

LAW ENFORCEMENT MANAGERS MUST BE WILLING TO
FACE UP TO SECURITY IN ORDER TO PREVENT CRIME AND TERRORISM

Article

By

Captain Mike Callagy
San Mateo Police Department

Command College Class XXXIV

San Mateo, California

October 2003

34-0671

Due to new biometric facial recognition (BFR) technology, wanted individuals and terrorists will, in the future, find it very difficult to blend in with society. The theory about detecting terrorists and criminals starts with the basic premise that all criminals and all terrorists have a face. No matter how hard they may try to hide it, due to exciting emerging advances in biometric technology, their face is like a visual fingerprint that will one day be the reason they are captured and brought to justice. There will always be someone watching for them through the millions of cameras that have been spread out over the country.

Public safety is a major concern to Americans with the battle against terrorism now being fought on our own soil. Never before have Americans been so concerned about their own safety as they come to grips with violent crime and the ever-present real threat of terrorism. Law enforcement agents struggle every day to identify suspects who have committed crime in an effort to take them off the street before they strike again. Federal agents are seeking ways to protect our borders and airports from known terrorists, who, like two of the September 11, 2001, hijackers, were well-known to law enforcement. Lack of communication about wanted individuals and terrorists in the law enforcement field has acted to give criminals the ability to blend in with society until they are ready to strike.

In an effort to combat these increasing threats to public safety, private companies and law enforcement should be working together to develop biometric technology that may someday identify terrorists or criminals before they strike. Use of biometrics as an identification tool is not new, but the use of biometric facial recognition technology as an identification tool is an emerging technology. This technology has been deployed in limited capacities, yet is still in its infancy stage in regard to practical applications by law enforcement agencies.

The long-term capabilities of biometric facial recognition technology are unknown, yet exciting to law enforcement due to the potential ability of this technology to identify wanted individuals and terrorists before they commit crimes. Biometric facial recognition technology, if perfected, might have the ability to save incredible amounts of law enforcement resources, while providing unprecedented security to areas where Americans feel most vulnerable. September 11th has been a transforming event not just because of its enormity, but also because of the nature of the attacks. Fifty thousand Americans were killed in a decade of fighting in Vietnam, combatants who died on battlefields. Over 3,000 people were murdered in one morning in New York, Washington, and Pennsylvania.¹

The United States, which was easily the most patriotic country in the world,² had patriotism go off the charts as it led allied troops in a battle that was now brought to the homeland of every American. Extraordinary times call for extraordinary measures. The United States had clearly and decisively won the battle against terror in Afghanistan, but this was just one battle in an ongoing war with no end in sight.

What remains to be seen is how Americans will adjust to this ongoing war and what expectations they will have in the area of personal security, as well as what liberties they might be willing to relinquish to reach that level of security. Lack of security was not a moment in time and must not be forgotten. Americans thought that with all the intelligence, with all the police, with all the screening processes in place, the United States was safe. The September 11, 2001, terrorist attacks came like a blow by a hammer to the heads of most Americans.

How could so much go so wrong, so fast? One day, Americans woke up to a different country than they left when they went to sleep. The United States was no longer safe from a

catastrophic attack by terrorists. The question loomed: What would be the long-term impact on law enforcement and the public as a result of that unforgettable day in September 2001?

Americans are scared, and this may be a strong signal that the timing is right for new security technology to help fill the void in America's confidence in regard to the security of this nation. The University of Michigan, Institute for Social Research (ISR), polled 613 Americans in March 2002 in regard to their relative feelings of security in light of the September 11, 2001, terrorist attacks. According to a study, 11% of the 613 Americans surveyed in March 2002 were reported to be more shaken when re-surveyed in May 2002; 13% said they were less shaken, while 75% said their sense of insecurity was unchanged.

The findings from this survey suggest that the psychological, social, and political effects of those September 2001 events have been in fact profound and enduring. "Despite attempts by the government to assure Americans that homeland security is a priority, most Americans don't feel any safer today than they did right after the attacks."³

Research by the Michigan's ISR shows that women are almost twice as likely as men to remain shaken by the terrorist attacks, they reported that their feeling of personal security has been profoundly impacted.⁴ An increasing number of Americans are feeling that terrorism represents a real threat to not only all of America, but also to their own personal safety and that of their family.

The Michigan ISR study showed that an overwhelming amount of Americans polled (84%) felt that it was likely or very likely that another terrorist attack in the United States would take place in the near future. The ISR research went even further to try and establish when Americans feel most vulnerable to terrorism. The results show that most Americans feel

vulnerable to terrorism when flying, attending sporting events, going to the mall, and attending movies.⁵

Biometric facial recognition is most effective when it is used in controlled settings, which may be found or created in the above-referenced environments. The very fact that Americans are looking for more security in these given areas may act to expedite the use of this emerging technology.

Biometrics is defined as the “automated methods of identifying or authenticating the identity of a living person.”⁶ In its purest sense, before automation, biometric identification can be traced as far back as 1879, when, at the age of twenty-six, Alphonse Bertillon joined the Paris Police Department as a clerk. According to Clive Reedman, author of “Biometrics and Law Enforcement,” young Alphonse was the son of an anthropologist, who had spent a large portion of his career attempting to prove that no two human beings possessed identical physical characteristics and that the distinct characteristics were in fact measurable.⁷

How Facial Recognition Systems Work

Facial recognition falls into a larger group of technologies known as biometrics. This technology uses biological technology to verify identity. Faces are a very important part of who we are and how we are recognized. The most basic idea about biometrics is that every human body possesses unique properties that can be distinguished from others. Besides facial recognition, other examples of biometrics include, but are not limited to: fingerprint scan, retina scan, and voice identification.⁸

Facial recognition is something that every human being uses on a daily basis. It can be used as a tool of survival as humans act to friends and foes. As we walk down the street, our

eyes act as sensors and send a message to our brain, which acts as a computer with stored images. This simplistic example acts to underscore the basic principles of biometric facial recognition systems. It can be said, then, that faces are the most unique physical trait of humans.⁹ Starting with that premise, it can be easily understood why agencies would want to use the physical characteristics of the face to identify an individual who may harm or pose a threat to society.

“Generally speaking, the system works by first obtaining the image of a person. This is usually accomplished by the use of a video camera with at least 320x240 resolution at 3-5 frames per second.”¹⁰ Obviously, a higher quality camera will produce better results. Facial recognition systems may vary, but the steps usually include capturing a face, analyzing the face, and comparing it to facial images stored in a database.

When it is connected to a video surveillance system, the recognition software will search a given field of view for faces. The system can detect a face within a fraction of a second, and a multi-scale algorithm (program that provides instruction to do a certain task) is used in situations of low or varied light. Lighting, as will be explored in more depth later in this article, can be a major factor in the identification process.

Once a face is detected, an alignment takes place. The head’s position, along with size and pose, is noted. For most systems, the face needs to be turned at least 35° in the view of the camera for the system to register. Normalization then takes place as the face is mapped and registered into a standardized pose. In this process, light is not a factor. The software then translates the collected data into a unique code. This unique code will allow for a more simple comparison against stored data. The acquired data is then compared against that of the stored data in the effort to make a match.¹¹

The four main methods of capturing the needed information are eigenfaces, feature analysis, neural network, and automatic face processing.¹² Eigenfaces was developed at MIT and is a tool that extracts characteristics through the use of two-dimensional gray scale imagery. This technology, used by many leading companies today, uses a sophisticated algorithm based on principle component analysis that can translate characteristics of a face into a unique set of numbers.¹³ There is then a real-time comparison for both identification and verification in an existing database.

Feature analysis, which is also called local feature analysis, is one of the most widely used methods of identifying faces, because it can adapt to changes in facial aspects, which is crucial in light of the ability of criminals or terrorists to attempt to change facial appearances or features. The Local Feature Analysis uses an algorithm of 84 bytes in size to create a facial print for comparison.¹⁴

A neural network extracts facial features to create a template used against contrasting elements that is then matched against the existing database. This particular product may be the future of facial recognition. The last system is the automatic face processing technique that measures distances and ratios between certain facial features.¹⁵ This system is commonly used in poor lighting conditions.

The speed of automation is what makes biometric facial recognition technology so attractive to law enforcement. For example, the Local Feature Analysis can match multiple face prints at a rate of 60 million from memory or 15 million per minute from a hard disk.¹⁶ As the comparisons are made, the system will assign a value between one and ten. The operators of the system establish a predetermined threshold, and if a score above the threshold is indicated, a

match is declared. The operator can then visually compare the match to help determine the validity.

This system would function like many modern day dispatch centers. Cameras would be monitored by trained staff, who would either look for suspicious suspects and direct cameras to capture their photos, or simply monitor the automated process. Once a match is detected, the observer is able to contact police to make an arrest, while the suspect's every move is followed on camera.

Drawbacks of Biometric Facial Recognition Technology

Biometric facial recognition technology is not without controversy or drawbacks. It is becoming more and more common, yet many see this emerging technology as a governmental intrusion on their right to privacy. Though hardly 100% accurate and certainly not foolproof, biometric facial recognition technology is on the fast track to implementation as a promising crime deterrent. In 2001, MIT Technology Review named biometrics as, "one of the top ten technologies that will change the world."¹⁷ Others, like the American Civil Liberties Union (ACLU), have big brother taking society one step closer to a full-fledged surveillance society.¹⁸

Is it possible that, as we leave behind an escalating number of data trails, we are giving the government the opportunity to combine information from different sources? Will those sources result in the recreation of one's activities with such detail that it would be like being followed with a camera twenty-four hours a day? The ACLU seems to believe that this is exactly what the government will be able to do if not stopped.

According to the ACLU, the biggest threat to privacy comes from the government.¹⁹ The ACLU attributes this statement to several factors that include expansive government databases,

communications surveillance (such as the FBI's new Carnivore Program), the Patriot Act (which overnight changed the United States surveillance laws), and the loosened domestic spying regulations.²⁰

Critics of government surveillance are not so worried about where we are today, but rather, where we are going tomorrow. Critics say thus far the enormous information that has been collected on Americans is somewhat protected in that this information exists in many different databases that do not communicate with each other. Says the ACLU, "The real threat to privacy will come when the government, landlords, employers, or other powerful forces gain the ability to draw together all this information."²¹

Some see the well-intentioned attempt to safeguard American security as a slippery slope that could someday lead from specific surveillance to general surveillance and then morph into a national ID card system, which many believe is an invasion of privacy. The government officials argue that facial recognition systems will add another layer of security, but will not undercut civil liberties.²²

The question remains as to how far facial recognition systems will be able to go before they are considered an invasion of privacy, but it seems that they will remain legal for now. In Richmond, Virginia, a bill was introduced that would have required a judge's signature to use facial recognition technology. That senate, in an 11-4 vote, ultimately shelved deployment of the bill. There currently are no standard guidelines for the use of biometric facial recognition surveillance, leading some lawmakers to feel that the databases are on the verge of an explosion.²³ There has clearly been a proliferation of cameras since September 11, 2001, but are they really an invasion of privacy?

While the human recognition of a face is cognitive in nature, it could be said that the biometric recognition of a face is more computerized and automated. Does this mean that it violates Americans' rights to privacy? We have to start with the premise that in the United States Constitution there is no mention of the word privacy. Yet, several amendments of the Constitution, namely the First, Third, Fourth, Fifth, and Fourteenth, address the concern of government intrusion into the lives of individuals. So, with a closer look at the Constitution, we find implicit physical privacy rights that can be accompanied with the Supreme Court's espoused concern with the, "accumulation of vast amounts of personal information in computerized data banks or massive government files."²⁴

While some civil libertarians might argue that the massive dragnet that takes place on busy weekends in Ybor City, Florida, or during the Super Bowl in Tampa is improper and in violation of an individual's Fourth Amendment Right against illegal search and seizure, these searches are surely constitutional.²⁵ The Court has consistently found that an individual does not have an expectation of privacy for personal physical characteristics that are constantly exposed to the public, like facial features.²⁶

John Woodward, Jr., of the Rand Corporation foresees that as facial recognition systems become interlinked, the threat to information privacy increases.²⁷ If systems become superlinked, governments could potentially trace the movements of any individual whom they have in their database. This would include the widespread proliferation of cameras that would potentially capture our image on the freeway, on the subway, at the ATM, about town, and even in the cleaners! Woodward suggests that the possibility exists for the government to then enter all your friends in the database and put them on the watch list, while "reverse engineering" their identity to track where they were for the last several months.²⁸ Yet, the only real way that even

this super surveillance²⁹ may be found to be unconstitutional is if it had a chilling impact on an individual's ability to attend First-Amendment-protected activities. This is unlikely to be found true, but only time will tell if and when databases are in fact connected in the future.

What has clearly been found to be the case, especially in light of September 11, 2001, is that Americans seem ready to give up some civil liberties in order to secure their safety. In one study by the University of Michigan, ISR, after September 11, 2001, and in March 2002, over 70% of individuals polled said they would be willing to give up some of their civil liberties to ensure more security.³⁰ This research also revealed that most Americans would support increasing security measures.³¹

Benefits of Biometric Facial Recognition Technology

The emerging technology of biometric facial recognition must be explored because of the potential it has for preventing crime and capturing terrorists. Crime has been on the rise in recent years and promises to get worse before it gets better. In the first nine months of 2002, the California Crime Index, which tracks homicide, forcible rape, robbery, aggravated assault, burglary, and motor vehicle theft, showed a 5.3% increase.³² Most surprising is that homicide was up 13.1%, forcible rape was up 2.6%, and robbery was up 4.5%.³³

Terrorism is likewise on the rise. In 1996, in Saudi Arabia, a terrorist truck bomb exploded killing 19 service men. Truck bombs in Kenya killed 224 and wounded 4,600 others. The USS Cole in Yemen was attacked killing 17 sailors and wounding 42 more. Then, on September 11, 2001, the United States changed forever when over 3,000 were murdered in the worst terrorist attack in history.

The threat of continued terrorism and crime in the homeland is a real one. Federal and local law enforcement agencies need as many tools as possible to separate the good guys from the bad guys in order to prevent criminal acts before they occur. As it stands now, there are millions of cameras all over the United States, but there is no one centralized database or way to classify or sort these images. Criminals are caught on tape everyday, yet they continue to go unpunished because of the lack of ability to identify them.

One of the most unforgettable and haunting images of the September 11, 2001, terrorist massacre was that of the face of hijacker Mohamed Atta as he walked passed a metal detector in the Portland, Maine, airport. Could the terrorist attacks of September 11, 2001, have been stopped if a biometric facial recognition system were in place at the Portland Airport? That question will never be answered, because there was no system in place. Federal and local law enforcement officers are at a distinct disadvantage in this highly mobile and transient-oriented society. Police are constantly caught in a game of here today and gone tomorrow.

Typically, in today's law enforcement, officers will respond to a scene of a crime where the image of the suspect has been captured on closed-circuit television (CCTV) or some digital surveillance camera system. The officers will look at the image to determine if they know who the person is from past encounters, or they may sift through thousands of in-house photos in an effort to identify the suspect. The officers may also send out on a TRAK system (technology to recover abducted kids) to all local police agencies with the suspect's image and a brief synopsis of the crime. When they become completely frustrated, they may forward the photo to the print media or news agencies for distribution. But unless these cases are high profile or somehow newsworthy, police will never get the opportunity to get help from the public that might lead to the identity of the suspect. Police spend countless frustrating hours looking to identify the

suspect in the image, yet, usually, the end result is that another suspect goes free to victimize again.

Biometric facial recognition technology promises to be the tool that acts to level the playing field. The beauty of this system is that it is so convenient and non-intrusive. At the 2001 Super Bowl, over 80,000 fans passed through the system and were totally unaware of it. Bill Todd, a detective with the Tampa Police Department, who was responsible for crime watch at the Super Bowl said, “The facial recognition technology is an extremely fast, technologically-advanced version of placing a cop on a corner, giving him a face book of criminals, and saying, ‘Pick the criminals out of the crowd and detain them.’ It’s just very fast and accurate.”³⁴

Though Super Bowl XXXV may have been the first location where biometric facial recognition was used at a major sporting event, it is by no means the only place that it can be used. From airports to every location where there is potential for crime or a terrorist attack, this technology can be deployed. In fact, one of the first uses of this technology by law enforcement in New York City was at the Statue of Liberty. David Barna, Chief of Public Affairs for the National Park Service called the technology, “A cost-effective means of improving security at the statue.”³⁵ The list of possibilities goes on to include check cashing and credit card security, which is a major concern throughout the United States due to the onslaught of identity theft cases. Beyond surveillance, facial recognition systems promise to be big security items in personal computers, the Department of Motor Vehicles, security door companies, and automated tellers. Biometric facial recognition technology may even someday be used to prevent auto theft. The possibilities are endless. Someday this same system could be stores as a way to expedite customers through lines while automatically billing them.

Even Rand, who historically has been the arbitrator of controversial issues and rarely takes sides, sees the benefits of facial recognition. Biometric facial recognition systems are described as a tool that can provide significant benefits to society.³⁶ There is no doubt that this technology must be balanced against the privacy concerns of the public, but it has the potential to be a very powerful law enforcement tool that is less intrusive than a fingerprint scan. Society as a whole must decide how to harness the extreme power of this tool, while ensuring that individual freedoms are not completely trampled in the process.

If this technology keeps evolving, there is strong likelihood that officers will have the capability to identify suspects in the field with handheld devices that could be as small as PDAs, thus providing a tremendous in-field tool that they don't have today. If biometric facial recognition is not explored to its full potential, we may have to live with the prospect of a disaster that could have been prevented.

Law enforcement managers not only have the responsibility of ensuring a safe society today, but they also have an obligation to prepare for the safety of society tomorrow. Biometric facial recognition technology may not be the panacea to the countless security issues, but it certainly has the potential to become one of law enforcement's best partners.

ENDNOTES

¹ Night Fell on a Different World. September 7, 2002. The Economist, p.22.

² Ibid.

³ Ibid

⁴ Swanbrow, D. "Homeland Insecurity: Survey Shows Many Americans Still Worried and Shaken." UM News. May 2002. Internet. <http://www.umich.edu/2newsinfo/released/2002/may02/r050302a.html>. Accessed: 10 January, 2003.

⁵ Ibid

⁶ Seffers, G. "How Biometrics Works." Federal Computer Week. April 2002. Internet. <http://www.fcw/articles/2001/0430/pol-biobox-04-03-01.asp>. Accessed: 6, January 2002.

⁷ Reedman, C. Biometrics and Law Enforcement November 2002. Distributed at Biometric Conference, 11 November 2002, Waikiki Beach, Hawaii, (quoted with the author's permission).

⁸ Bonsor, K. "How Facial Recognition Systems Work." Internet. <http://www.computerhowstuffworks.com/facial-recognition1.htm>. Accessed: 16 December 2002.

⁹ Ibid.

¹⁰ "Face Recognition," Gaits Technology . Internet. <http://www.gaits.com>. Accessed 1 March 2003.

¹¹ Ibid.

¹² Ibid.

¹³ "Technology," Viisage. Internet. <http://www.viisage.com/technology.htm>. Accessed: 23 January, 2003.

¹⁴ "Face Recognition," Gaits Technology (Face Recognition) Internet: <http://www.gaits.com/biometrics-face.asp>. Accessed: 23 January 2003

¹⁵ Bonsor, K. How Facial Recognition Systems Work. Internet. <http://www.computerhowstuffworks.com/facial-recognition1.htm>. Accessed: 16 December 2002.

¹⁶ Ibid.

¹⁷ Atick, J. "Biometrics: The Technology Review Ten." An MIT Enterprise Technology Review. January/February 2001. Internet. <http://www.technologyreview.com/articles/tr10-atick0101.asp>.

Accessed: 1 March, 2003.

¹⁸ "Is the U.S. Turning Into a Surveillance Society?" ACLU, Web site. Internet. <http://www.aclu.org/Privacy/Privacylist.cfm?c=39>. Accessed: 1 March, 2003.

¹⁹ Ibid.

²⁰ Ibid.

²¹ Ibid.

²² Matthews, W. "Privacy Still a Priority, Officials Say." Federal Computer Week. July 2002. Internet. <http://www.fcw.com/print.asp>. Accessed. 12 February 2003.

²³ Drummond, D. "Restraints Shelved on Facial-Recognition." The Washington Times. March 2002. Internet. <http://asp.washtimes.com/printarticle.asp?action=print&ArticleID=20020305-14688454>. Accessed: 13 January 2003.

²⁴ *Whaler v. Roe* 429 U.S 589, 605 (1977).

²⁵ Woodward, J. Jr. "Super Bowl Surveillance: Facing Up To Biometrics." Rand Study;Arroyo Center. May 2002

²⁶ *United States v. Dionisio*, 410 U.S 1,14 (1973).

²⁷ "Super Bowl Surveillance," Rand Study.

²⁸ Ibid.

²⁹ Ibid.

³⁰ Swanbrow, D. "Homeland Insecurity: Survey Shows Many Americans Still Worried and Shaken." UM News. May 2002. Internet. <http://www.umich.edu/2newsinfo/released/2002/may02/r050302a.html>. Accessed: 10 January 2003.

³¹ Ibid.

³² Preliminary Report Bill Lockyer, Attorney General, Crime 2002 California: 2003.

³³ Ibid.

³⁴ Bonner, J. "Looking for Faces in the Super Bowl Crowd." Access Control and Security Systems Integration March 2001: v.44 no3 P.1, 14-18.

³⁵ Kilgannon, C. "Cameras to Seek Faces of Terror in the Vistors to the Statue of Liberty." New York Times p.10, May 25 2002. Internet.
<http://www.nytimes.com/2002/05/25/nyregion/25CAME.html>>. Accessed: 16 February 2003.

³⁶ "Super Bowl Surveillance," Rand Study.

BIBLIOGRAPHY

- Atick, J. "Biometrics: The Technology Review Ten". 2001. Internet.
<http://www.technologyreview.com/articles/tr10-atick0101.asp>>. Accessed: 1 March 2003.
- Bonner, J. (2001) "Looking for Faces in the Super Bowl Crowd." Access Control and Security Systems Integration no3, 14-18.
- Bonsor, K. "How Facial Recognition Systems Work." 2002. Internet.
<http://www.howstuffworks.com/facial-recognition1.html>. Accessed: 16 December 2002.
- Drummond, D. "Restraints Shelved on Facial-Recognition." 2002. Internet.
<http://asp.washtimes.com/printarticle.asp?action=print&ArticleID=20020305-14688454>.
Accessed 13 January 2002.
- "Face Recognition." Gaits Technology. Internet. <http://www.gaits.com/biometrics-face.asp>.
Accessed: 1 March 2003.
- "Is the U.S. Turning Into a Surveillance Society?" ACLU, Web site. Internet.
<http://www.aclu.org/Privacy/Privacylist.cfm?c=39>; Accessed: 1 March 2003.
- Kilgannon, C. "Cameras to Seek Faces of Terror in the Visitors to the Statue of Liberty." New York Times, May 25, 2002, p10. Internet. <http://www.nytimes.com/2002/05/25/nyregion/25CAME.html>. Accessed: 16 February 2003.
- Matthews, W. "Privacy Still a Priority, Officials Say." Federal Computer Week. June 2003.
Internet. <http://www.fcw.com/fcw/articles/2002/0729/pol-priv-07-29-02.asp>. Accessed: 12 February 2003.
- "Night Fell on a Different World". The Economist, p.22. 7 September 2002.
- Preliminary Report Bill Lockyer, Attorney General, Crime 2002 California: March 2003.
- Reedman, C. "Biometrics and Law Enforcement; Personal View of the Role that Biometrics May Play in the Near and Long-Term Future of Law Enforcement." Distributed at Biometric Conference, 11 November 2002, Waikiki Beach, Hawaii, (quoted with the author's permission).
- Seffers, G., "How Biometrics Works." Federal Computer Week. April 2002. Internet.
<http://www.fcw.com/articles/2001/0430/pol-biobox-04-03-01.asp>. Accessed: 6 January 2002.
- Swanbrow, D. "Homeland Insecurity: Survey Shows Many Americans Still Worried and Shaken." UM News. May 2002. Internet. <http://www.umich.edu/2newsinfo/released/2002/may02/r050302a.html>. Accessed: 10 January 2003.

“Technology.” Viisage (Face Recognition Advantages), Web site. Internet.
<http://www.viisage.com/technology.htm>. Accessed: 23 January 2003.

Whaler v. Roe 429 U.S 589, 605 (1977).

Woodward, J. Jr., (May 2001). “Super Bowl Surveillance: Facing Up To Biometrics”. Rand Study; Arroyo Center.

United States v. Dionisio, 410 U.S 1,14 (1973).