Hollywood, Surveillance Technology, and Privacy Concerns

Trenton Abrego

July 8, 2019

WASHINGTON—On a night in 1998, an engineer from Lawrence Livermore National Laboratory and his wife went to the movie theater and watched Will Smith star in *Enemy of the State*, a film that features wide-area surveillance systems.

"Where everyone else in the audience was no doubt terrified by what they saw on the screen, he was absolutely thrilled," said Arthur Holland Michel, author of *Eyes in the Sky: The Secret Rise of Gorgon Stare and How It Will Watch Us All*, at a CATO Institute discussion June 25. "He thought it was amazing he thought 'we should do this,' and so he rushed home and left a message with his supervisor saying something very simple: 'I have a great idea, call me.'"

The movie sparked a transformation of how surveillance works around the world today.

After the engineers at the Lawrence Livermore National Laborator had put together rough versions of the surveillance, the CIA got involved.

"They became very interested because they could use it to unravel networks and insurgents in Iraq where these networks were really wreaking havoc on U.S. service members with ambushes and IED attacks," Michel said.

The CIA isn't the only government organization that has shown interest in the surveillance programs.

"[The] FBI and Department of Homeland Security have taken a great interest in it," Michel said.

Use in Warfare

Overseas, the technology has been implemented in conflict—most notably in Afghanistan. According to Michel, a wide-area surveillance satellite was "credited with the capture or killing of 1,200 people in Afghanistan." And he added that developmental programs using wide-area surveillance technology are still underway with the United States military.

"The Army has new programs to develop similar capabilities; so does the Marine Corps," he added. "The Air Force has continually developed more in this technology."

The technology has also been used in cases of counter narcotics.

“That had nothing to do with what the CIA initially intended for the technology,” Michel said. “But, once it’s there in battle, those checks don’t apply.”

Use in America

Wide-area surveillance has also been implemented domestically.

Most notably, in 2016 Baltimore citizens were being surveilled without their knowledge.

“They did everything they could—Baltimore PD—to keep the use of that system absolutely secret.” Michel said. “They didn’t want the public to know about it. City officials maintain to this day that they had no knowledge of it.”

The reason city officials and the public were unaware was because the surveillance was privately funded.

“There was a Texas billionaire philanthropist by the name of John Arnold who actually gave the city enough money to run the program,” Michel said.

It’s also expected that the technology will be rolled out in both Chicago and St. Louis.

Not only can the use be for legality and criminal issues. The use of wide-area surveillance use could improve global positioning systems, such as Google Maps.

“The technology can be used to identify chokepoints in real time; it can be used to gather data to create traffic models to figure out how to best optimize the flow of traffic for a city, how to space and time traffic lights,” Michel said.

Is it Legal?

Despite the use in Baltimore, Sean Vitka, policy counsel for the nonprofit group Demand Progress, questioned the legality of the wide-area surveillance use.

“I’m not so sure that I would agree with the contention that it is legal,” he said. “I think accounted for perhaps.”

The panel also brought up the decisions of *Carpenter v. United States* and *United States v. Jones*—two landmark cases. In the Jones case, police attached a tracking device to Antoine Jones’ vehicle without a warrant. In the Carpenter case, law enforcement tracked the use of Carpenter’s cell phone use.

Michel made the case that the use of surveillance could potentially be protected under the First Amendment and used the example of being the same as taking a picture from an airplane.

However, if the technology used infrared surveillance, it would be illegal, as the broad public cannot possess such technology, Michel added.

Questions of Safety

Another concern the panel discussed was the potential of recorded information being released to adversaries.

If the recording doesn't show a crime, the video is required to be deleted, according to Michel. He added that this is difficult to distinguish, as crimes are happening throughout cities daily.

According to Vitka, the additional markers that the software would use would include "name, gender, age, weight, religion, skills, biometrics, values, race, email, address, and even personality traits."

"Red flag," Patrick Eddington, the moderator and a policy analyst at Cato Institute, said after Vitka presented the list.

Despite the presented benefits of the technology, the general public hasn't had positive reactions to the implementations.

"Every time, so far, a city has revealed that it either has this technology in use or is intending to use it, it has been met with public pushback," Michel said. "Perhaps we have met a technology that is one step too far."