A. Jarvis

BIOMETRIC IDENTIFICATION

FACIAL RECOGNITION, RETINAL IRIS SCANS, DNA, FINGERPRINTING, BRAIN PRINTING, EAR MATCHING, SMART CARDS . . . WHAT'S NEXT?

"As the technology of biometrics grows, so too should the law and policy concerns."John D. Woodward, Jr. Lawyer, Senior Policy Analyst, RAND and former CIA Operations Officer.

Due to the public's earlier reluctance toward biometrics technology, the research and development of the 1970s science has been slow. In recent years, however, the allure of this increasingly diverse technology has become irresistible to law enforcement as well as to increasingly security-conscious businesses. Since the September 11 attacks, the public outcry for better and more universally available identification technology has been significant and civic leaders have responded with legislation mandating not only better security but achieving that result using high-tech biometrics devices in airports and in immigration offices. While the risk of privacy infringement is still the most compelling argument against the widespread use of biometric technology in law enforcement, this view holds less weight today, in light of the recent tragedies.

Proponents of biometric technology feel that education and appropriate policymaking can greatly diminish any lingering concerns regarding the new technology. While this may be the ideal, we must also recognize that there is still an ongoing debate among biometric experts and policymakers about what policies are "appropriate." On one hand, there are people like Woodward, who insist that biometrics is actually privacy's friend because biometrics safeguards information integrity and thwarts identity theft. Others, however, continue to emphasize the possible dangers to privacy associated with the widespread use of the technology. Robert Gallagher of Visionics, maker of facial recognition systems, notes the possibility of people getting unauthorized access to personal data collected with such technology, and of possible misuse of the information. Also, he admits that some technologies are far from infallible. There are still questions as to the devices' accuracy. This article will discuss some of the current uses of biometrics technology and will give a general overview of the big issues involved with its use in law enforcement.

What is "biometrics technology?"

Biometrics technology can be used for either identification or authentication purposes. In general, biometric identifiers can acquire unique biological information from people for the purpose of verifying identity, much like a pin number for an ATM card or a drivers' license functions. The most commonly known method of biometric identification is fingerprint biometrics, which is used by police forces throughout the United States and in more than 30 countries. DNA identification is also a popular and increasingly non-controversial use of biometric technology. Other biometrical methods of identification include retinal and iris scans, hand geometry, facial feature recognition, ear shape, body odor, brain fingerprinting, signature dynamics, voice verification, and computer keystroke dynamics. Fingerprint biometrics and hand geometry systems are among the systems most ready for widespread use by American authorities. Also, facial recognition biometrics are predicted to do well in airport security.

These technologies have many potential uses in the criminal justice system: to enhance access control and identity verification in correctional facilities; as an investigative tool for identifying missing and exploited children as well as criminals captured by surveillance systems. It can accurately identify people when they cash checks, collect welfare benefits, use ATMs, cross borders into the U.S., sign on to computer networks, or enter secure buildings.

Some uses of the technology are not controversial: West Virginia's Missing Children Clearinghouse uses facial identification technology to look for missing children by scanning pictures found on the internet. A major U.S. prison system recently decided to integrate a biometric access control system to help track the movement of prisoners throughout each facility. The access control device can authorize that the prisoner is who he is purporting to be when he/she tries to gain access to another part of the facility through an embedded fingerplate template in the access control unit.

Immigration authorities are testing a similar technology as part of immigration and airport security reform. Most Americans polled after September 11 expressed their approval for the use of biometric technology by the INS and airport authorities to track down suspected terrorists. The terrorist-watch proposals have focused mainly on facial recognition systems and hand geometry, both of which would center on the use of a "SmartVisa" system. The smart card stores the biological information of a particular subject and when the card is swiped at the border, for instance, the device also records the subject's facial characteristics and/or hand patterns on a small metal surface to verify the subject's identity. The technology would also allow us to safeguard against identity theft as well as identifying people on terrorist-watch lists as they move around the world.

Other uses of the technology appear more threatening to the general public. Last year's Super Bowl, a number of U.S. embassies, and the city of Los Angeles are places that have used some form of facial recognition systems. Having their likeness randomly scanned by law enforcement was to many in the general public a clear violation of personal privacy. The public responded with outrage to the camera scanning at the Super Bowl (now known as the "Snooper Bowl"), but its voice was apparently discounted by Ybor City (Tampa) law enforcement. In mid-summer 2001, as a way to deter crime, Ybor City posted signs warning "Area Under Video Monitoring" while 36 surveillance cameras connected to computers randomly compared faces in the crowd to its database of 30,000 images of wanted felons and missing children. Local citizens, the ACLU, and some members of Congress likened the technology to a "virtual lineup." The legal director of the ACLU's Florida chapter, Randall Marshall, questioned the constitutionality of such surveillance operations.

Facial recognition programs have been criticized for their inaccuracies and unreliability. The digitized photographs are highly susceptible to changes in lighting and facial positioning. Also, the system may not pick up a match if the picture in the database is two or more years old since the technology has a difficult time recognizing the effects of aging. Different hairstyles, the addition of facial hair, or glasses may also fool the system. Additionally, the Tampa cameras have not yet caught one suspected criminal or terrorist and have only "made" several false positives, which caused even more skepticism. Of course, proponents of the system, like Detective Bill Todd of the Ybor City Police Department, are convinced that the surveillance is preventing crime by deterring criminals from coming into their city. James Wayman, director of the National Biometrics Test Center at San Jose State University, acknowledges that facial recognition technology is very new and that it is still in its infancy.

Iris scanning is another biometric system that has a great potential for widespread use, but the technology for that systems is still in the testing phase as well. Several sites have been established for testing the technology and many have been quite successful. Iris scans were mentioned as a possible component in the identity cards proposed by the Home Office in the U.K. after September 11. One of the biggest problems with the technology is the variability of the iris, which changes characteristics depending on whether one has been drinking or taking drugs, whether the person is pregnant, and with the variabilities of age in general. Recent reports indicate that the most promising area of research and application with this technology is in financial transactions and for medical record keeping.

A proposed brain fingerprinting system includes a 10-minute computerized security screening to be conducted by each individual every few years to see whether they possess particular knowledge, like how to carry out specific types of terrorist activities. Each person would be given a "security risk profile," which would be stored in a federal databank to be used for authentication purposes at airports and public buildings. The FBI feels that this technology would be very helpful to law enforcement, but the cost of such a system is great and the public fears that this form of biometric technology may be or may lead to the ultimate widespread government intrusion into everybody's lives.

Ear shape and body odors are biometric technologies that have yet to prove their value in the American marketplace. Researchers at the (U.K.) National Training Centre for Scientific Support to Crime Investigation are currently working hard to compile a database of ear images. E-signature systems are also being developed and used in the internet banking and loan business with some success.

In general, the error rate of biometrics devices is relatively low. The systems are susceptible to the same kinds of identification errors as humans, i.e. mistaking a stranger for a known person (false acceptance) or failing to recognize a known person (false rejection). Biometrics researchers are trying to strike a delicate balance between convenience and security with these systems. The systems can be adjusted to reduce false rejection rates, but only at the cost of increasing false acceptance rates. This tradeoff presents various issues unique to the purposes of each system.

The future of biometrics technology: beyond September 11

Legislators and the American public are now embracing the inevitability of biometric technology as a means of preventing future terrorism. According to U.S. Senator Dianne Feinstein (D-CA), "Many experts believe that if we had been using biometrics for visa applicants and visa holders and at customs, baggage and passenger checkpoints at airports, we could have potentially forestalled the September 11 attack." With this in mind, government and aviation officials are considering various proposals that will improve airport security. Several programs are currently being installed and tested in airports throughout the United States.

Biometrics technology has undoubtedly risen in either popularity or acceptability since that infamous day, but many people wonder if our safety concerns fears will be dwindling with the passing of time and if the increased popularity of this historically controversial technology is only temporary. Recent studies find that the opposite is true.

Public opinion was arguably leaning more and more toward acceptance of the new technology even before the September 11 attacks. Financial institutions and the health care industry were integrating these technologies to greater ensure the confidentiality of their dealings well before September 11. The widespread use of biometric technologies in these areas was inevitable and it was forecasted that the public would readily accept these uses, as they are designed to provide more privacy and security to customers and patients. The advent and marketing of identification devices designed to provide the consumer with a more convenient way of identification, such as Microsoft's Smart Card, were also working to familiarize the public with the technology, and continue to do so.

Even if September 11 never had happened, law enforcement uses were just around the corner. Support for these systems was starting to grow before the terrorists struck. There were already biometric programs up and running throughout the United States' criminal justice and correctional systems. The only difference now is that the public is beginning to embrace biometric uses on a much greater scale. The horrors of September 11 appear to cause the public to be willing to sacrifice a little of its precious privacy for the sake of feeling greater personal security.