Drawing a Blank:

The failure of facial recognition technology in Tampa, Florida

AN ACLU SPECIAL REPORT

By Jay Stanley and Barry Steinhardt

January 3, 2002

****

Introduction

Since September 11, facial recognition systems -- computer programs that analyze images of human faces gathered by video surveillance cameras -- are being increasingly discussed and occasionally deployed, largely as a means for combating terrorism. They are being set up in several airports around the United States, including Logan Airport in Boston, T.F. Green Airport in Providence, R.I., San Francisco International Airport, Fresno Airport in California and Palm Beach International Airport in Florida. The technology was also used at the 2001 Super Bowl, and plans are underway to use it at the NFL championship again in 2002.

The technology is not just being used in places where terrorists are likely to strike, however: in Tampa, Florida, it is also being aimed at citizens on public streets. Last summer, the Tampa Police Department installed several dozen cameras, assigned staff to monitor them, and installed a face recognition application called Face-IT® manufactured by the Visionics Corporation of New Jersey. On June 29, 2001, the department began scanning the faces of citizens as they walked down Seventh Avenue in the Ybor City neighborhood.

Acting under a Florida open-records law, the ACLU was able to obtain all existing police logs filled out by the operators of the city's face recognition system in July and August, 2001. Those documents and logs reveal several important things about the technology in one of its first real-world trials:

- The system has never correctly identified a single face in its database of suspects, let alone resulted in any arrests.
- The system was suspended on August 11, 2001, and has not been in operation since.

- In the brief period before the department discontinued the keeping of a log, the system made many false positives, including such errors as confusing what were to a human easily identifiable male and female images.
- The photographic database contains a broader selection of the population than just criminals wanted by the police, including such people as those who might have "valuable intelligence" for the police or who have criminal records.

The problems with facial recognition technology

Facial recognition systems are built on computer programs that analyze images of human faces for the purpose of identifying them. The programs take a facial image, measure characteristics such as the distance between the eyes, the length of the nose, and the angle of the jaw, and create a unique file called a "template." Using templates, the software then compares that image with another image – such as a photograph in a database of criminals – and produces a score that measures how similar the images are to each other. The software operator sets a threshold score above which the system sets off an alarm for a possible match.

One potential problem with such a powerful surveillance system is that experience tells us it will inevitably be abused. Video camera systems are operated by humans, who after all bring to the job all their existing prejudices and biases. In Great Britain, which has experimented with the widespread installation of closed circuit video cameras in public places, camera operators have been found to focus disproportionately on people of color; and the mostly male (and probably bored) operators frequently focus voyeuristically on women.

An investigation by the Detroit Free Press also shows the kind of abuses that can take place when police are given unregulated access to powerful surveillance tools. Examining how a database available to Michigan law enforcement was used, the newspaper found that officers had used it to help their friends or themselves stalk women, threaten motorists, track estranged spouses – even to intimidate political opponents.[1] The unavoidable truth is that surveillance tools will inevitably be abused.

Facial recognition is particularly subject to abuse because it can be used in a passive way that doesn't require the knowledge, consent, or participation of subjects. It is possible to put a camera up anywhere and train it on people; modern cameras can easily view faces from over 100 yards away. People act differently when they are being watched, and have the right to know if their movements and identities are being captured.[2] "I've seen it all," Tampa-police camera operator Raymond C. Green told the St. Petersburg Times. "Some

[1] M.L. Elrick, "Cops tap database to harass, intimidate," *Detroit Free Press*, July 31, 2001. At http://www.freep.com/news/mich/lein31_20010731.htm.

[2] It is important to note that the ACLU is making no accusation that the Tampa PD has misused the system and has no evidence of any such misuse.

things are really funny, like the way people dance when they think no one's looking. Others, you wouldn't want to watch."[3]

This technology has the potential to become an extremely intrusive, privacy-invasive part of American life. History shows that once installed, this kind of a surveillance system rarely remains confined to its original purpose. Already, in the case of face recognition, it has spread from purportedly looking for terrorists at the high-profile Super Bowl to searching for petty criminals and runaways on the public streets of Tampa.

Given the problematic social consequences of going down the path of widespread deployment of facial recognition-enabled video surveillance systems, proponents of the technology must at least demonstrate that it will be highly effective in achieving the goal for which it is being justified: combating terrorism and other crimes. However, all prior indications have been that the technology is not effective and does not work very well. Two separate government studies have found that it performed poorly even under ideal conditions where subjects are staring directly into the camera under bright lights.[4] Several government agencies have abandoned facial-recognition systems after finding they did not work as advertised, including the Immigration and Naturalization Service, which experimented with using the technology to identify people in cars at the Mexico-US border. And the well-known security consultant Richard Smith, experimenting with FaceIT® – the same package used by the Tampa police – found that it was easily tripped up by changes in lighting, in the quality of the camera used, in the angle from which a face was photographed, in facial expression, in the composition of the background of a photograph, and by the donning of sunglasses or even regular glasses.[5]

How the ACLU obtained documents on Tampa's facial recognition system

Because facial recognition is such a potentially powerful and invasive surveillance tool – and because the Tampa police department's deployment represents one of the first real-world tests of facial recognition technology, the ACLU was eager for details on the system and how it was being used. On August 2, 2001, the ACLU of Florida filed a request[6] under Florida's open-records law[7] (the state equivalent of the federal Freedom of Information Act) for all documents pertaining to:

- the decision-making process by which Tampa elected to deploy the system

[3] Lane DeGregory, "Click. BEEP! Face captured," *St. Petersburg Times*, July 19, 2001. Search online at http://pqasb.pqarchiver.com/sptimes/index.html.

[4] See http://www.dodcounterdrug.com/facialrecognition/DLs/Feret7.pdf for a study by the National Institute of Standards and Technology, and http://www.dodcounterdrug.com/facialrecognition/DLs/FRVT_2000.pdf for a study by the Department of Defense.

[5] See http://users.rcn.com/rms2000/facescan/

[6] See http://www.aclu.org/news/2001/n070601a.html#letter and http://www.aclu.org/issues/privacy/flsunlet.html

[7] See Fla. Stat. 119.01(4).

- camera locations
- the technical capabilities of the system being used
- the procedures, instructions and training provided to system operators
- the contents of the image databases
- written procedures for how the identification process is handled
- future plans for these systems

A second request was submitted on October 19, 2001. A third letter was sent to the department on November 27.

On December 4, the ACLU was furnished with copies of police logs filled in by system operators between July 12 and August 11, 2001; a Memorandum of Understanding between the software manufacturer, Visionics, and the police department; the department's Standard Operating Procedure governing the use of the system; and a training video.

The results: no hits, no arrests, many false positives

The Tampa Police Department Face-IT® operator logs obtained by the ACLU show that the system not only has not produced a single arrest, but it also has not resulted in the correct identification of a single person from the department's photo database on the sidewalks of Tampa. Tampa police Detective Bill Todd not only confirmed these results to the ACLU in phone conversations on December 17-18, but he also acknowledged that the system has been out of operation since the last log sheet was filled in on August 11.

The earliest logs provided by the department show activity for July 12, 13, 14, and 20, 2001. On those dates, the system operators logged 14 instances in which the system indicated a possible match. Of the 14 matches on those four days, all were false alarms. Two of the "matches" were of the opposite sex from the person in the database, and three others were ruled out by the monitoring officers due to differences in age, weight or other characteristics that made the mismatch obvious to a human observer. The rest of the false positives were simply notated with a terse "not subject." These results are consistent with an anecdotal report in the July 19, 2001 *St. Petersburg Times* that "the alarm sounds an average of five times each night."[8]

After July 20, 2001, the remaining logs provided by the department are blank, and no logs were provided for dates later than August 11. Based on conversations with representatives of the Tampa Police, it appears that the blank logs are attributable to one of two possibilities or a combination of those possibilities:

- Because of the high number of false positives, the department changed the software's "threshold" setting that determines how firm a match is required before an alarm is sounded. That change resulted in far fewer false positives (but would

[8] For a description of the system's operation, see Lane DeGregory, "Click. BEEP! Face captured," *St. Petersburg Times*, July 19, 2001. Search online at http://pqasb.pqarchiver.com/sptimes/index.html.

have also further reduced the chances that anyone in the database who wandered in front of the department's cameras would actually be identified by the software).

- Acting either on their own or at the direction of an internal policy decision, the officers operating the system decided to record only genuine matches, and not false positives. The log sheets are blank because there were no genuine matches.

Because the system does not automatically scan the faces of people on the sidewalks – operators must manually zoom in on a citizen's face before it registers in the software – it would not be surprising that system operators faced with an endless string of negative results would spend less and less time and energy searching out and capturing facial images, as opposed to simply watching the video images for signs of trouble.

A reporter for the St. Petersburg *Times* reported on July 19 that on the night he visited – at the apparent peak of the system's operation – the operator captured 457 faces out of the estimated 125,000 people who visit Ybor City on a typical Friday.[9] If that proportion were to decline further, the already tiny chances for obtaining a genuine match with a photo in the database would shrink even more.

Detective Todd explained the lack of any log sheets after August 11 by confirming that the Face-IT® system was taken out of service. (A notation of "N/A" on the August 11 log sheet may have indicated that the system was used only for a test or demonstration that day, he said.) Todd explained the decision as a result of a police redistricting, which necessitated training new officers in the system's operation. He said that the department planned to resume use of the system at some point in the future. However, it is reasonable to assume that the professionals in the Tampa PD would not have let the system sit unused for so long because of a mere redistricting process had they previously found facial recognition to be a valuable tool in the effort to combat crime.

One nation, under suspicion?

The department's written guidelines for "Utilization of Face-IT® Software" reveal several other interesting points about Tampa's use of face recognition. First, the guidelines state that photographs are entered into the database if the subjects are wanted by the police; if "it is determined that valuable intelligence can be gathered from contact" with a person; or "based upon an individual's prior criminal activity and record."

"Twenty percent of the criminals commit 80 percent of the crimes," the guidelines state. "It is the intention of the Tampa Police Department to identify those subjects through the use of this software. Through this proactive approach, the Tampa Police Department can deter criminal activity prior to a criminal offense being committed."

Far from protecting citizens against the next terrorist strike or other violent crimes, the department's guidelines thus make clear that the system was used in an attempt to assist the full range of cases in which local police are involved. Not just terrorists and violent

[9] Ibid.

criminals, but anyone who might have "valuable intelligence" for the cop on the beat, according to these guidelines, will have his or her photograph entered into a police database so that they may set off an alarm whenever they visit a public place that is within the lens of a department camera.

The move to permanently brand some people as "under suspicion" and monitor them as they move about in public places has deep and significant social ramifications. If we are to take that path -- a step that the ACLU opposes -- we should do so as a nation, consciously, after full debate and discussion, and not simply slide down that road through the incremental actions of local police departments.

Conclusion

The documentary record obtained by the ACLU of the Tampa Police Department's experience with facial recognition technology adds an important new piece of evidence that the technology does not deliver security benefits sufficient to justify the Orwellian dangers that they present. What the logs show -- and fail to show -- tells us that face recognition software performs at least as badly in real-world conditions as it has in the more controlled experiments that have been carried out.

The only possible justification for deploying such an ineffective technology would be that it somehow deters crime because citizens believe that it works. There are several problems with that argument. First, it is premised on a Wizard of Oz-style strategy of hiding the truth about facial recognition technology from the public – a stance that is not compatible with the vital importance of public scrutiny of the tools, technologies and techniques that police departments deploy.

Second, even if face recognition cameras did deter wanted criminals from frequenting the areas under surveillance, all that would happen is that the criminals would move to other locations. Indeed, sociological studies of closed circuit television monitoring of public places in Britain – where residents are widely aware of the cameras – have shown that it has not succeeded in reducing crime.[10]

Given the system's poor performance in Tampa – which the police department there has implicitly recognized in their decision to stop actively using it – the ACLU hopes that police departments around the nation will step back, objectively examine the costs and benefits of the system, and reject them as ineffective. Other cities have voted to deploy these systems, including Virginia Beach, Palm Springs and Boulder City, Nevada. We ask those cities to consider the documentary evidence from Tampa and not waste precious resources on this illusory path toward public safety.

The worst-case scenario would be if police continue to utilize facial recognition systems despite their ineffectiveness because they become invested in them, attached to government or industry grants that support them, or begin to discover additional, even

[10] See http://www.scotcrim.u-net.com/researchc2.htm for the full text of the research findings of the Scottish Office Central Research Unit.

more frightening uses for the technology. The continued use of facial recognition technology under these circumstances would divert limited law enforcement resources from more productive pursuits, create a dangerous false sense of security, and ultimately threaten the privacy, freedom and safety of everyone in America.