Driver's License Emerges as Crime-Fighting Tool, but Privacy Advocates Worry

Jodi Hilton for The New York Times

In a demonstration of facial-recognition technology, officials from the Digimarc Corporation matched a photograph of an employee with his photograph as it might appear in the driver's license database.

By ADAM LIPTAK
<http://topics.nytimes.com/top/reference/timestopics/people/l/adam_liptak/index.html?inline=nyt-per>

Published: February 17, 2007

BOSTON, Feb. 12 - On the second floor of a state office building here, upstairs from a food court, three facial-recognition specialists are revolutionizing American law enforcement. They work for the Massachusetts motor vehicles department.

Last year they tried an experiment, for sport. Using computerized biometric technology, they ran a mug shot from the Web site of "America's Most Wanted," the Fox Network television show, against the state's database of nine million digital driver's license photographs.

The computer found a match. A man who looked very much like Robert Howell, the fugitive in the mug shot, had a Massachusetts driver's license under another name. Mr. Howell was wanted in Massachusetts on rape charges.

The analysts passed that tip along to the police, who tracked him down to New York City, where he was receiving welfare benefits under the alias on the driver's license. Mr. Howell was arrested in October.

At least six other states have or are working on similar enormous databases of driver's license photographs. Coupled with increasingly accurate facial-recognition technology, the databases may become a radical innovation in law enforcement.

Other biometric databases are more useful for now. But DNA and fingerprint information, for instance, are not routinely collected from the general public. Most adults, on the other hand, have a driver's license with a picture on it, meaning that the relevant databases for facial-recognition analysis already exist. And while the current technology requires good-quality photographs, the day may not be far off when images from ordinary surveillance cameras will routinely help solve crimes.

Critics say the databases may therefore also represent a profound threat to privacy.

"What is the D.M.V.?" asked Lee Tien, a lawyer with the Electronic Frontier Foundation and a privacy advocate. "Does it license motor vehicles and drivers? Or is it really an identification arm of law enforcement?"

Anne L. Collins, the Massachusetts registrar of motor vehicles, said that people seeking a driver's license at least implicitly consent to allowing their images to be used for other purposes.

"One of the things a driver's license has become," Ms. Collins said, "is evidence that you are who you say you are."

The databases are primarily intended to prevent people from obtaining multiple licenses under different names. That can help prevent identity theft and stop people who try to get a second license after their first has been suspended.

"The states are finding hundreds of cases of fraud each year in each state," said J. Scott Carr, executive vice president of the Digimarc Corporation, which says it has sold biometric technology to motor vehicle departments in seven states and has a role in the production of more than two-thirds of all driver's licenses in the United States.

But the databases can also be used for law enforcement purposes beyond detecting fraud.

A page concerning Mr. Howell, printed out from the "America's Most Wanted" Web site, is taped to the wall of the investigators' office here. It is a kind of trophy.

"It's always exciting when you get a hit and you're getting someone really bad off the streets," said Maria Conlon, a facial-recognition specialist at the Registry of Motor Vehicles. "That's when everyone's morale goes up."

Most of the work is less glamorous. The analysts' main job is to check roughly 5,000 new driver's license photographs every day against the database. A computer algorithm that takes into account about 8,000 facial data points does a rough cut, and analysts examine potential matches, rejecting the vast majority.

That computers alone cannot do the job does not surprise Richard M. Smith, an expert in digital security. "It's probably one of the more inaccurate biometrics," Mr. Smith said, referring to facial-recognition technologies.

After computers narrow the field of potential matches, Ms. Conlon and her colleagues get to work.