Unlimited law enforcement application of facial recognition software to surveillance footage is an unreasonable search and a violation of Constitutional rights for people in a peaceful crowd. An officer should need to demonstrate probable cause that the investigated face on camera is a criminal in order to receive official permission to identify a face in a crowd with artificial intelligence.

This should not be controversial.

I wrote that we are swimming in a sea of digital surveillance cameras and that police should be required to secure a warrant before running facial recognition software on a public crowd – particularly a crowd assembled for political protest. I believe this approach is practical for law enforcement, protective of our First and Fourth Amendment rights, and consistent with the current U.S. Supreme Court’s decisions on how to limit police access to information only available due to rapidly improving technology.
And I am not alone in this belief. In November of last year, U.S. Senators Coons and Lee introduced bi-partisan legislation requiring federal law enforcement to obtain a court order before using facial recognition technology. This law provides a logical framework for protecting Americans from a powerful new state-operated technology that has grown unchecked as a tool for intruding on citizens’ privacy.

Obtaining a warrant is practical for law enforcement. This is the system all of our policing agencies use when they want to go somewhere or do something that might otherwise intrude on the Fourth Amendment right to be secure in our persons, homes and papers. The officer simply needs to show that she has a reasonable suspicion that a person has committed a crime, and then the officer is issued a warrant that allows intrusion on private spaces and information.

This keeps our police force from just searching everyone and everything hoping to find something to arrest someone for. That’s why the protection was written into the Constitution by our nation’s founders. It is supposed to slow the process down so that someone can think about whether the one group in society with a legal monopoly on violence should be pushing down your front door and rifling through your underwear drawer.

Police already have the right forms to fill out. They know how the process works. Judges are addressing these matters all the time. In other words, the only extra time required will be the extra time that police are supposed to take when they intrude on a person’s privacy.

Nothing lost from how law enforcement is supposed to be operating.

And requiring a warrant for police to run facial recognition software would protect our Constitutional rights. Let’s say that a crowd was lawfully demonstrating against the police force itself – this could be because the police are enforcing restrictive gun laws or because the police have misbehaved in some way. Every color of the political spectrum is affected by this concern. Would demonstrators feel violated if law enforcement used its multiple surveillance cameras to capture their activity? Maybe, but they are likely to expect to be seen by cameras. Would they feel violated if police ran an artificial intelligence program over the camera footage to take down the names of all people who demonstrated against them? You bet.

As a judge for the Seventh Circuit Court of Appeals pointed out in language quoted by the U.S. Supreme Court, “Awareness that the Government may be watching chills associational and expressive freedoms. And the Government’s unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by 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.”

Seventh Circuit Judge Flaum was writing in 2011 about tracking a person’s body around town everywhere it goes. The same logic also applies to technology that allows police to not only see all the people in a given space at any particular time, but to apply names to all the faces that appear there.
We can’t just bury our heads and pretend that the new technologies aren’t affecting the relationship between police and citizens. Even self-claimed originalist Justice Scalia has written, “Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice.” Because, in an “Originalist greatest hit” that may help in my argument, Scalia wrote, “We must assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.” In other words, if the technology allows law enforcement to intrude deeply into our lives in new ways that would have been unconsidered two hundred and fifty years ago, it must be checked by the Fourth Amendment – requiring police to obtain a warrant before using the intrusive tech.

When we operate in this manner, if you are caught on camera throwing a Molotov cocktail through the plate glass window of a local business, the police can clearly and easily use a facial recognition program to find you and bring you to justice. But, under my rule as supported by Senators Coon and Lee and Justice Scalia, if you are simply walking in a peaceful political demonstration the police would not be allowed to run facial recognition software to place you in the crowd at that time. They can run the program now under no limitations.

Finally, requiring a warrant to use this powerful tech is not an outlandish request and it may even be required soon by this U.S. Supreme Court as currently constituted. The Court has already begun to move toward this conclusion, and has started to insist on Fourth Amendment protections for transformative technologies, requiring for example that police need a warrant to place a thirty-day tracking beacon on your personal vehicle and that police need a warrant to open and review the contents of your smart phone. SCOTUS even changed their previous rule that information held by a third party was not protectable in this manner when they recently held that police need a warrant to request the past month’s worth of cell phone tracking records to pinpoint your location at different times in the past.

Seventy years ago the Supreme Court held that keeping your name from being associated with your political causes was a part of your right to free speech and free association. You may have reason to fear the government taking note of your association, which is why that particular Supreme Court decided that the State of Alabama in the 1950s was not allowed to require a list of all local NAACP members. The unfettered technology to see who is entering gay bars, gun clubs, and political protests, and then to identify each individual, allows the government to invade and chill people’s speech and assembly rights.

This concern for privacy even in public places is echoed by our current Chief Justice, writing, “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. In the past, attempts to reconstruct a person’s movements were limited by a dearth of records and the frailties of recollection. . . [With current technology] police need not even know in advance whether they want to follow a particular individual, or when.”

So the court has recognized that attending politically sensitive meetings anonymously is an important right covered by the First Amendment, and that limited technological intrusions on privacy is an important value of the Fourth Amendment.
So it seems well within the court’s present mindset to limit the government’s use of overly intrusive technology, like running facial recognition systems on people in the public sphere without specific law enforcement reason to do so.

Chief Justice Roberts notes recently, harkening back to one of the first important privacy opinions written in 1928, “As Justice Brandeis explained in his famous dissent, the Court is obligated—as “[s]ubtler and more far-reaching means of invading privacy have become available to the Government”—to ensure that the “progress of science” does not erode Fourth Amendment protections. Here the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers, “after consulting the lessons of history,” drafted the Fourth Amendment to prevent.” [citations omitted]

And when will the technology rise to level that a warrant is required? The court, in the recent Kylo decision, held that “a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.” If peaceful political protesters subjectively fear being named to police during political gathering, their concern certainly seems reasonable to me.

“I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of [new technology] through lawful conventional surveillance techniques.” Writes Justice Sotomayor. She continues, “I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment’s goal to curb arbitrary exercises of police power to and prevent “a too permeating police surveillance.”

I know that the best choice in this circumstance is for Congress or multiple state legislatures to place limits on policing power by requiring warrants to run biometric ID software. Several Justices agree, as they joined Justice Alito in his sentiment, “In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. . . In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.”

So forward this to your legislators – or relevant portions of it, as many people don’t like to read long discussions. Make the argument that we would all be better off by limiting the police from using powerful identification technology without a reasonable suspicion that the person on camera has committed a crime. Don’t wait for the off chance that a suitable case rises to the Supreme Court within the next five years. We need the protection now.

Copyright © 2020 Womble Bond Dickinson (US) LLP All Rights Reserved.
Source URL: https://www.natlawreview.com/article/constitution-protects-faces-crowd