THE IMPACT OF BIOMETRIC TECHNOLOGY ON A SMALL UNIVERSITY POLICE DEPARTMENT BY 2009

Article

By

Chief Fred D. Hardee, Jr.
California State University
Monterey Bay Police Department

Command College Class XXXVI

Sacramento, California
September 2004

THE IMPACT OF BIOMETRIC TECHNOLOGY ON A SMALL UNIVERSITY POLICE DEPARTMENT BY 2009

In the 2002 science fiction movie "The Minority Report," actor Tom Cruise portrays a police officer who's trying to prevent his own arrest for murder. The movie depicts a futuristic society where the use of biometric technology has run amuck. In the movie, citizens' retinas are scanned anywhere and everywhere they go: in stores, in the street, taxis, subways and even in their own bathtubs. In one unsettling scene from the movie, Cruise's character is barraged by interactive advertising billboards as he walks through a mall. His retina is scanned and his identity is instantly uncovered and a profile is quickly formed. The billboard posts advertisements based on his unique characteristics and background. In this brave new world, a citizen's retina was used as a bar code.

While some may view this movie and biometric technology with skepticism, this technology is gaining popularity in law enforcement for a variety of uses, including the possibility of site security in a university setting.

Overview of Biometric Technology

Biometric technology refers to the automated capture of a person's unique biological data that distinguishes him or her from another individual. Biometrics can be measured in many forms, including fingerprints, voice patterns, iris patterns, hand geometry and facial features. The main reason biometrics works for identification is that an individual cannot control these unique aspects of their biology. For example, a person can't change their fingerprint or the identifying features of their iris.[1]

In a basic sense, there are two phases involved in implementing a biometrics system. The first phase involves having an individual's physiological characteristics

recorded. This can be accomplished by having a fingerprint, iris, hand or face scanned. The data from the scan is converted to a unique template, encrypted, and stored as numerical data. The second phase requires the individual to present his or her unique features (fingerprint, iris, hand, or face) for comparison with the data previously recorded. The system then returns a "yes" or "no" after comparing the presented date with data already on file.[2]

Biometrics can be used in two ways – verification and identification. Verification is the act of authenticating an individual's identity by comparing the biometric data to the data previously on file.[3] This is considered a one-to-one search because it is comparing the information an individual is presenting to the information already on file for the particular individual. In this particular case, there is not a search of an entire database for the unique biometric feature, but rather a verification that authenticates the individual is who he or she claims to be.

Identification is similar in concept to verification, except the presented biometric data is compared to the entire population enrolled in the system via a search of the entire database. This is sometimes referred to as a "one-to-many" search technique because an entire database is searched to match the presented biometric data with information already in the database.[4]

Biometric verification and identification leads to one of three outcomes: a positive match, a false rejection, or a false acceptance. A positive match indicates the person is who he/she says they are. A false rejection occurs when an authorized user is rejected and a false acceptance occurs when an imposter is accepted as an authorized user.[5]

There are a variety of biometric technologies currently available. Some are more

popular and more technologically advanced than others, with the fingerprint being the most common. Other biometric technologies include the iris scan, hand geometry, facial recognition, facial thermography and voice recognition.[6] The technologies are further described as follows:

Iris Scanning Devices: The iris scan operates by using a photograph of an individual's iris. If the iris data matches what is on file, the individual is granted access to the desired event or site. The iris scanner can read through contact lenses, glasses, and most sunglasses. Researchers say the iris is the most unique feature of the human body with 266 measurable characteristics (as opposed to approximately 35 in fingerprints) and does not change over time. They also claim iris scanning is more accurate than DNA testing.

Hand Geometry Devices: Hand geometry is based on the shape of the hand. A device measures finger length, thickness, and curvature. It is used for authentication rather than identification. The data is easier to collect because there isn't a need for good skin contact, which is required to obtain a good fingerprint or the need for special lighting required for retina and iris scans.

Facial Recognition: facial recognition is based on capturing facial images by measuring the curves of the face from various angles and measuring the distance between the features. The image is stored as a mathematical algorithm and can be referenced at a later time to verify someone's identity. Facial thermography is implemented by measuring the heat pattern in a person's face. Manufacturers of facial thermography systems claim the systems can identify individuals despite surgery or facial hair. One major drawback of this technology is that alcohol consumption has a drastic effect on the

accuracy of thermography.

Voice Recognition: Voice recognition operates by translating voice tones into a unique corresponding mathematical pattern. A microphone, sound card, and software are required for implementation.

The Current State of Biometric Technology

Biometrics are used in a variety of ways in the United States. One major use of biometrics is for access to sensitive military agencies, intelligence agencies, and other federal organizations requiring very high levels of security. They are also used for physical access control.

Employee time clocks have even moved into the age of biometrics. A time clock company in Florida that has been selling time clocks and punch cards for 30 years is now manufacturing time clocks with fingerprint reading devices. The devices are called the HandPunch system and essentially they work like this: An employee places a hand in the machine and the device photographs the hand three times, noting its dimensions, such as the length and width of the fingers. Then, every time an employee clocks in or out, he or she places a hand on the reader and the device matches the hand size and shape to the image in its memory. The time is then recorded electronically in the company's computer system, eliminating the need for paper time cards.

At this time, hand readers still have some kinks. Dick Parker, who owns Tampa, Florida-based Edwards Time Equipment, hasn't sold any hand readers yet, but has seen them in action. Parker said the new system takes slightly longer than the old punch card systems. Also, if an employee doesn't place his/her hand on the device properly, it can hang up the process. If a hundred people are waiting to clock in, there will be a wait.

"The biometric systems will be the systems of the future," Parker said. "No one has taken it right now and ran with it that much, but eventually, it will be the system."[9]

Rex Healthcare of North Carolina recently installed 39 HandKey terminals to heighten security for patients and 3,500 employees at its 61-acre main hospital campus. According to Chris Main, Rex Healthcare Director of Protector Services, "We wanted a higher level of security than a badging system or PIN code alone could offer. After much research, we tested and then chose the biometric HandReaders. We started using the HandKey readers where there was a perceived need for a higher level of security in the birth center. The hand scanners are very accurate. No unauthorized person has ever gotten past one."[10] The HandKey hand readers automatically take a three-dimensional reading of the size and shape of a person's hand and identify their identity in less than one second. At the hospital, users enter a PIN code that they select and then place their hand on the reader. The system quickly verifies if the hand presented matches the one associated with the PIN, and if so, permits access. HandKey terminals are now used in the birth center, information technology data center, other major informational technology areas, the operating rooms and the emergency room department.

Public Acceptance of this Technology

When examining the potential use of biometric technology for university site security purposes, it is important to consider the Social, Technological, Economic, Environmental and Political (STEEP model)[11] implications surrounding this technology. Two main obstacles emerge that work against implementation of biometric technology in public facilities: first, the social and political opposition with concerns of

violations of the Fourth Amendment, unreasonable search and seizure, the "Big Brother is Watching" fear, as well as worries personal data will be used for something other than its advertised purpose. Despite the formation of a few advocacy groups, mainly sponsored by biometric device manufacturers, there is still no enforceable guidance concerning the use of biometric devices and data.

Regarding the potential social and political opposition to this technology, many feel that privacy is a personal right.[12] Most individuals desire the ability to maintain some control over their own personal space and to be free of interference from other individuals and organizations. An individual's personal space comes in many forms, including the physical body, personal behavior traits, communication patterns, and personal information. In today's high technology and information age, it is not difficult to collect data about an individual and to use that information to exercise control over the individual. Individuals generally do not want others to have personal information about them unless they decide to reveal it, and individuals are even more leery of third parties who may acquire information without the consent of the rightful owner.

Privacy must be balanced with many competing interests, including the rights of individuals and society as a whole.[13] With the rapid development of technology, it is becoming increasingly difficult to maintain the levels of privacy that citizens knew in the past. Everywhere we turn, data is being collected. With advances in databases, datamining, and telecommunications, it is almost effortless to circulate personal information to any interested party.[14]

For those advocating the widespread use if biometrics, there appears to be numerous advantages to doing so. Biometric supporters say this technology increases

privacy rather than invading it. Many see biometrics as a quality of life enhancement for society as a whole.[15] Some feel biometrics would be a big asset when conducting background investigations to ensure the individual does not have a negative history, particularly in the areas of child abuse and sex offenders.

State welfare programs also fall into the category where biometrics proponents feel the benefits of widespread biometric implementation outweigh personal privacy concerns. In San Diego County, a biometric fingerprint identification system was installed for all welfare recipients. Within the first 18 months of installation, the county paid out $200,000 less than it normally paid out. The department of social services believes the savings is mainly a result of those who were applying (and receiving funds) for welfare under more than one name.[16]

Application of Biometric Technology at California State University, Monterey Bay

There are many uses for biometric technology at California State University Monterey Bay (CSUMB), which is a small university on the Monterey Peninsula. CSUMB currently has approximately 4,000 students with 1,200 students currently living in residential halls on campus. The campus opened in 1995 and its growth has increased by approximately 500 students annually. By 2015, it is projected the campus will have approximately 9,000 students.[17] Security of the dorm rooms, containing both female and male students, is of utmost importance to the students and their parents, as well as the university. While stranger sexual assaults are rare on the CSUMB campus, nationwide, sexual assaults are a concern at any college or university campus. In fact, federal legislation (Clery Act) was enacted in 1998 which requires any college or university with a certified police department receiving state or federal funding to adequately document

and report any and all Part I crimes and to compile and release those statistics annually to faculty, staff, students, prospective students and their parents.[18] This federal legislation was enacted after Jeanne Clery, a student at Lehigh University in Bethlehem, Pennsylvania, was raped and murdered by a sexual offender who gained access to her dorm room while she was sleeping. The suspect gained entry into the residence hall via an unsecured outer door.[19]

Unfortunately, lax site security is commonplace in residential halls in many colleges and universities, and CSUMB is no different. Biometric technology could be utilized at key entry points in residential halls utilizing biometric handreaders. This technology would eliminate any problems with unauthorized entry into the residential halls, thereby enhancing the safety of the students residing there.

Another biometric technology use at CSUMB could be the enhancement of building/classroom security. Currently, the university has a proximity reader alarm system with a magnetic lock at all doors leading to classrooms, administrative offices, meeting halls, lecture forums and all other buildings on campus. The door to these buildings open when an authorized user presents a key fob or alarm card. The issue with this is that key fobs or alarm cards can be shared or provided to non-university students, which can allow an unauthorized access. Biometric technology, specifically hand reader technology, would be an enhancement to the existing system because the system would know specifically who was requesting entry. If an unauthorized person attempted entry into the building that had biometric hand reader technology, entry would be denied.

CSUMB is a computer technology-oriented university. Computer security for information systems that would prevent unauthorized use is another area that could

benefit from the use of biometric technology for identification and verification. An individual could gain access to the university information system and ease the log-on process by providing a fingerprint. Using this concept, when the fingerprint on the mouse or keyboard match the fingerprint that is already on file, the individual is allowed access to the information system.

Because of the challenges facing small university police agencies with limited resources, implementing biometric technology to enhance site security poses great challenges. However, the safety of the students, faculty and staff should be a priority. Biometric technology can enhance site security at CSUMB by not allowing unauthorized access to those who may be looking to commit crimes or prey upon students, faculty or staff.

The best chances to develop buy-in from university wide stakeholders regarding the implementation of this technology rests in an incremental approach to implementation. It is recommended that the first step in the incremental approach would be the installation of biometric technology hand readers in residential halls on the CSUMB campus. Using this strategy as an example for a cost estimate, there are fifteen residential halls on campus housing approximately 1,600 students. Based on the current hand reader technology available, it is estimated the cost to equip each common entrance of the residential hall will be $25,000 per building, totaling $375,000 to equip all residential halls on campus. It is expected this technology will be available and accepted in the next few years in a university setting.

Collaboration and cooperation during biometric technology site security development on campus may reduce privacy concerns expressed by civil libertarian

groups and the students, faculty and staff. Cost concerns of the biometric technology will need to be addressed through annual budget requests, to include seeking out grant funding and collaborative partnerships with private enterprise.

Conclusion

Visionary and pro-active law enforcement leaders always look toward the future, trying to anticipate trends and events that will impact the quality and type of police service they will provide to meet the needs of the communities they serve. The future of biometric technology for site security in a university setting seems almost a certainty. In many ways, it is a natural extension of those universities that currently have proximity cards readers for building and site security; biometric technology will take site security on campus to the next level in the future.

ENDNOTES

---

[1] Curt Blakeney, "Can Biometrics Save the World?" Newsweek Magazine, October 2003

[2] A. Jain, "Biometrics: Personal Identification in a Networked Society." Kjluwre Academic Publishers, 1999.

[3] Kellie Speed, "Biometrics Gain Momentum", Security Magazine. March 2003, 44-45.

[4] Bill Spence, "How is Biometrics Integrated Into Access Control Applications?" Public Venue Security Magazine website, 2003; available from http: www.publicvenuessecurity.com; internet accessed July 7, 2004

[5] S. Lui and M. Silverman, "A Practical Guide to Biometric Security Technology", IEEE Computer Society Magazine, January 2001.

[6] Joseph Campbell, "Government Applications and Operations", Biometric Consortium website, 2004; available from http://www.biometrics.org; internet accessed June 21, 2004

[7] ibid.

[8] Michael Sasso, "New Time Clocks Keep Employees Honest." The online ledger website, 2004; available from http://www.business@theledger.com; internet accessed May 21, 2004

[9] ibid.

[10] ibid

[11] Charles Hill and Gareth Jones, "Strategic Management: An Integrated Approach", 4th ed., (Boston: Houghton Mifflin Company, 1998).

[12] P. Prabhakar, "Biometric Recognition: Security and Privacy Concerns", IEEE Security and Privacy Magazine, Vol. 1, No.2, pp-33-42, March 2003 edition.

[13] ibid.

[14] John Taschek, "An Eye on Biometrics." Available from http://www.eweek.com; internet accessed May 28, 2004.

[15] Gail R. Light, "Security vs Liberty: Weighing the Options." MSU Today; available from http://biometrics.cse.mse.edu; internet accessed June 16, 2004

[16] ibid

[17] CSU Master Plan, available from http://cpd.csumb.edu/master_plan_index.html; internet accessed July 5, 2004.

[18] CSU Monterey Bay annual crime statistics report, available from http://police.csumb.edu; internet accessed May 5, 2004

[19] Security on Campus web site, available from www.securityoncampus.org; internet accessed May 17, 2004.

BIBLIOGRAPHY

Begley, Sharon. "What Price Security?" *Newsweek*, (October, 2003).

Blakeney, Curt. Can Biometrics Save the World? Public Venue Security Magazine website, 2003; available from http://www.publicvenuesecurity.com; internet accessed 7 July 2004.

Blakeney, Curt. Super Bowl, Super Security. Public Venue Security Magazine, November/December 2003, 12-13.

Brin, David. Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom? Addison-Wesley Press, New York, NY, 1998.

Campbell, Joseph. Government Applications and Operations. Biometric Consortium

Coleman, Stephen Ph.D. Solving Cases of Mistaken Identity and More With Biometrics. The Journal. Fall 2002. Computer World.

D'Agostino, Salvatore. Leveraging the Infrastructure, Seeking the Holy Grail of Building Systems. Buildings Magazine, July 2004, 36.

Delbecq, Andre; Andrew Van de Ven and D. Gustafson. Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes. Green Briar Press, Middleton, WI, 1986.

Etzioni, A. "Big Brother or Big Benefits? The Limits of Privacy. New York: Basic Books, 1999.

Hill, Charles W. and Gareth Jones. Strategic Management: An Integrated Approach, 4th ed. Houghton Mifflin Company, Boston, 1998, 5.

Jain, A. "Biometrics: Personal Identification in Networked Society". Kjluwre Academic Publishers, 1999.

Kouzes, James and Barry Posner. The Leadership Challenge. Jossey-Bass Publishers, San Francisco, 1995, 88-94.

Light, Gail R. Security vs Liberty: Weighing the Options. MSU Today; available from http://biometrics.cse.mse.edu; internet accessed 16 Jun 2004

Lui, S. and Silverman M., "A Practical Guide to Biometric Security Technology", IEEE Computer Society IT Pro-Security (January 2001), 27-32.

Prabhakar, P. Biometric Recognition: Security and Privacy Concerns, IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp 33-42, March 2003 edition.

Sasso, Michael. New Time Clocks Keep Employees Honest. They Are Activated Only by One's Hand. The online ledger website, 2004; available from http://www.business@theledger.com; internet accessed 7 Jan 2004

Speed, Kellie. Biometrics Gain Momentum. Security Magazine, March 2003, 44-45.

Spence, Bill. How is Biometrics Integrated Into Access Control Applications? Public Venue Security Magazine website, 2003; available from http://www.publicvenuesecurity.com; internet accessed 7 July 2004.

Taschek, John. An Eye on Biometrics. Available from http://www.eweek.com; internet accessed 30 Jun 2004.