

“The Human Factors Involved When Implementing A Biometric System-Part I”

Now that, you as the owner of your business, have looked into the business and technical factors involved in implementing a biometric system and have examined various alternatives such as Single Sign On or Multi Modal Solutions, there is another very important aspect you need to take into consideration-how your employees will react to the implementation of a biometric system. This can also be referred to as the “Human Factor” component of biometric technology.

There tends to be a certain apprehension, fear, and hesitation among people when they found out that they will become a part (enrolled and verified) of a biometric system at their place of employment. Many of these fears stem from the issue of privacy rights. Of all of the technologies available today, biometrics has been the most scrutinized with regards to privacy rights. This article is a two part series. The first series will look at the Human Factor issues, you the business owner, could face as you implement a biometric system. The second series will examine how these issues can be overcome.

In our culture, the respect for privacy is one of the core values that we possess. Therefore, when you implement a biometric system, the first line of concern you, as the business owner, will face from your employees is how their privacy rights will be affected at the workplace. So, it is important that you understand why privacy rights is such a hot topic with the use of biometric technology.

First, when anybody is scanned by a biometric system, for a brief moment in time, that individual is actually giving up a part of their physical, biological attributes-such as a fingerprint, facial image, or iris and retina structure. The fear is that these physical attributes that are scanned by the biometric system will be stored somewhere in a “black box” without the knowledge of the user. This ambiguity leads to further fear about the possible theft of these physical attributes. Whenever anybody loses or forgets their PIN Number or password, they could very easily be reset. But one of the main fears and concerns with biometric technology is that if these physical attributes are stolen, there is nothing you can do to change, or “reset” your physical attributes in question. After all, you cannot change the physical structure of your finger or your eye. As a result, this leads to feelings of loss of control and autonomy.

Second, privacy rights issues also stem from two other main areas of concern:

(1) The release of biometric data to various third parties; and (2) Private information which could be obtained from the physical characteristics scanned and gathered by the biometric system. With the former, the fear is that the physical characteristics obtained could be shared with many other third parties in a manner very similar to purchasing or selling mailing lists. Currently, there is no legal environment or legal precedent to govern the privacy rights regarding biometric data that is gathered. In this context, “. . . the technology is fast and the law is slow” Source: 1.

With regards to the latter, the fear is that the physical characteristics obtained by the biometric system will be used by law enforcement on a much grander scale than it is used right now. For example, there is a large scale fingerprint database maintained by the government-called the Automated Fingerprint Identification System, or AFIS. This database contains fingerprints of wanted criminals-although this database is used to track down known or suspected criminals, the fear is that this database has the potential to be expanded to include other physical traits. Also, there is the fear that the physical characteristics captured could reveal other private information about a person-such as their medical condition: "... recent scientific research suggests that fingerprints and finger imaging might disclose medical information about a person." Source: 2

All of these issues regarding privacy rights have led to an umbrella fear of "Big Brother" watching over you. That is, the government keeping tabs on the people via the physical characteristics gathered from the biometric system. The concern is that the government will use biometric technology for covert purposes without the consent of the people. With the heightened state of terrorism, the topic of a National ID Card system-which would contain biometric data-has received a lot of attention, both here in the U.S. and Europe (especially England). While the intention of the National ID Card system is to have a means of positively identifying people, it has met very stiff resistance because of the fear of "Big Brother" watching over your shoulders.

Additionally, there have been objections to biometric technology based on both philosophical and religious grounds, such as the "Mark of the Beast", and that biometric technology is nothing but a form of tattooing at a technological level. Your employees could raise objections because they may feel that they are forced to wear this type of tattoo, without having a choice in the matter. There have been many advances made in identification technology, such as the miniature chip that can be surgically implanted in your skin. As a result, this has only fueled the stigma of "Big Brother" even more.

There are also a number of other key issues and objections that will probably be brought up by your employees as the biometric system is being implemented. One of these is the concern if people could contract any sickness from using a biometric system, or if the biometric system itself could cause any sickness or injury. For example, if you have many employees, there could be concern that any sick employee could leave their germs on the biometric system, and thus transmit their sickness to other employees as they interface with the biometric system. Also, it is a part of human nature to become very defensive when something is pointed at your eyes. This is the case with eye-scanning biometrics. If you are implementing an iris scanning system, the biggest objection will be if the iris scanning device itself will cause any damage to the eye, cause blindness, or exacerbate further any eye ailments.

Finally, fingerprints have long been associated with law enforcement, and identifying criminals. As you implement a biometric system, especially a fingerprint system, there could be a feeling of the "presumption of guilt" association among your employees. This association could lead to a fear of unreasonable search and seizure in the workplace, as well as the freedom of movement being heavily restricted upon.

Our next article, “The Human Factors Involved When Implementing A Biometric System-PartII”, will examine how you the business owner, can address the fears and concerns brought up in this article.

Also, please note that the next article (Part II) will conclude our series on biometric technology. Our next series of articles will examine security on different applications and areas.

- (1) “Biometrics: Identifying Law & Policy Concerns”, John D. Woodward, Jr. Article is from the book: "Biometrics: Personal Identification in Networked Society", By Anil Jain, Ruud Bolle, and Sharath Pankati. P. 392.
- (2) “Biometrics: Identifying Law & Policy Concerns”, John D. Woodward, Jr. Article is from the book: "Biometrics: Personal Identification in Networked Society", By Anil Jain, Ruud Bolle, and Sharath Pankati. P. 393