Instant facial recognition a two-edged sword

November 21 2012, by Laura J. Nelson

By the time Joe Rosenkrantz took his seat in his company's conference room, a video camera had already handled the introductions. An image of Rosenkrantz, taken as he walked toward his chair, instantly popped up on a nearby TV screen.

"FaceFirst has found a possible match," the caption read. "Joe Rosenkrantz, Founder and CEO."

The process took less than a second, a demonstration of a capability that developer FaceFirst says could transform facial-recognition technology into an everyday security tool.

It addresses one of the key drawbacks in the current generation of video surveillance systems. Such identification technology has been limited to airports and casinos, where security officials have to wait several minutes for the software to identify terrorists or card counters.

But the technology is too expensive for most businesses and too slow to alert store owners or building owners about shoplifters or unwelcome visitors.

"It doesn't do me any good if I'm able to look at a face with a camera and five minutes later, there's a match," said Paul Benne, a security consultant who has recommended that his clients use FaceFirst in high-security areas. "By then, the person's gone."

FaceFirst hopes to leverage the speed of its software to gain military contracts, Chairman Peter Wollons said. But the company's main target is retailers. The software can be installed in almost any high-definition video camera, making it easy for stores to identify potential shoplifters - as well as big spenders.

And that is worrying privacy advocates. Although it isn't much different from retailers pulling personal shopping information from credit cards, the added feature of having a face instantly attached to that data is worrisome, said Jennifer Lynch, a lawyer with the Electronic Frontier Foundation.

"I see no reason for retail to know everything about us," Lynch said. "People who show their face in public aren't thinking about how their image is being stored or connected with other data."

FaceFirst's technology marks a dramatic advancement for an industry that 10 years ago seemed like it would never make the transition from science fiction to real life. After the Sept. 11, 2001, terrorist attacks, officials in Tampa, Fla., and at Boston's Logan International Airport installed cameras designed to identify criminals. Within a year, both had scrapped their systems.

It took five more years before facial-recognition technology was reliable enough to be used for security measures, but such systems have been mainly limited to law enforcement and government use. More than 70 percent of biometrics spending comes from law enforcement, the military and the government.

This year, the industry is projected to gross an estimated $6.58 billion, according to data from IBG, a biometrics analysis company. But that amount is expected to grow to $9.37 billion by 2014 as the technology becomes more affordable, faster and adaptable for nongovernmental uses.

FaceFirst founder Rosenkrantz started developing biometric technology as a way to remember a friend who was on one of the hijacked planes in the Sept. 11, 2001, terrorist attacks. Several of the terrorists were later identified in an airport surveillance video.

"I couldn't stop thinking about ways this could have been avoided," Rosenkrantz said. "I realized that with the right technology, we could have saved lives."

He tinkered with existing algorithms and operating systems for more than two years in his Calabasas, Calif., garage before founding FaceFirst. The company is a subsidiary of Camarillo, Calif., military contractor Airborne Biometrics Group Inc. Kayne Anderson Capital Advisors, an $18 billion investment company in Los Angeles, has invested in the development of the FaceFirst technology.

The company's success depends on the wide availability and decreasing prices of computer processors, Rosenkrantz said.

The software program takes a number of steps in less than a second to make an identification, starting with a freeze-frame of the live video feed. The software zooms in on the face, using the distance between the eyes as a guide.

Then an algorithm encodes the face based on distinct patterns and textures. The software cross-references that information with a database of similarly encoded images, which it can comb through at a rate of 1 million comparisons a second.

The database could include Homeland Security's terrorist watch list or a proprietary file generated by the user. When the system finds a match, it sends an alert to desktop computers and mobile devices.

National chains are particularly interested in using the technology, said Wollons, FaceFirst's chairman, because it helps them identify shoplifters. The retail industry lost an estimated $34.5 billion to shoplifting last year.

Other clients include security and surveillance companies, with whom FaceFirst has signed nondisclosure agreements, Wollons said. But inside FaceFirst's conference room, a row of baseball caps shows the agencies he's talked to: Los Angeles Police Department, U.S. Border Patrol, U.S. Navy, Department of Defense.

Last year FaceFirst installed cameras at the Panama City airport that tap into FBI and Interpol databases to identify suspected murderers and drug dealers. A law enforcement agency in San Diego now issues hand-held devices with cameras that use FaceFirst to match suspects against a database shared among 51 federal, state and local law agencies.

In addition, FaceFirst has signed a deal with Samsung that will make it the official provider of facial-recognition services on Samsung's surveillance cameras.

But as business grows, so do questions over how companies deal with biometric information and privacy concerns.

Privacy laws are the same for facial-recognition cameras as normal surveillance cameras, said Lynch of the Electronic Frontier Foundation. People have a reasonable expectation of privacy in places that aren't open to the public, such as bathrooms, hotel rooms and their own homes. Anywhere else is fair game.

The Federal Trade Commission issued guidelines last month telling companies to be more transparent about how they collect and store information. No such guidelines exist for law enforcement agencies.

FaceFirst doesn't provide the "watch list" databases. Its system only stores information about people when they register as a match.

At a Senate privacy hearing this summer, Sen. Al Franken, D-Minn., said he was worried that law enforcement would be able to use new technology - like the facial-recognition binoculars that the Justice Department is developing - to identify protesters and suppress free speech.

"You don't need a warrant to use this technology on someone," Franken said. "You might not even need to have a reasonable suspicion that they're involved in a crime."

Benne, the security consultant, often doesn't tell his clients that he's using FaceFirst technology because they don't always want to know. The level of sophistication is hard for people to swallow, he said.

"Bad things will happen, and the public will cry out for more to be done," Benne said. "A lot of it may not be very palatable right now, but as perpetrators try to do more things in more ways, we have to be prepared."

(c)2012 Los Angeles Times
Distributed by MCT Information Services

Citation: Instant facial recognition a two-edged sword (2012, November 21) retrieved 25 April 2024 from https://phys.org/news/2012-11-instant-facial-recognition-two-edged-sword.html