MarketWatch

Opinion: Giving TSA facial-recognition software isn't worth a faster security line

Matthew Feeney

September 24, 2018

Earlier this month, officials at Washington Dulles International Airport unveiled a facial-recognition system designed to replace boarding passes. Travelers who loathe the long lines and waiting associated with airports may applaud the move; the scans take less than a second.

Yet we shouldn't be so quick to welcome timesaving face scanners. Facial-recognition technology poses a unique surveillance threat and is being deployed without adequate privacy protections. It should be kept far away from airports.

While certainly a member of the biometric family, facial recognition is very different from other biometric technology (DNA, fingerprints, etc.) in two important ways.

First, law enforcement can only collect DNA and fingerprints if that information has been volunteered or collected as part of an investigation. According to a 2016 study by the Center on Privacy & Technology at Georgetown Law, the Federal Bureau of Investigation's DNA database only includes DNA related to arrests and investigations. About 60% of the FBI's fingerprint database includes those associated with criminal or forensic investigations, with many of the remaining prints being volunteered by immigrants and those who have a job requiring fingerprints. Thanks to the FBI's access to passport photos and numerous states' driver's license databases, at least 80% of the images in the FBI's Facial Analysis, Comparison, and Evaluation Services Unit are not related to criminal or forensic investigations.

Second, unlike DNA and fingerprint tools, facial-recognition technology measures something that most people cannot hide in their day-to-day lives. Most of us happily go about our days unconcerned about law enforcement collecting and analyzing our fingerprints and DNA. It's true that you could seek to avoid facial recognition by wearing masks, but such behavior is likely to draw unwanted attention and incur a social cost.

When it comes to air travel, biometric collection is becoming harder to avoid. In a Privacy Impact Assessment issued last year, the Department of Homeland Security, Customs and Border Protection's parent agency, bluntly stated, "the only way for an individual to ensure he or she is not subject to collection of biometric information when traveling internationally is to refrain from traveling."

Officials say that law-abiding travelers need not worry. According to John Wagner, CBP assistant commissioner for the Office of Field Operations, once the system is fully implemented, the agency will delete the facial images of U.S. citizens almost immediately after identity verification.

This may sound reassuring, and facial recognition is already becoming commonplace in the private sectors thanks to companies such as AppleAAPL, +1.01% and VIQ Solutions VQS, -3.45% but we should keep in mind that CBP's facial recognition is operating in a relatively unregulated field, and this policy could change suddenly.

In the wake of a terrorist attack or other violent incident, we should expect CBP to collect and share more data, including facial images, with other law enforcement agencies. As the Electronic Privacy Information Center's Jeramie D. Scott nicely put it, "there is very little [CBP] could do at this point that would clearly violate any privacy-protecting law."

For now, American citizens have the option to opt out of CBP's facial scans. Foreigners aren't so lucky. And CBP is testing biometric technology at 15 airports across the country. We should expect the technology to appear at more airports in the near future.

Unfortunately, the latest news is only the latest example of CBP's enthusiasm for facial recognition, with small drones outfitted with facial recognition tools being included in a CBP solicitation reported last year.

CBP's enthusiasm for facial recognition is hardly unique. Law enforcement agencies across the country at the local and state level are using facial recognition technology. Whether it's large departments such as the New York City Police Department and the Los Angeles Police Department, state departments such as Michigan and Virginia state police, or smaller departments like the Washington County, Oregon, sheriff's department, law enforcement is acquiring and using facial-recognition tools.

Without restrictions in place, facial recognition could be merged with body cameras, posing even more risks to our privacy.

The widespread use of facial recognition technology may cut down on time spent in lines, but — absent restrictions — it could also be used to allow the government to identify law-abiding Americans engaged in constitutional activities, such as protests and gun shows, thereby stifling attendance at these lawful gatherings.

Some might argue that "if I've done nothing wrong, I have nothing to hide." Those making this kind of argument should take a look at the history of American government surveillance. The list of surveillance targets is long and diverse. At the moment, Islamic extremists are one of the main targets of government surveillance. No one knows for sure who the focus of government surveillance will be in the next few years. What we do know is that government officials will conduct this surveillance with the most intrusive tools in their toolkit. Accordingly, it's worth taking steps to limit data we volunteer to the government, including facial images.

It's understandable that many people are willing to submit to a facial scan if it means cutting down on time spent waiting in lines. Yet we shouldn't be so quick to sacrifice our privacy on the altar of convenience. Congress has been asleep at the wheel when it comes to facial recognition — not to mention almost everything else — and the use of this technology without strict restrictions on data sharing and retention is too great a risk to take in exchange for faster airplane boarding.

Matthew Feeney is the director of Cato's Project on Emerging Technologies. Follow him on Twitter @M_feeney.