Keep Facial Recognition Away From Body Cameras

Matthew Feeney

April 22, 2018

The Chinese tech giant Alibaba recently invested $600 million in a start-up that specializes in facial and object recognition. Thanks to the investment the start-up, SenseTime, is now the world's most valuable artificial intelligence start-up.

Although such technology undoubtedly has potential when it comes to picking up your morning coffee and easing congestion at metro ticket lines, it has been making news in China because it is playing an increasingly prevalent role in that country's growing surveillance state. While the Chinese are leaders in surveillance technology innovation, we should keep in mind that facial recognition in the U.S. also poses a unique and significant threat to privacy, and it's a threat that is not being adequately addressed.

Facial recognition fits in the family tree of biometric investigatory technologies, which determine identity via analysis of unique biological and physical traits. Many are familiar to anyone who watches CSI shows or other fictional portrayals of law enforcement: fingerprint and DNA analysis are a couple of examples.

If law enforcement has access to your fingerprints it's likely because you volunteered them as part of a job requirement, you're an immigrant, they were recorded after you were arrested, or they were collected at a crime scene. About 40 percent of fingerprints in the FBI's fingerprint database are not related to arrests or forensic investigations. The FBI's DNA database only includes DNA related to criminal arrests or forensic investigations.

Unlike databases for fingerprints and DNA, one of the FBI's facial recognition services allows agents to search through databases that mostly include information related to law-abiding Americans, with only 8 percent of the facial images in the network being associated with criminal or forensic investigations. This is in part thanks to the fact that the FBI has access to drivers license photos from at least 16 states as well as passport photos from the State Department. All told, this Facial Analysis Comparison and Evaluation services allows the FBI to access more than 411 million facial images. A Georgetown study on facial recognition estimates that about half of American adults can be found in a law enforcement facial recognition network.

This is especially concerning because facial recognition can be used to conduct surveillance. It's already being used for the purpose in China, and here in the U.S. the law enforcement community seems poised to spread the use of facial recognition without sufficient limitations in place.

At the federal level, the Department of Homeland Security (DHS) has been especially keen to use facial recognition, where the technology is sought for small border dronesand used to verify

airport travelers' identities. The use of facial recognition at airports is especially controversial because Congress never authorized DHS to collect and analyze American citizens' facial images. Nevertheless, DHS is subjecting American citizens to face scanning at select airports across the country.

While hardly ubiquitous among states and local law enforcement, facial recognition looks set to become a common feature of policing. Body cameras outfitted with real-time facial recognition capability are set for deployment this fall, and some police departments, such as the New York City Police Department, already use facial recognition tools to review surveillance footage. The Los Angeles Police Department also has a history of using facial recognition tools.

Police officers with real-time facial recognition capability will dramatically change law enforcement, especially if their facial recognition tools are linked to databases that are mostly made up of law-abiding Americans' face images.

Even if facial recognition on police body cameras was only able to identify people with outstanding warrants there would still be issues. In 2015, the Department of Justice's Civil Rights Division issued its report on the Ferguson, Missouri, police department. The report noted that police officers in Ferguson were regularly cracking down on minor infractions, putting many residents in dire financial straits.

Ferguson is hardly the only city city where warrants are issued for failing to pay fees. A 2014 NPR report on unpaid court fees and fines noted that many of New York City's 1.2 million outstanding warrants were for unpaid court fines and fees. The same NPR article reported that in 2011 courts in Philadelphia sent bills to about one in five of the city's residents.

Police pursuing these fees can lead to the worsening of police-community relations, as shown by the following anecdote from the DOJ Ferguson report, which its authors state reflected the treatment many African Americans "have come to expect from Ferguson police."

An African-American man recounted to us an experience he had while sitting at a bus stop near Canfield Drive. According to the man, an FPD patrol car abruptly pulled up in front of him. The officer inside, a patrol lieutenant, rolled down his window and addressed the man:

Lieutenant: Get over here.

Bus Patron: Me?

Lieutenant: Get the f*** over here. Yeah, you.

Bus Patron: Why? What did I do?

Lieutenant: Give me your ID.

Bus Patron: Why?

Lieutenant: Stop being a smart ass and give me your ID.

The lieutenant ran the man's name for warrants. Finding none, he returned the ID and said, "get the hell out of my face."

Had the police officer been wearing a body camera with real-time facial recognition capability he would perhaps have passed this man by, but other residents with outstanding warrants for minor

infractions or small fines would have to fear a similarly unprofessional and confrontational encounter. It doesn't take a great imagination to speculate about how disastrous real-time police body cameras would be for police-community relations in a city where a sizable portion of the population have outstanding fines or warrants for non-violent and non-property crimes.

Lawmakers could propose a policy of linking police body cameras with real-time facial recognition capability to databases that only include suspects wanted for violent or property crimes. However, this is a slippery slope that we should avoid altogether.

Such a policy would quickly become target for amendment. In the wake of a sex offense policymakers who backed this policy would eventually be asked, "Why didn't the database include the sex offender registry?" In some jurisdictions lawmakers would face pressure to include vast and error-prone gang databases in real-time facial recognition networks. Once a facial recognition database is built there will be continued pressure from lawmakers law enforcement officials for more images to be added.

Facial recognition poses a unique threat to law-abiding American citizens, millions of whom are in facial recognition networks merely because they drive. Lawmakers can prevent increased risk of surveillance by forbidding real-time facial recognition on police body cameras. With such devices, police won't need a "Papers, please" law to identify citizens going about their business; our faces will be our papers.

Matthew Feeney is a policy analyst at the Cato Institute, where he works on issues concerning the intersection of new technologies and civil liberties.