

Biometrics is formally defined as “the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits” (wikipedia.org), however there is much more to this growing technological advancement in security. Using human characteristics, authentication is tested using various forms of cameras, scanners, and transmission devices.

The earliest form of biometrics still used to today is fingerprinting. It began in the 1300's in China, when it is believed that the Chinese took the children's fingerprints in order to differentiate one from another. Fingerprinting was not widely used again until the 1890's, when it was implemented into the criminal justice system after various other methods of identification were deemed inaccurate. Standard fingerprinting is still used greatly for criminal identification, but thanks to technology, electronic fingerprinting has become widely used for security of all types. Fingerprinting is the least expensive form of electronic biometrics, and therefore many have opted for this fast and easy identification service. For example, for years, many ATM and bank services have implemented electronic fingerprint scanners to not only ease use but also enhance security. All types of businesses, from grocery stores to tanning salons, have implemented fingerprint scanners for these reasons. Of course, businesses have also installed these instruments, along with many other forms of biometrics, in order to keep track of employees and secure information or spaces within an office. Fingerprints remain the most reliable form of identification; the FBI is said to have over 45 million fingerprints on file, much more than any other type of biometrics.

Although it is the most common, fingerprinting is certainly not the only type of biometrics available. Another well known form of biometric security is voice recognition

(also known as voice verification). In order to gain access to whatever the voice verification software is protecting, a user must say a password or pass-phrase out loud into the system through a microphone. The sounds are then separated into tones and compared against the preset password. In the 20th century, voice recognition was originally used as a form of issuing commands. By simply speaking, a person could control a device that was run by a computer. It wasn't until later that voice recognition was used as a form of security. Voice recognition has become more popular because of its user-friendly set up and its low cost. However, this form of security has some drawbacks that make it unreliable. For example, some conditions such as sickness or lethargy could cause a person's tone of voice to change, and therefore access would not be granted to the user. Also, recording a user's voice and playing it back into the microphone could easily give others access to the account.

Iris scanning is another type of biometric security that is helping businesses increase protection. During use of the iris scanning system, a user places his or her eyes within scanning distance of the device (usually between 2 inches and 2 feet). As the iris (which is the colored part of the eye) is scanned, the device compares about 200 different spots in the eyeball to a previously captured photograph of the same person's eye. Patterned lights are also used to prevent someone from using a photograph of the eye, instead of the real thing. Because there are so many points in the eye to test, iris scanning is a very powerful tool for security. The software makes it nearly impossible for an intruder to use anything other than the user's eyes to gain access. Other than cost, there are no major drawbacks to this technology. It is believed that this will be a more

prominently used form of security in the very near future, with some prisons already integrating these systems for prisoner identification.

Another growing field of biometrics is facial recognition. Like other types of biometric recognition software, an image of a face is first captured for later comparison. The main factor that sets face recognition apart from all other types of biometrics is the way in which the images of faces are captured. Unlike iris scanning, a person does not need to volunteer him or herself for scanning. Cameras placed in public areas can easily examine thousands of faces for identification. This is especially helpful in finding missing persons or criminals. Of course, this method also has its drawbacks because of personal privacy. During one incident, Tampa police officers secretly scanned over 100,000 people at the 2001 Super Bowl in Tampa, Florida. Because no criminals were found in the audience, this episode alarmed scores of people and left many questioning this system of security.

A less controversial type of security is the use of smart cards. A smart card is like a credit card, only it is embedded with a microprocessor which can be used for a great assortment of applications. Smart cards were first introduced in the 1970's and were primarily used as memory cards. Smart cards were not widely used until the mid 1990's in Europe, where they were used like a cash card, with the value stored on the internal chip. They were also used widely in France as a form of debit card. To this day, they are still more common in Europe than in the United States. Many Europeans use them for insurance, banking, and simple personal identification. However, smart cards are commonly used in the United States as "SIM cards", the tiny chips found in the back of some cell phones.

Radio Frequency Identification Devices (RFID's) covers a wide variety of security applications. The idea of Radio Frequency Identification Devices was first introduced in the 1940's, but it was not until 1997 that it became widely accepted as a secure method of data transfer and security. With the drop in cost because of the growth of the industry, RFID's became easier to get and to use for all types of businesses. RFID's, along with smart cards and bar codes, belong to a group of technology devices know as Automatic Identification and Data Capture devices. A RFID is a mechanism that stores and transfers information using radio waves. RFID's can be passive or active. Passive means they do not have an internal power supply and rely on some method of retaining power, such as through an antenna. Active RFID's are much more reliable because they hold their own power supply. They also have better signal strength and can hold more information than passive RFID's. There are two types of RFID's: implantable and non-implantable. Non-implantable RFID's are much more common and are seen in every day life. For example, stores often equip their products with RFID tags in order to prevent theft. Toll paying tools (such as the Pennsylvania Turnpikes Easy Pass service) use RFID's to ease travel stresses. The new technology of implantable RFID's has certainly raised some questions about how far people will go to protect their security. These devices were originally designed as animal tracking devices for both pets and livestock, but are now being implanted into humans. This is mostly used for business purposes, usually for those employed by very secure businesses. However, in some countries in Europe these chips are even being used as a form of "VIP card" for night clubs. The most popular form of implantable RFID is the VeriChip. This device was created by VeriChip Corporation and was approved by the FDA for use in humans in

2002. This chip was originally designed for medical reasons to store important information such as medical history and allergies in the case of an emergency. Unfortunately, many hospitals and doctors offices have opted out of using the chip because of privacy reasons. Many people believe these chips invade their privacy because it may give the government the ability to watch them or find them whenever necessary. Also, the chips might store valuable information, and a thief may attempt to kidnap a person in order to retrieve it. However, because of privacy concerns, the chips can also be implanted into jewelry such as a watch, though this would increase the chances of the information being stolen.

The future of biometrics is going to be an exciting one as new technologies are introduced in the world of security. As previously mentioned, as of now the only large database of physical characteristic identifiers is the record of fingerprints. As time goes on, the government and criminal justice system hope to make searchable catalogues of other types of characteristics as well, such as copies of iris scans or facial pictures. Courts and police stations have already begun taking a wider variety of mug shots for the databases to provide more accuracy when searching for people. Of course, in order to better the files of biometric pictures and scans, the way of collecting biometric data is going to have to be improved too, as well as the technologies themselves.

Scientists and technological gurus have already begun the process of producing newer and better forms of biometric security. These upgrades in biometrics will not only help individuals in their daily lives, but also large businesses and even our country as a whole. The House of Representatives will spend around one billion dollars in the next 3 years developing standards for biometrics so that they can become more safe and reliable,

and hopefully also more widely accepted than they are currently. Biometrics are also going to be integrated even more into the United States Homeland Security department and the wars against terrorism and other foreign threats. The United States government already has a database of biometrics having to do with known terrorists in the world, and this is going to need to be improved and enlarged over the coming years. The push for more standards in biometrics has been strong since the devastation of September 11th, 2001. Fernando Podio, program manager at the National Institute of Standards and Technology's Biometric Standards Program, stated that "After 9/11, we championed the successful establishment of national and international standard-development bodies focused on the rapid development of consensus biometric standards." After these standards are all placed into effect more time and money can be spent on the development of new biometric technologies.

The question remains, how technologically advanced will biometrics become? Other than updating and improving current methods of biometric security, there is a large variety of human characteristics that can be tested for security measures. Some of the newest biometrics in testing include body odor and breath recognition. Also, the ways in which biometrics are used will continue to change as our society pushes for more security in every day life.