

Bringing facial recognition to the security table

Written by Kevin Gordon

According to Thompson's press release, this bill, which was introduced in May, requires the Transportation Security Administration (TSA) to:

- Study existing and proposed industry programs that enhance our biometric security systems at airports;
- Study how airports can transition to uniform, standards-based and interoperable biometric identifier systems for airport workers with unescorted access;
- Submit to Congress a breakdown on best practices for issuing biometric credentials for airport workers;
- And the Secretary of Homeland Security to spearhead a working group with industry stakeholders to strengthen private and public partnerships as they support the secretary and assistant secretary in carrying out this act. This bill may be the push that is needed to bring enhanced biometrics, especially facial recognition to the security table. All public safety personnel are familiar with fingerprints and, on a lesser level, iris scans. Many are less familiar and have less experience with facial recognition. The general non-intrusive application of facial recognition and the great technological advances over the past 20 years will certainly make it a popular option in today's world of homeland security.

As is often the case in the world of crime-fighting technology, the UK is ahead of the U.S. in this area. This can be seen not only in facial recognition, but also in other security and police areas such as automatic license plate readers (ALPR), public area surveillance cameras, and head cams on police officers' hats. The UK Home Office, the government department that is charged with leading the efforts of the nation in protecting the public from crime and terrorism, expects facial recognition, iris recognition and fingerprint verification to play an ever-growing role in the future of passport control and border security. This includes ID cards that will use all three of these technologies, face, iris and fingerprint. These IDs are part of a \$30 million program, called Project Semaphore, which is part of the UK's electronic borders (e-borders) program.

While facial-recognition technology can be used in a variety of areas, the average person thinks of it being used at airports, ports, and other areas where immigration and border control is an issue. In those instances, it is generally used to view people entering a location, not just scanning the general public. But because it can be used as a mass surveillance method, which by definition is the surveillance of an entire population or fraction of that population, the use of such technology almost always has opponents who are concerned about the loss of privacy. Public safety likes the technology because it can be used in a non-intrusive, passive manner, but those are the same reasons some are fearful of the technology.

The ACLU's stated mission is to preserve the protections and guarantees of the Bill of Rights, and as it applies to this concern, the right to privacy and "freedom from unwarranted government intrusion into your personal and private affairs." The ACLU asks two questions to determine if security technology of any sort should be utilized or not. The first question: "Is the technology effective in increasing safety and security?" If answered yes, the second question is. "Does the technology violate 'the appropriate balance between security and liberty.'" The ACLU believes facial recognition can't pass this test on either question. Proponents of the technology disagree.

It is important that public safety professionals understand and appreciate the reasons some oppose the technology just as much as they need to understand the technology and how it can be used. The most effective technology cannot work if it isn't installed and used. This isn't just a facial-recognition issue. Some of the same arguments are being made concerning public area surveillance cameras, red light cameras and so on. In such controversial areas, some public safety folks often avoid the technology in order to avoid the resulting battle. Quite simply, you can't win the war if you don't fight the battles. Public safety officials should take a good hard look at facial-recognition technology and see if it can work for them. One of the leading providers of biometric identity management systems is Cross Match Technologies Inc., which has many solutions for public safety.

Cross Match was founded in 1996 and serves an international market with its home offices in Florida and additional operations in Virginia, Canada and Germany. Cross Match products are presently installed in more than 80 countries. You may have heard of Cross Match and its partnership with the Nashville, TN school district. This school security measure was widely reported in the national news. Working with Cross Match, the Nashville school district was the first district in the country to use face-recognition software with security cameras. The district processed video from three test schools and the district office as the test sites. The facial images are extracted and stored in the system, and if a face is detected that is in the undesired, watch list database, it immediately notifies the appropriate personnel.

Cross Match has achieved many "firsts," including the first to be certified by the FBI for its image quality standard, the first to be certified by the FBI for 1,000 pixels per inch quality, and the first to introduce mobile fingerprint scanners. Cross Match provides a variety of biometric solutions, including fingerprint and palm scanners and iris-capture devices.

Cross Match's facial-recognition system, FaceCheck® Server software, serves public safety on a variety of levels, including visitor management, jail intake and entry monitoring and courthouse surveillance. Using a high-resolution digital camera for live verification, when a person enters the designated secure area, the system automatically captures the facial image and then compares the facial patterns (distances between the eyes, mouth, nose, etc.) against the data in the watch list. The system stores one or more watch lists with portraits of identified people. Facial images

are compared with the watch list images, and when locating a person of interest, (a similarity score exceeding a set threshold value), it notifies the appropriate personnel.

FaceCheck can speed up jail intake and the booking process by verifying the ID of those being booked. Advantages to courthouse surveillance are obvious, once again allowing all visitors to the courthouse to be viewed in a non-intrusive manner while looking for persons of interest. The editing software in FaceCheck is based on pre-selected criteria and automatically standardizes facial images and crops those images. There is no posing necessary as the software only recognizes and records the facial images. No matter where the person is positioned in the field of vision of the camera, it auto captures the person's face. It is extremely useful if you have a lot of people to photograph, such as a large employee base, as it provides the best image by automatically performing color corrections, contrast, and brightness.

Another feature in Cross Match's facial-recognition solution is facial video surveillance with video analysis. This tool, known as FaceSnap Recorder, locates and extracts images from existing video footage to assist in identification and/or verification of the suspect. These images are then viewable as time-stamped portraits, which allow personnel to isolate those individuals who are associated with the actual event time. FaceSnap Recorder software can recognize faces in a crowd and at a distance.

Other uses for facial recognition include live verification of ID photos used in high security areas, border control, and ID photo-based identity checks.

Kevin Gordon spent 25 years in law enforcement and retired as a chief of police. He holds an MA in security management, is a CEM and a CPP. He is a national officer with the International Police Association. He can be reached at kevin@kgordon.com.

Originally Printed in Public Safety IT Magazine, July 2008