FUTURE takes
Transcultural Futurist Magazine
ISSN 1554-7744

Vol. 3, no. 1 (Winter-Spring 2004)

Biometrics: A Future Take

by Russell Wooten

Place your hand on an electronic pad to open a door. Log on to your computer by looking into the monitor. Determine the identity of a person from a photo taken 20 years ago. Speak into your car's keyhole to both unlock the door and verify sobriety. You will accomplish all this and more in part through biometric technologies.

Biometric technology makes use of identifying characteristics that are unique to an individual, such as fingerprints, an iris pattern, facial features, voice, or hand geometry. These characteristics can be encoded into software that is installed in a variety of electronic devices, such as computers, scanners, television monitors, and credit-card-size "smart cards."

The science fiction thriller ***Minority Report*** depicted a world in which human identity boiled down to the shape of an eye. Everyone's movements and habits were linked and identified by their unique pair of eyes. Marketing computers scanned people's retinas, so they could identify individuals and constantly offer "the perfect" products and services. The movie main theme depicted futuristic and proactive law enforcement procedures based on this biometric technology.

Today, biometrics are used primarily as a means of controlling access to buildings or computer systems. The technology required to electronically verify biological signatures has become cheaper and easier to use. Research in biological signatures and biometrics is g rowing rapidly.

Biometrics could hold great promise for security, but there are also concerns, exemplified in the movie ***Minority Report***. The hero (a police officer) tries to conceal his true identity from the police by having his eyes surgically removed and replaced with someone else's eyes. This was necessary because a higher-ranking policy official was manipulating the system to frame the hero! The possible theft of fingerprints, retinal or voice print data isn't fiction.

The National Academy of Sciences struggles with the complex and unnerving issues surrounding protection of biometric data, in terms of ensuing both security and personal privacy. They note that the biggest reason biometrics are vulnerable to misuse is that unlike computer passwords or bankcard PIN numbers, they're not secret. Biometrics are unique human qualities that anyone can see and even steal, given the proper tools. For example, an industrial spy could lift someone's fingerprint off a glass or window, much the same way crime scene analysts do, and use the print to gain access to a facility or proprietary information. The financial services industry considers this a major security threat and vulnerability.

In order to ensure thieves can't use biometrics, whether replicated or in real form, the sensitivity of the device reading the biometric data must be increased. In the case of a fingerprint scanner at a cash machine, that might mean requiring the human digit bearing the print to be presented at a certain temperature-specifically, 98.6 degrees Fahrenheit. But what if you are running a fever? Or what if, you need money from an outside cash machine and it is a very cold day in Chicago? Also, if someone were suffering from a cold or laryngitis, it's conceivable a voice reader would have trouble recognizing that person. False readings could trigger frustration, even outright hostility, among those being scanned. It is conceivable that certain legal groups would reject the use of biometrics based on the fact that biometrics are not 100% accurate.

Biometrics also have some innate security features. Guessing a biometric code isn't as easy as guessing someone's password or using a computer program to randomly generate PIN numbers until the right one has been found. In order to use someone's biometric information, a thief would need the original or an exact copy. That's why in addition to the risk posed by someone swiping a fingerprint, there's also a security trapdoor lying in the databases that hold the copies used to validate the real identifiers. If those massive caches were ever compromised the results could be catastrophic.

Gaining access to a repository of biometric data is not only possible, it's conceivably not that hard to do. The best way to keep a database from being hacked is to keep it separated from an electronic network that could be easily accessed. Therefore, as more locations are added to a biometric network, the more vulnerable that network becomes. Hacking a biometric database isn't a major threat right now, because the technology isn't that widely used. But as biometrics systems become more prevalent, the risk will grow. The National Academy of Science recommends that biometrics should not be used for remote authentication; in other words, scans should not be sent over a network and to a central location for validation. That would mitigate the risk of the biometric code being captured in transit.

It would be far more damaging to compromise a database of biometrics than, for instance, a cache of PIN numbers. If PIN numbers are confiscated, they can be canceled, and their owners can choose new ones. But once someone has stolen your biometric signature, we can't just ask you to change it. Anyone who steals the electronic version of a fingerprint or retina has "a digital derivative of your actual, physical being. It can't be replaced.

POINTS FOR THE CLASSROOM *(send comments to forum@futuretakes.org):*

- *What possible implications of biometric technology deployment can you identify? Think in terms of a futures wheel, with "biometric technology deployment" as the event, or try brain-writing if you prefer.*