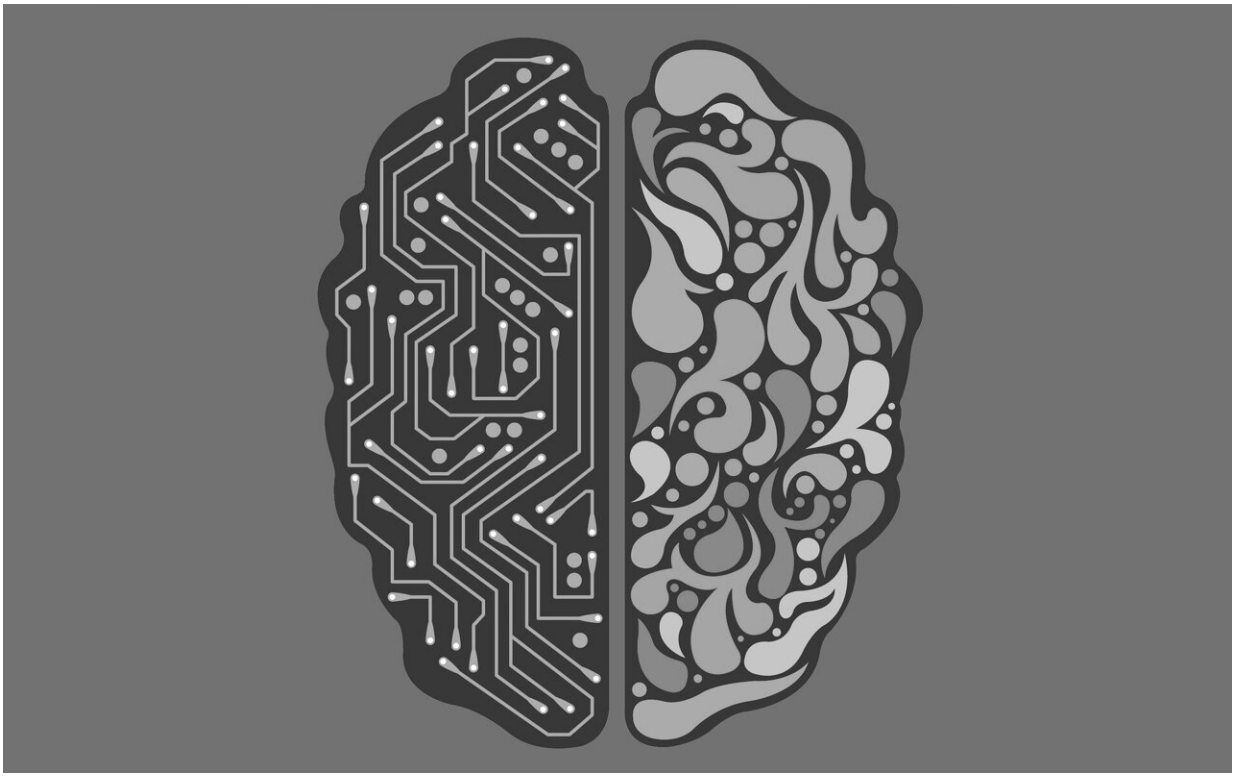
Next step in surveillance AI: Finding out who your friends are

March 3 2023, by Noah Bierman



Credit: Pixabay/CC0 Public Domain

A gray-haired man walks through an office lobby holding a coffee cup, staring ahead as he passes the entryway.

He appears unaware that he's being tracked by a network of cameras that

can detect not only where he has been but also who has been with him.

Surveillance technology has long been able to identify you. Now, with help from artificial intelligence, it's trying to figure out who your friends are.

With a few clicks, this "co-appearance" or "correlation analysis" software can find anyone who has appeared on surveillance frames within a few minutes of the gray-haired male over the last month, strip out those who may have been near him a time or two, and zero in on a man who has appeared 14 times. The software can instantaneously mark potential interactions between the two men, now deemed likely associates, on a searchable calendar.

Vintra, the San Jose-based company that showed off the technology in an industry video presentation last year, sells the co-appearance feature as part of an array of video analysis tools. The firm boasts on its website about relationships with the San Francisco 49ers and a Florida police department. The Internal Revenue Service and additional police departments across the country have paid for Vintra's services, according to a government contracting database.

Although co-appearance technology is already used by authoritarian regimes such as China's, Vintra seems to be the first company marketing it in the West, industry specialists say.

But the firm is one of many testing new AI and surveillance applications with little public scrutiny and few formal safeguards against invasions of privacy. In January, for example, New York state officials criticized the firm that owns Madison Square Garden for using facial recognition technology to ban employees of law firms that have sued the company from attending events at the arena.

Industry experts and watchdogs say that if the co-appearance tool is not in use now—and one analyst expressed certainty that it is—it will probably become more reliable and more widely available as artificial intelligence capabilities advance.

None of the entities that do business with Vintra that were contacted by The Times acknowledged using the co-appearance feature in Vintra's software package. But some did not explicitly rule it out.

China's government, which has been the most aggressive in using surveillance and AI to control its population, uses co-appearance searches to spot protesters and dissidents by merging video with a vast network of databases, something Vintra and its clients would not be able to do, said Conor Healy, director of government research for IPVM, the surveillance research group that hosted Vintra's presentation last year. Vintra's technology could be used to create "a more basic version" of the Chinese government's capabilities, he said.

Some state and local governments in the U.S. restrict the use of facial recognition, especially in policing, but no federal law applies. No laws expressly prohibit police from using co-appearance searches such as Vintra's, "but it's an open question" whether doing so would violate constitutionally protected rights of free assembly and protections against unauthorized searches, according to Clare Garvie, a specialist in surveillance technology with the National Assn. of Criminal Defense Lawyers.

Few states have any restrictions on how private entities use facial recognition.

The Los Angeles Police Department ended a predictive policing program, known as PredPol, in 2020 amid criticism that it was not stopping crime and led to heavier policing of Black and Latino

neighborhoods. The program used AI to analyze vast troves of data, including suspected gang affiliations, in an effort to predict in real time where property crimes might happen.

In the absence of national laws, many police departments and private companies have to weigh the balance of security and privacy on their own.

"This is the Orwellian future come to life," said Sen. Edward J. Markey, a Massachusetts Democrat. "A deeply alarming surveillance state where you're tracked, marked and categorized for use by public- and private-sector entities—that you have no knowledge of."

Markey plans to reintroduce a bill in the coming weeks that would halt the use of facial recognition and biometric technologies by federal law enforcement and require local and state governments to ban them as a condition of winning federal grants.

For now, some departments say they don't have to make a choice because of reliability concerns. But as technology advances, they will.

Vintra executives did not return multiple calls and emails from The Times.

But the company's chief executive, Brent Boekestein, was expansive about potential uses of the technology during the video presentation with IPVM.

"You can go up here and create a target, based off of this guy, and then see who this guy's hanging out with," Boekestein said. "You can really start building out a network."

He added that "96% of the time, there's no event that security's

interested in but there's always information that the system is generating."

Four agencies that share the San Jose transit station used in Vintra's presentation denied that their cameras were used to make the company's video.

Two companies listed on Vintra's website, the 49ers and Moderna, the drug company that produced one of the most widely used COVID-19 vaccines, did not respond to emails.

Several police departments acknowledged working with Vintra, but none would explicitly say they had performed a co-appearance search.

Brian Jackson, assistant chief of police in Lincoln, Neb., said his department uses Vintra software to save time analyzing hours of video by searching quickly for patterns such as blue cars and other objects that match descriptions used to solve specific crimes. But the cameras his department links into —including Ring cameras and those used by businesses—aren't good enough to match faces, he said.

"There are limitations. It's not a magic technology," he said. "It requires precise inputs for good outputs."

Jarod Kasner, an assistant chief in Kent, Washington, said his department uses Vintra software. He said he was not aware of the co-appearance feature and would have to consider whether it was legal in his state, one of a few that restricts the use of facial recognition.

"We're always looking for technology that can assist us because it's a force multiplier" for a department that struggles with staffing issues, he said. But "we just want to make sure we're within the boundaries to make sure we are doing it right and professionally."

The Lee County Sheriff's Office in Florida said it uses Vintra software only on suspects and not "to track people or vehicles who are not suspected of any criminal activity."

The Sacramento Police Department said in an email that it uses Vintra software "sparingly, if at all" but would not specify whether it had ever used the co-appearance feature.

"We are in the process of reviewing our Vintra contract and whether to continue using its service," the department said in a statement, which also said it could not point to instances in which the software helped solve crimes.

The IRS said in a statement that it uses Vintra software "to more efficiently review lengthy video footage for evidence while conducting criminal investigations." Officials would not say whether the IRS used the co-appearance tool or where it had cameras posted, only that it followed "established agency protocols and procedures."

Jay Stanley, an American Civil Liberties Union attorney who first highlighted Vintra's video presentation last year in a blog post, said he is not surprised some companies and departments are cagey about its use. In his experience, police departments often deploy new technology "without telling, let alone asking, permission of democratic overseers like city councils."

The software could be abused to monitor personal and political associations, including with potential intimate partners, labor activists, anti-police groups or partisan rivals, Stanley warned.

Danielle VanZandt, who analyzes Vintra for the market research firm Frost & Sullivan, said the technology is already in use. Because she has reviewed confidential documents from Vintra and other companies, she

is under nondisclosure agreements that prohibit her from discussing individual companies and governments that may be using the software.

Retailers, which are already gathering vast data on people who walk into their stores, are also testing the software to determine "what else can it tell me?" VanZandt said.

That could include identifying family members of a bank's best customers to ensure they are treated well, a use that raises the possibility that those without wealth or family connections will get less attention.

"Those bias concerns are huge in the industry" and are actively being addressed through standards and testing, VanZandt said.

Not everyone believes this technology will be widely adopted. Law enforcement and corporate security agents often discover they can use less invasive technologies to obtain similar information, said Florian Matusek of Genetec, a video analytics company that works with Vintra. That includes scanning ticket entry systems and cellphone data that have unique features but are not tied to individuals.

"There's a big difference between, like product sheets and demo videos and actually things being deployed in the field," Matusek said. "Users often find that other technology can solve their problem just as well without going through or jumping through all the hoops of installing cameras or dealing with privacy regulation."

Matusek said he did not know of any Genetec clients that were using co-appearance, which his company does not provide. But he could not rule it out.

2023 Los Angeles Times.

Distributed by Tribune Content Agency, LLC.

Citation: Next step in surveillance AI: Finding out who your friends are (2023, March 3) retrieved 8 April 2024 from https://techxplore.com/news/2023-03-surveillance-ai-friends.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.