Privacy fears over artificial intelligence as crimestopper
12 November 2017, by Rob Lever

A display shows a vehicle and person recognition system for law enforcement during the NVIDIA GPU Technology Conference, which showcases artificial intelligence, deep learning, virtual reality and autonomous machines.

Police in the US state of Delaware are poised to deploy "smart" cameras in cruisers to help authorities detect a vehicle carrying a fugitive, missing child or straying senior.

The video feeds will be analyzed using artificial intelligence to identify vehicles by license plate or other features and "give an extra set of eyes" to officers on patrol, says David Hinojosa of Coban Technologies, the company providing the equipment.

"We are helping officers keep their focus on their jobs," said Hinojosa, who touts the new technology as a "dashcam on steroids."

The program is part of a growing trend to use vision-based AI to thwart crime and improve public safety, a trend which has stirred concerns among privacy and civil liberties activists who fear the technology could lead to secret "profiling" and misuse of data.

US-based startup Deep Science is using the same technology to help retail stores detect in real time if an armed robbery is in progress, by identifying guns or masked assailants.

Deep Science has pilot projects with US retailers, enabling automatic alerts in the case of robberies, fire or other threats.

The technology can monitor for threats more efficiently and at a lower cost than human security guards, according to Deep Science co-founder Sean Huver, a former engineer for DARPA, the Pentagon's long-term research arm.

"A common problem is that security guards get bored," he said.

Until recently, most predictive analytics relied on inputting numbers and other data to interpret trends. But advances in visual recognition are now being used to detect firearms, specific vehicles or individuals to help law enforcement and private security.

Elliot Hirsch of Deep Science holds a fake gun as he demonstrates the company's security system to
Recognize, interpret the environment

Saurabh Jain is product manager for the computer graphics group Nvidia, which makes computer chips for such systems and which held a recent conference in Washington with its technology partners.

He says the same computer vision technologies are used for self-driving vehicles, drones and other autonomous systems, to recognize and interpret the surrounding environment.

Nvidia has some 50 partners who use its supercomputing module called Jetson or its Metropolis software for security and related applications, according to Jain.

One of those partners, California-based Umbo Computer Vision, has developed an AI-enhanced security monitoring system which can be used at schools, hotels or other locations, analyzing video to detect intrusions and threats in real-time, and sending alerts to a security guard's computer or phone.

Israeli startup Briefcam meanwhile uses similar technology to interpret video surveillance footage.

"Video is unstructured, it's not searchable," explained Amit Gavish, Briefcam's US general manager. Without artificial intelligence, he says, "you had to go through hundreds of hours of video with fast forward and rewind."

"We detect, track, extract and classify each object in the video. So it becomes a database."

This can enable investigators to quickly find targets from video surveillance, a system already used by law enforcement in hundreds of cities around the world, including Paris, Boston and Chicago, Gavish said.

"It's not only saving time. In many cases they wouldn't be able to do it because people who watch video become ineffective after 10 to 20 minutes," he said.

Facial recognition can be useful for law enforcement and public safety but raises questions about secret profiling

'Huge privacy issues'

Russia-based startup Vision Labs employs the Nvidia technology for facial recognition systems that can be used to identify potential shoplifters or problem customers in casinos or other locations.

Vadim Kilimnichenko, project manager at Vision Labs, said the company works with law enforcement in Russia as well as commercial clients.

"We can deploy this anywhere through the cloud," he said.

Customers of Vision labs include banks seeking to prevent fraud, which can use face recognition to determine if someone is using a false identity, Kilimnichenko said.

For Marc Rotenberg, president of the Electronic Privacy Information Center, the rapid growth in these technologies raises privacy risks and calls for regulatory scrutiny over how data is stored and applied.

"Some of these techniques can be helpful but there
are huge privacy issues when systems are designed to capture identity and make a determination based on personal data," Rotenberg said.

"That's where issues of secret profiling, bias and accuracy enter the picture."

Rotenberg said the use of AI systems in criminal justice calls for scrutiny to ensure legal safeguards, transparency and procedural rights.

In a blog post earlier this year, Shelly Kramer of Futurum Research argued that AI holds great promise for law enforcement, be it for surveillance, scanning social media for threats, or using "bots" as lie detectors.

"With that encouraging promise, though, comes a host of risks and responsibilities."

© 2017 AFP