Technology Update

Note: *The views and opinions in this article are those of the authors and do not reflect an official position of the U.S. government. References to any specific commercial products by trade name, trademark, manufacturer or otherwise do not constitute or imply its endorsement, recommendation or favoring by the U.S. government.*

Biometrics: Separating Myth From Reality

By Allan Turner and Duane Blackburn

During recent years, biometrics (automated methods of recognizing a person based on physiological or behavioral characteristics) have received a great deal of public attention. Since Sept. 11th, interest in biometric technologies to help improve public safety has increased dramatically. The media have reported extensively on the increasing use of biometrics in such diverse environments as airports, banks, defense facilities, casinos and correctional institutions. Additionally, Hollywood continues to sensationalize biometrics in movies and on television. So which pieces of the hype are accurate, and which are not? What does a correctional administrator need to know when considering use of a biometric technology? This article discusses five of the most prevalent myths about biometrics technology today.

Myth No. 1: Biometrics work the way people in the news or in television/movies say it does.

In an effort to present both sides of the story, most news articles show two conflicting positions. Naturally, proponents of the technology overstate biometrics' capabilities while opponents of it understate its capabilities. As with most public debates, the truth is somewhere in the middle of the two viewpoints. One should also be wary of believing that a technology works the same way it is portrayed on television or in the movies. Producers of these clips are much more interested in advancing their storylines or getting a gee-whiz response from the audience than they are of showcasing accurate capabilities of a technology. Although biometric technology can be successfully used for many applications today, the bottom line for correctional administrators is that it is still a maturing technology that has its limitations.

> There is little doubt that biometrics technologies will, over time, result in profound and lasting change in corrections.

Myth No. 2: A person can simply buy a biometric technology, plug it in and it works.

External factors play a huge role in how well a biometric technology will work. Before selecting a technology, the environment in which it could be installed must be thoroughly examined. Questions to ask include:

- What are the lighting conditions (types of light, placement)?
- How many users will there be?
- What are the characteristics of the user (physical abilities, technology-savvy, easy/rough on equipment)?
- Will the device be employed covertly or overtly?
- What is the required throughput rate?
- How much time will pass from initial enrollment to subsequent uses?
- What is the environment in which it will be installed (temperatures, humidity, dust level, inside/outside)?
- How secure must it be?

The National Institute of Justice and the Space and Naval Warfare Systems Center (SPAWAR) are conducting an ongoing biometrics field-test in the Naval Correctional Facility in Charleston, S.C. The purpose is to answer two basic questions: Which biometrics function most effectively in a prison or jail environment? And is further development of existing technologies necessary to meet the special needs of prisons and jails? Thus far, this project has evaluated five different biometrics technologies with mixed results. Consistent with the general consensus of others, the preliminary results obtained in a correctional environment indicate that iris recognition is the most accurate method, while facial recognition produces the most mismatches. This assessment will vary considerably for other applications, even those within corrections. The bottom line is that correctional administrators considering use of biometrics must answer the above questions before selecting any biometric technology.

Myth No. 3: Biometric technology works for everyone.

Not everyone can use a biometric device. Some devices are physical in nature and must be planned for prior to installation. For example, physical laborers who routinely use their hands typically have worn fingerprints and a mute person cannot be recognized using speaker recognition. Other people simply cannot be recognized by some biometric systems. These individuals are sometimes referred to as "goats" of that particular system. Although these numbers are small, they also need to be considered. In addition, physical changes will occur with age or injury. Fingerprints, for example, become harder to read with changes caused by cuts that leave scars. Last, some individuals may simply refuse to use the biometric device for philosophical or religious reasons. The NIJ/SPAWAR research in the Naval Correctional Facility indicated that inmates will actively attempt to disrupt accurate enrollment in a biometric system. Proper training on actual capabilities and limitations of the device and the institution's data security policy will minimize these concerns. Biometric enrollment is not a one-time action. Procedures must provide for periodically updating biometric data for each enrollee.

Myth No. 4: Results from any biometric test can be used to help determine if a biometric is right for an individual.

A biometric device is not a computer mouse — it cannot simply be plugged in and expected to work at any location for any related purpose. Selection of a biometric technology or vendor is application-specific. What is by far the best selection for application X may be a terrible selection for application Y, even if the two applications seem somewhat similar. The article, "Evaluating Technology Properly — Three Easy Steps to Success," published in the July 2001 issue of *Corrections Today*, provides several ideals to follow when evaluating technology and the three different types of evaluations. Correctional administrators must understand that it is only by following these evaluation ideals and performing all three types of evaluations that they will be able to select which biometric type and vendor are best for their application, assess how well it will work and assess the impact of the technology insertion on daily operations.

Myth No. 5: Data exist regarding using biometric technology for specific applications, with straightforward performance statistics.

Biometric technology is still very much an emerging technology. As such, most individuals familiar with it have a scientific rather than an operational background. More operational users have become interested in the technology since 2001, but both sides are still learning to effectively communicate with each other. The good news is that NIJ is heavily involved in bringing technologists and corrections practitioners together to discuss these issues, as well as performing well-documented evaluations. This helps the technology mature as well as develop a corrections knowledge base for future installations.

Biometrics was named one of the top 10 technologies that will change the world in the January 2000 *MIT Technology Review*. There is little doubt that biometrics technologies will, over time, result in profound and lasting change in corrections. At a minimum, correctional administrators must stay well-informed as biometric technologies evolve. The ability to separate myth from reality is critical.

To learn more about biometrics, visit the *Biometrics Catalog* at www.biometricscatalog.org. The catalog, a federally funded database provided as a service of NIJ, was developed for the biometrics community and potential users of biometric technology. It was designed to provide multiple search options so visitors can find the information they want — and only the information they want — quickly and easily. Adding a posting to the *Biometrics Catalog* is free and encouraged. The catalog also provides an introduction to biometrics and information on evaluating biometrics.

Allan Turner, DPA, is a research professor at George Mason University in Fairfax, Va., and a visiting scientist at the National Institute of Justice's Office of Science and Technology in Washington, D.C. Duane Blackburn is a program manager for the National Institute of Justice and the Department of Defense Counterdrug Technology Development Program Office in Dahlgren, Va.

Reprinted from the December 2002 issue of *Corrections Today*, Vol. 64, No. 7 with permission from:

FOUNDED 1870
The American Correctional Association, 4380 Forbes Blvd., Lanham, Maryland 20706