The Future Of Surveillance Is About Behaviors, Not Faces

With lack of regulations and legislation, ubiquitous surveillance is way beyond simple biometric identification and is now focussing on behaviors, including pre-crime analysis. Facial expressions, eye movements, gait, respiration, etc., are fed to AI algorithms to sense mood, personality and emotions. TN Editor

In 1787, English philosopher Jeremy Bentham came up with an idea for a prison that would cost a fraction of the cost of other contemporary jails to run with virtually no internal crime. His theoretical prison, the panopticon, was curved, the cells facing inward toward a center point where a guard tower would stand. The windows in the guard tower were to be darkened on one side. This way, a single guard would be able to observe the behavior of all the prisoners. But more importantly, the prisoners would never know whether the guard had his or her gaze trained on them. The end result, every individual within the prison internalizes a sense of being watched all the time and behaves accordingly.

This idea of the panopticon has become a stand-in for the threat of

ubiquitous surveillance, due mostly to Bentham's choice of setting — a prison. But Bentham aimed not to frighten people, but to furnish a way to manage a scarce resource: the attention of law enforcement.

A new trend in video surveillance technology is turning Bentham's panopticon into reality, but not in the way he imagined. Instead of a prison, the new panopticon would focus the attention of law enforcement on a person when her behavior becomes relevant to the guard tower. Imagine it were possible to recognize not the faces of people who had already committed crimes, but the behaviors indicating a crime that was about to occur.

Multiple vendors and startups attending ISC West, a recent security technology conference in Las Vegas, sought to serve a growing market for surveillance equipment and software that can find concealed guns, read license plates and other indicators of identity, and even decode human behavior.

A company called ZeroEyes out of Philadelphia markets a system to police departments that can detect when a person is entering a given facility carrying a gun. It integrates with any number of closed-circuit surveillance systems. But machine learning algorithms don't just come out of a box knowing how to recognize a firearm any more than a drug dog arrives from the breeder knowing the difference between marijuana and oregano. To teach the algorithm, a team from the company shows up on location and proceeds to stage mock attacks. Slowly, the algorithm begins to learn what a gun looks like in that specific setting, depending on light, angles, and other conditions. They're currently working with New York City Schools and have a contract with U.S. Customs and Border Patrol, but are not yet deployed to the border, said Kenny Gregory, a software engineer at the company.

Automated firearm detection is one solution to a growing problem that has no clear policy cure: curbing mass shootings and gun violence. While some polls show that 70 percent of Americans support stricter gun laws, that number is far lower, about 31 percent, among conservatives. And so the political debate, while fiery, has stalled. Gun-detection algorithms that alert security personnel when an armed person arrives might

reduce the number of victims — though likely not as much as if there were no armed shooter in the first place.

It’s a predictive indicator of potential violence, rather than a lagging indicator, such as facial recognition, and carries less political baggage. More and more, cities and police departments are experimenting with facial recognition to detect the presence of suspects in real time. They’re meeting with stiff resistance from privacy advocates in San Francisco, where some lawmakers are looking to block deployment, and elsewhere.

Read full story here…