microsoft will refrain from selling facial recognition to the police "until there is a strong national law grounded in human rights." Yet other companies like Clearview AI remain undeterred, relishing the opportunity to pick up the surveillance slack.

The most important thing that's missing is an uncompromising national policy, but this could change. Democratic lawmakers (Ed Markey, Jeff Merkley, Pramila Jayapal, and Ayanna Pressley) are advocating for the *Facial Recognition and Biometric Moratorium Act of 2020*. The bold legislation deserves everyone's support. It prevents the federal government from using the technology and incentivizes state and local governments to follow suit.

THE LEGAL GAPS

Local, state, and federal police departments and immigration agencies in the United States have had access to information-rich databases that store details like names, demographic data, and license plate numbers for many years. However, a national ID–which would, by its nature, include a federal database of personal information, some of which might be biometric–has never been created.

Unfortunately, law enforcement agencies are on their way to creating an equally dangerous repository by availing themselves of information stored in a patchwork of databases, including ones that contain mugshots (even though not everyone who gets arrested gets convicted) and driver's license photos (which can be used without affirmative legislative approval informed by public debate). Technology companies are making things worse. For example, while Clearview AI didn't ask for people's consent, it still scraped the internet to create a name-face database containing three billion faces.

This consolidation is occurring because facial recognition technology is a textbook example of the speed of innovation outpacing the velocity of regulation. Even over the months of the COVID-19 pandemic, as widespread mask-wearing causes the error rates of facial recognition algorithms to reach anywhere from five to fifty percent, technology companies around the world have been trying to rapidly adapt, insisting on the technology's continued utility and effectiveness. And yet, Congress has not restricted how the government can use facial recognition technology. Meanwhile, the courts, which haven't meaningfully limited the government's use of it, remain either reluctant or ill-equipped to comprehensively do so.

In the absence of regulation, police can now take your picture and check it against a facial recognition technology database without your permission, judicial oversight, probable cause, or reasonable suspicion. This is true even if you are engaging in lawful activities, so long as you are in public or using the open internet. Such permissiveness extends far beyond the capacity to identify who is in a given image. It also frees law enforcement to use facial recognition technology to engage in ongoing, retrospective, and real-time face surveillance with few barriers by monitoring public places—remotely and automatically, with the push of a button.

In the United States "at least one out of four state or local police departments has the option to run face recognition searches through their or another agency's system," according to the Georgetown Center on Privacy and Technology. Why does law enforcement have such extensive legal latitude for using facial recognition technology? Why haven't federal rules been established that are comparable to the ones in place for conducting wiretaps? It's because the Fourth Amendment, which protects against unreasonable searches and seizures, hasn't historically covered what people willingly expose in public. Fortunately, the law has started

recognizing problems with this view. Justices in recent Supreme Court cases acknowledge that advances in surveillance technology, which make it incredibly easy and cheap to track people at scale, are challenging traditional conceptions of privacy. Most recently, in the majority opinion for the 2018 Supreme Court case, *Carpenter v. United States*, Chief Justice Roberts declared, "A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, 'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'"

To put the massive power of facial recognition technology and the regulatory gaps in perspective, it's helpful to clarify why it isn't just, as some allege, merely the new fingerprint technology. Since physical contact isn't required to take a photograph, and hiding your face is more suspicious than covering your hands in many circumstances, it is much easier to capture an image of a person's face than a fingerprint from far away and in bulk (group photos), with less resistance (because less physically intrusive), and through non-transparent means. Furthermore, there is more information available through facial recognition databases than ones with fingerprint information. For example, the Government Accountability Office states that the FBI can scan approximately 640 million pictures (mugshot, driver's license, and passport photos), but only has 145 million fingerprint records in its database. Finally, unlike fingerprints, which can only be used to establish personal identity, faces can be analyzed for additional information (e.g., emotions and demographics). If you want to know as much about someone as possible facial surveillance is the way to go.

THE HARMS

There are many ways that law enforcement can harm people by using facial recognition technology. Historically, government surveillance has disproportionately targeted marginalized communities and has been carried out "overwhelmingly on the shoulders of immigrants, heretics, people of color, the poor, and anyone else considered 'other.'" Without robust regulation, these communities have good reason to be concerned that history will repeat itself—that they will be excessively surveilled even while engaging in law-abiding conduct, and that some of the interactions could result in verbal abuse and physical violence, in addition to the risk of wrongful arrests.

This concern is exacerbated by the lack of transparency surrounding law enforcement's use of the technology and the fact that while facial recognition systems are improving, inaccuracies remain. Even though their use can result in false positives or negatives that make everyone vulnerable to unjust stops, searches, and arrests, the most likely errors will, as Joy Buolamwini, Timnit Gebru, and Deb Raji have long cautioned, result in discriminatory outcomes. That's because the technology displays the greatest biases against women and people of color.

Additional errors can result from poor standards governing how law enforcement can use the technology. For example, if the police are given photos of suspects who have their eyes closed or only have parts of their faces visible, they might be tempted to model the missing detail with proxy information that distorts the results. Misleading proxy images also can find their way into investigations if law enforcement lacks a photo of a suspect and uses one that resembles eye witness accounts—as was the case when an image of the celebrity Woody Harrelson served that role.

Biases and errors can lead to severe harm, even death. As Georgetown University researcher Clare Garvie aptly states:

"What happens if a system like this gets it wrong? A mistake by a video-based surveillance system may mean an innocent person is followed, investigated, and maybe even arrested and charged for a crime he or she didn't commit. A mistake by a face-scanning surveillance system on a body camera could be lethal. An officer alerted to a potential threat to public safety or to himself, must, in an instant, decide whether to draw his weapon. A false alert places an innocent person in those crosshairs."

Additionally, as Jay Stanley, Senior Policy Analyst at the ACLU, rightly notes, problems with facial recognition and facial characterization are closely linked: "...a 'smart' body camera falsely telling a police officer that someone is hostile and full of anger could contribute to an unnecessary shooting."

Facial recognition software has already contributed to serious cases of mistaken identity. A Brown University student and Muslim activist was erroneously identified as a bombing suspect in 2019. In January 2020, the Detroit police wrongfully arrested Robert Williams for robbery in front of his wife and young daughters and locked him up for almost 30 hours. This was months after they had wrongfully arrested Michael Oliver on a felony count of larceny.

But even if, hypothetically, facial recognition technology became 100 percent accurate problems would remain. In fact, accurate facial recognition might even be more dangerous because those in power will find it irresistible and they'll want to use it more often.

The mere prospect of additional facial surveillance can have a chilling effect, discouraging citizens from engaging in First Amendment-protected activities, such as free association and free expression (from protesting to worshipping), for fear of ending up on government watchlists. Not too long ago the police reportedly used facial recognition to locate and arrest people who protested the death of Freddy Grey while in police custody. Recently, Mr. Williams strikingly declared: "Even if this technology does become accurate…I don't want my daughters' faces to be part of some government database. I don't want cops showing at their door because they were recorded at a protest the government didn't like." These are especially harrowing words given brutal police responses to Black Lives Matter protestors and the fact that not enough journalists or protestors realize it is prudent to presume that law enforcement could use facial recognition technology on any image associated with these events.

It's also reasonable to expect that due process ideals will be weakened by continued use of facial recognition technology. Through a technologically-induced shift, citizens could stop being presumed innocent and, instead, become coded as risk profiles with varying potential to commit crimes. Should this happen, the government will find it too easy to excessively police minor infractions as pretexts to cover up more invasive motives and secretly monitor gadflies, like journalists and whistleblowers. The net result would be anxious and oppressed citizens who are denied fundamental opportunities and rights.

SOLUTION

Cities and states have taken the lead in banning facial recognition technology so far. The Facial Recognition and Biometric Technology Moratorium Act of 2020, introduced in June by Senators Edward Markey and Jeff Merkeley and

Representatives Pramila Jayapal and Ayanna Pressley, would build on these bans and serve two important purposes. First, it would ban federal agencies' use of facial recognition technology and other biometric technologies. The ban would apply to Immigration and Customs Enforcement, the Drug Enforcement Administration, the Federal Bureau of Investigation, and Customs and Border Patrol. Second, it would, by withholding some federal funding from state and local law enforcement that fail to enact moratoria on the use of these technologies, create incentives for the local and state bans that have otherwise been slow to come. The legislation is supported by an array of civil liberties and racial justice organizations, including the ACLU, Electronic Frontier Foundation, Fight for the Future, Color of Change, Project on Government Oversight, and New America's Open Technology Institute.

CONCLUSION

There is no future in which we are, on whole, better off with facial recognition technology. It is a fundamentally corrosive tool. Law enforcement should be banned from using facial recognition technology outright. Supporting the Facial Recognition and Biometric Technology Moratorium Act of 2020 is the best approach for preventing an Orwellian future and ensuring that the United States is committed to protecting everyone's constitutional rights and liberties.

COVER PHOTO
iStockPhoto