OPINION | INSIDE VIEW

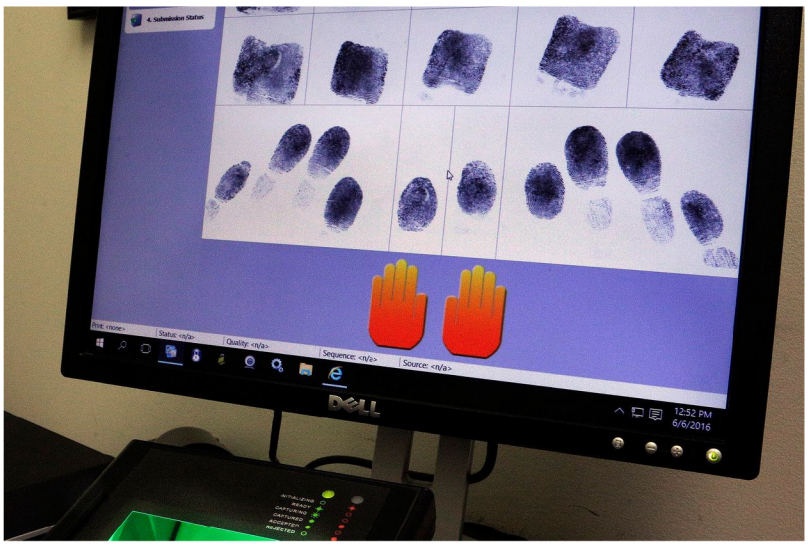
Have No Fear of Facial Recognition

If it is bound by good legal protections, the technology is a boon, not a tool for tyranny.

By

Andy Kessler

Aug. 4, 2019 5:51 pm ET



Fingerprints are compared digitally in Springfield, Ill., June 6. PHOTO: SETH PERLMAN/ASSOCIATED PRESS

Englishman Francis Galton first noted the unique arches, loops and whorls in our fingerprints back in the 1880s. Thirty years later, Clarence Hiller confronted an intruder in his Chicago home and was fatally shot. The culprit fled, but not before leaving a fingerprint in fresh paint on a railing. Thomas Jennings became the first defendant convicted using fingerprints as evidence. This is now routine, but back then there was public hysteria over the fingerprint's invasion of privacy and then questionable accuracy.

Today, with faces matched almost instantly via machine learning and artificial intelligence, fears of Big Brother have created similar hysteria—especially after Georgetown legal scholars

discovered last month that Immigration and Customs Enforcement has access to driver's license photos from 21 states.

So much so that the crime-ridden cities of San Francisco and Oakland, Calif., along with Somerville, Mass., have banned the use of facial recognition by law enforcement, even though local businesses can use it to track who enters and leaves their buildings. Pretty crazy.

Paranoid? Is someone watching you? Let's get some constitutional rights out of the way first, especially "unreasonable searches and seizures." In *Katz v. U.S.* (1967), the Federal Bureau of Investigation used an electronic eavesdropping device, attached to the outside of a phone booth, to record the defendant's gambling transactions. Charles Katz won and the Supreme Court ruled that in a phone booth, "like a home, and unlike a field, a person has a constitutionally protected reasonable expectation of privacy." On the flip side, the justices held that "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."

But we are still protected against dragnets (dum du dum dum)—the use of cameras or other surveillance to track collectively where everyone goes and what they do. Even in public, where you have no reasonable expectation of privacy, law enforcement can't record everything in hope that someone commits a crime. The USA Patriot Act weakened some of these protections, but the 2015 USA Freedom Act fixed that.

There's added hysteria around the potential bias in facial recognition's mistakes. About a year ago, the American Civil Liberties Union did a study, using Amazon's Rekognition tool, in which it ran photos of members of Congress against a database of 25,000 arrest mug shots. It falsely matched 28 congressmen, 40% of whom were "people of color." The headlines blared: "Facial recognition's racial bias problem."

But if you read the fine print, the ACLU admits that it "used the default match settings that Amazon sets for Rekognition," which is an 80% confidence level. Amazon reran the study with 30 times as many mug shots and the 99% confidence threshold they recommend for law enforcement use and the "misidentification rate dropped to zero." You probably missed the media's retractions.

To see if this technology is any good, I spoke to someone who actually uses it, Capt. Chuck Cohen of the Indiana State Police. He reminisced about the bad old days of passing around grainy videotapes from security cameras asking if "anyone recognized this guy." He tells me facial recognition is another tool in the forensic shed, along with fingerprints, tire imprints, partial license plates and DNA. He stressed repeatedly that he doesn't consider facial recognition as evidence in court, only as a lead in investigations.

Capt. Cohen says it works. During a physical altercation, someone was shot in the stomach and the victim's friend recorded phone video. Facial recognition identified the shooter, which was the lead police needed to find more evidence to nab the suspect. In another disturbing case, with explicit video, someone sexually harassed and extorted young girls. Police used facial recognition to identify 14 of 22 victims, who were carefully interviewed. They eventually identified the offender.

Hundreds of crimes have been solved. From other sources, I've heard that Alabama security cameras picked up a 90-year-old woman being robbed and beaten by an African-American woman. Police considered lineups, the proverbial usual suspects. Instead they used facial recognition and found the man who did it. You read that right: The culprit was a cross-dressing man, something a lineup would never have found.

The Chinese have powerful facial-recognition tools, SenseTime and Megvii. We know Beijing uses technology for mass surveillance, especially against the Muslim Uighurs. How do we safeguard U.S. citizens against similar abuses? Rather than banning its use, we need strong silos. Such protections exist today. Try getting President Trump's tax returns. Try finding the guy who cut you off with a license-plate number. Cops can't do extended surveillance without a judge's warrant. We can make databases inaccessible except with a judge's consent. Heck, use the judge's face as the ID.

Facial recognition will only get better. But we ought to can the hysteria. So long as the tech is properly limited in use to avoid fishing expeditions, we'll all be safer.