The New York Times | https://nyti.ms/2q59HnA

Here's a Way Forward on Facial Recognition

The police should be able to use it, but in a very limited way.

By Barry Friedman and Andrew Guthrie Ferguson
The authors are law professors.

Oct. 31, 2019

A furious debate is underway over the use of facial recognition technology for law enforcement purposes. San Francisco and a few other communities have banned their police departments from using it. Detroit is among other cities wrestling with the question. At the same time, law enforcement agencies say that software that analyzes human faces to identify them is essential for effective policing.

The debate over the technology took on added urgency in the summer when the Georgetown Law's Center on Privacy and Technology disclosed that Immigration and Customs Enforcement officials had mined state driver's license databases, using facial recognition technology to analyze millions of motorists' photos without their knowledge. The F.B.I. also has run thousands of searches through these state databases.

To our minds, there's pretty much *everything* wrong with this. Federal agencies have no clear democratic mandate nor any explicit legislative authority to use facial recognition. And this sort of data mining usually is done without a warrant. Society has yet to come to terms with this kind of invasion of privacy. As Senator Patrick J. Leahy, Democrat of Vermont, put it, "Americans don't expect — and certainly don't consent — to be surveilled just because they get a license or ID card."

What's more, tests show facial recognition is less accurate for darker-skinned people, and for women — leading to them more easily being caught in the dragnet of wrongful enforcement. Law enforcement is apparently using this powerful tool for offenses as trivial as petty theft or cashing a stolen check.

[If you're online — and, well, you are — chances are someone is using your information. We'll tell you what you can do about it. Sign up for our limited-run newsletter.]

It's no surprise, then, that Congress has been holding hearings about whether to ban or regulate the technology. We believe there is a way forward that can address the serious privacy concerns while also acknowledging the argument made recently by James P. O'Neill, New York City's police commissioner, in an Op-Ed article in The Times, that "it would be an injustice to the people we serve if we policed our 21st-century city without using 21st-century technology."

The solution is to distinguish between two very different uses of facial recognition technology, banning one and allowing but tightly regulating the other.

We should ban "face surveillance," the use of facial recognition (in real time or from stored footage) to track people as they pass by public or private surveillance cameras, allowing their whereabouts to be traced.

On the other hand, we should allow "face identification"— again, with strict rules — so the police can use facial recognition technology to identify a criminal suspect caught on camera.

With cameras so pervasive on street poles and buildings, widespread face surveillance would be Big Brother come to life, allowing for the tracking of our every movement and the stitching together of intimate portraits of our lives. Yes, banning it could cost the police the ability to nab a dangerous fugitive on the run. But allowing it could lead to the mass surveillance that China is deploying. Most Americans aren't going to be comfortable with that, nor should they be.

Law enforcement should not have a problem with banning facial surveillance. In his essay in The Times, Commissioner O'Neill did not argue for face surveillance. And the official who heads the F.B.I.'s information services branch, Kimberly del Greco, has said, "We do not perform real-time surveillance." The Chicago and Detroit police departments acquired the technology to conduct face surveillance, but after objections from the public, said they would not use it.

Let's settle this now and adopt a ban on face surveillance.

On the other hand, face identification counsels a different response. Police officers face a laborious and often fruitless task when they try to match photos of crime suspects to mug shots of people who have already been arrested. Why not use facial recognition technology to assist law enforcement in this effort?

We think legislatures should allow but tightly regulate face identification. We would impose five requirements.

First, face identification should not be deployed at all until it can recognize the faces of all races and genders equally effectively. There's enough racial bias in the criminal justice system without technology making matters worse. This can and will get solved, but until then we ought to declare a pause.

Second, face identification should be available to law enforcement only for the most serious of crimes, like murder, rape, robbery and aggravated assault. No more sniffing through motor vehicle department databases for unlawful immigrants, as I.C.E. has done, or chasing down petty criminals. The country already has overcrowded jails; too many people — disproportionately people of color — are dragged into the criminal justice system. Unless we limit the use of face identification to the most serious offenses, we will worsen this problem.

Third, and perhaps counterintuitively, use of facial recognition technology should not be limited to criminal databases. Commissioner O'Neill sought to reassure readers that his department was using only arrestee databases for searches, not motor vehicle photos. Even some civil liberties advocates assume "mug shot" databases are less problematic than databases of innocent people.

But this is exactly backward. Mug shot databases are the product of decades of discriminatory policing for offenses like drug crimes; using those will continue us on this course. To catch the people who commit serious offenses, the police should search a database that includes all our faces.

Fourth, face identification should not be allowed without a judicial warrant. Without judicial supervision, we can't be sure face identification is used only as permitted.

Finally, any law allowing face identification ought to come with penalties for misuse. Courts and legislatures constantly set up guardrails for law enforcement, but fail to impose penalties for violations. Officials and departments should face serious consequences if they fail to follow the rules.

This proposal isn't going to please everyone. But as we read the debates over the last months, this is a place where compromise might work. It allows law enforcement use of facial recognition where it makes sense, with serious protections against spillover and misuse.

Barry Friedman is professor and director of the Policing Project at New York University School of Law and the author of "Unwarranted: Policing Without Permission." Andrew Guthrie Ferguson is a professor at the David A. Clarke School of Law at University of the District of Columbia, a fellow at the Policing Project and the author of "The Rise of Big Data Policing."