Camera Shy

Jim McKay, Editor | April 16, 2002

Among the most notable images captured by the cameras along Seventh Avenue in Ybor City, Fla., were protestors flaunting Groucho Marx glasses and displaying their middle fingers in disdain. Officials are betting, however, that the cameras, equipped with facial-recognition software, will one day identify someone wanted by the law.

In its infancy, the controversial biometric technology has galvanized citizen groups and created odd bedfellows. Consider this: As the protesters rallied along Seventh Avenue, the ACLU and conservative House Majority Leader Dick Armey, R-Tex., were forming the unlikeliest of unions to make a stand against using the technology in a way they consider a blow to every American's right to privacy.

Each of the 36 Ybor City cameras was equipped this summer with Visionics' FaceIt technology, which "reads" faces in a crowd. The software creates a digital map of an individual's face by translating the contours into mathematical formulas that are nearly as distinguishable as fingerprints. It then searches a database for a match. The database contains digital photos of wanted persons, such as felons with outstanding warrants or missing children. If a match is found, the software alerts police.

The technology gained notoriety in this country when it was used during the last Super Bowl to scan the crowds for known criminals, though it found none. It is now being considered in other areas, including Virginia Beach, Va., which is grappling with the idea of placing facial recognition cameras at its Oceanfront. Colorado and West Virginia are planning to use the software in conjunction with driver's license photos to intercept duplicate or fake licenses. West Virginia also has the software on 24-hour alert, searching Internet pornography sites for images of missing or exploited children.

The technology is also lauded in other parts of the world. In Britain, it is credited with reducing crime by 34 percent in a London borough. The Israeli government uses the FaceIt software to keep tabs on the flow of individuals entering the Gaza Strip, and the Keflavik International Airport in Iceland plans to add FaceIt surveillance to its security system to guard against terrorism.

Reasonable Suspicion

In the United States, the technology is causing a stir. Advocates say the innocent have nothing to worry about. Critics argue implementing the technology the way Ybor City has is intrusive and amounts to "facial frisking" without reasonable suspicion. They also say it's Big Brother looking over your shoulder and could be used to intimidate government critics.

"These systems, in essence, put innocent people into a virtual police lineup without any evidence that the person in the lineup is involved in crime and without that person even knowing that they've been put in this police lineup," said Craig Nojeim, associate director and chief legislative counsel of the ACLU's national office.

Federal and local government representatives are concerned. Armey has asked relevant House committees to hold hearings on law enforcement's use of the surveillance technology. In Jacksonville, Fla., Councilwoman-at-Large Gwen Chandler-Thompson introduced legislation that would ban the use of facial-recognition technology by the Sheriff's Department and other city agencies.

The debate centers on the actions law enforcement takes after the software identifies a wanted person, what happens to the images of innocent people captured by the cameras and whether citizens should be under surveillance on a public street.

"Clearly when you are on a street with 30,000 people, there is very little expectation of privacy," said Tampa, Fla., City Councilman Bob Buckhorn. "With all due respect to the ACLU, this is not your bedroom."

But opponents contend that the cameras shouldn't be used to generate suspicion. "On the streets, the police can't stop you and demand ID without what the Supreme Court has called 'reasonable suspicion,'" Nojeim said.

Reasonable suspicion is different from probable cause, the necessary criterion for searching a residence or frisking a suspect. Reasonable suspicion means having facts that criminal activity is afoot and the suspect is involved in it. Police need reasonable suspicion to stop someone and ask for ID. Privacy advocates contend that reasonable suspicion needs to occur before cameras identify a suspect.

"The argument that only guilty people have to worry about the police searches is an argument that we should have no Fourth Amendment," Nojeim said. "The fact is the privacy interests protected by the Fourth Amendment are for everybody."

Just an Experiment

Officials in Tampa say the facial recognition cameras will create a safer environment in the entertainment district where they are being used. They are currently using the technology on a one-year trial basis. The equipment is on loan from Visionics. If the experiment proves effective, the city will purchase the equipment at a cost of about $30,000, a nominal price for getting "a pedophile out of a situation where kids are present," according to Buckhorn.

Tampa officials say the cameras have been in place for three years. The difference now is the addition of the facial recognition software and the database of wanted felons, sex

offenders and missing children. "I look at this not as Big Brother, not as little brother, not even as a distant cousin," Buckhorn said. "It's nothing more than a tool for the Tampa Police Department, at their request, that allows us to take advantage of new technology."

Buckhorn said he's gotten mostly positive input from his constituents. "The people I represent e-mail me and say, 'Thank you. If you don't have anything to worry about then it's not a threat to your privacy.'"

Buckhorn said officers will double check to make sure no one is falsely identified, but added, "Computers are not fool proof. You're always going to have the human factor, but with the facial-recognition technology, the likelihood of an inadvertent stop is probably diminished."

In fact, law enforcement officials say the software merely facilitates a process that officers around the country use every day - comparing photos of wanted people to people walking down the street. "Every day when police officers show up for work they get hot sheets, or they carry pictures of subjects in their cars that they're looking for," said Detective Bill Todd of the Tampa Police Department. "That is no different from what they're doing here."

When the camera captures a person whose image matches an image in the database, an operator will respond to an audible alarm and compare the two images. If the operator determines that they match, he or she will alert an officer on the street. That officer will then confront the individual, inquire as to his identification and determine if the person is wanted.

"It's an alert mechanism," Todd said. "We don't depend on the software to make a positive identification. We still accept that responsibility."

Clear-Cut Policy

To read a face, the software analyzes 80 points between the nose, cheekbones and eyes. Faces that match at least 85 percent of the points of a database image will trigger an alarm. Visionics says the technology is accurate; under optimal conditions, the error rate for matches is less than 1 percent; and the software is able to account for changes in lighting, facial hair and aging. The accuracy rate could decline, however, if the facial image was recorded at an odd angle or if the photos in the database are of poor quality.

Visionics officials also say images are dumped from the system in five to 10 seconds if they do not match a photo in the database. But privacy advocates want clear-cut policy on how the software can and cannot be used, especially since Visionics has received federal funds from the Defense Department to perfect surveillance technology.

"In any kind of regulations there also have to

be policies that outline what process you can take to protect yourself if there's a false match," said Kate Rears of the Electronic Privacy Information Center.

Protecting the Public

Motor vehicle departments are also using the technology. DMVs hope to prevent people from acquiring false identities, rather than search for felons. "The sole motivation for this was to try to protect the public from identity fraud and to protect bankers and merchants from being victimized by theft," said Dorothy Dalquist, communications director for the Colorado Department of Revenue. "It's a lot different then what they're doing in Tampa."

Still, it has not escaped the wrath of privacy advocates.

"The risk of the Colorado system is that no federal law prohibits law enforcement use of the driving records that are being compiled by the Colorado DMV," Nojeim said. "So one day, the FBI or another law enforcement agency could get access to this information without adequate control and the driver would never know it."

In essence, the technology is not the subject of the protests; it's the methods of use and lack of control over how it's used. "We think it can definitely be a good thing if used effectively and responsibly," Rears said. "We want to see a lot more public debate."

Tampa's Buckhorn promises there will be plenty of that. "We may be the first out of the box to use it," he said, "but we won't be the last."