

Towards Privacy Enhancing Applications of Biometrics

BY C. MAXINE MOST

Many people consider the widespread use of biometrics to be at least mildly disconcerting – a cross between 1984 and Minority Report. They imagine a world in which biometrics are integrated with massive centralized database applications designed to track and monitor our every move.

This indeed would be a frightening and menacing nightmare. In reality, the prospects are not quite so ominous.

These classic Big Brother scenarios represent the worst-case application of biometric technology. They have more to do with repressive government and the wholesale disappearance of civil liberties than with the actual use of these identification technologies. This is not to say that these fears are completely unwarranted. In the wrong context, biometrics could contribute to invasive, inappropriate and authoritarian identification systems. But the same can be said of computers, mobile phones, credit reports and even supermarket discount cards. The use of biometrics, however, engenders greater fear because



of the intimately personal nature of the data. The question to consider is how can privacy rights and civil liberties of individuals not only be maintained but be directly enhanced by the widespread deployment of biometrics.

Separating the Database Issue from the Technology Issue

One of the issues that seems integrally linked to biometrics is the deployment of massively integrated databases. It is extremely important to recognize the potential this approach has to create a surveillance society that is totally at odds with any sense of personal liberty. However, it is not the biometrics that makes this dangerous but the database linking itself.

In a recent letter to the International Civil Aviation Organization (ICAO), more than thirty human rights and civil liberty organizations worldwide expressed their mounting concern that plans for integrating biometrics and smart cards into passports and other travel documents (along with air passenger data transfer) constitutes the initial stages of “a larger surveillance infrastructure (for) monitoring the movement of individuals globally”. The most significant concerns, however, were in regards to centralized databases in combination with the establishment of standards for this still emerging and clearly fallible technology. The letter did mention that the local storage of biometrics, for example on a personally owned smart card was in fact not problematic. It is likely that even without the biometrics, this organization ought to be voicing their opposition to the use of centralized data storage and monitoring of passengers. Their base objection is to the surveillance capability not to promoting the verification of identity technology as a means to improve travel security. This distinction is important.

Verification versus Identification

In general, the use of biometrics to verify a claimed identity engenders less passion-

Guidelines for the Privacy Enhancing Application of Biometrics

- Separate centralized database issue from biometrics applications – massively interconnected, centralized digital databases are scary even without biometrics
- Keep storage of biometrics separate from personal data – If personal data must be linked use a distributed network computing approach.
- Local storage of biometrics on personal devices (i.e. smart cards) should be used whenever possible
- Non-repudiated anonymous identification is powerful privacy enhancing application of the biometrics.
- Biometrics should be applied as a means of protecting the privacy of an individual when bridging the human-machine identity gap.
- Privacy enhancing biometric applications should be designed to reduce the collection and processing of other personal data – name, address, sex, marital status, etc.
- Biometric matches or failures to match should always be verified through a human process so as not to falsely deny access to – physical or logical – or accuse any individual.
- Security measures must be taken when biometric data is processed – enrolled, stored, transmitted, extracted, template generation, matching.
- Enrollment processes must include an initial authentication process that prevents the linking of a forged identity to genuine biometrics.
- International standards must be developed in conjunction with data protection authorities.
- Clear and binding legislative/regulatory frameworks are required to ensure appropriate use of biometrics technology.

ate debate and poses significantly less of a threat to personal privacy than the use of the technology to identify an individual from some pool of known individuals – i.e. citizens, criminals, frequent fliers, etc. Using biometrics to confirm that an individual is who they claim to be does not require massive centralized databases or a link to volume of personal data. An individual must simply match a real-time biometric reading with one that has been previously validated, processed, encrypted and stored.

The least invasive way of doing verification is to store an individual’s biometrics on a personal device such a smart card, token, or PDA. Verification can then be based solely on matching a live biometric to one stored in the personal device. The biometric data is never stored in either a local reading device or a centralized database

and remains personal property, owned and managed by an individual.

Anonymous Identification

In regards to biometric identification, it is critically important to understand that it is possible to apply this technology in such a way that the privacy of the individual who supplies the biometric data is actually greater than if biometrics were not used at all. Biometrics can enable truly anonymous identification in a completely privacy enhancing way. Two currently active deployments illustrate this possibility.

The first is an iris recognition application on the Pakistan – Afghanistan border. In many ways this is a most unlikely environment for the application of advanced technology, a relatively remote location with limited electrical power and temporary building facilities (i.e. tents.) In this case, the United

Nations High Commission on Refugees (UNHCR) is using biometrics to confirm that each Afghani refugee returning home from Pakistan receives only one refugee care package. The UNHCR captures a digital image of each refugee's iris and stores it in a large database designed for one to many searches prior to distributing any benefits. This enables the organization to anonymously identify each individual who has collected benefits and prevents would be double dippers from passing through the UNHCR distribution point. The beauty of this application is that absolutely no other personal information or documentation is required in order for the UNHCR to confidently control refugee benefit distribution.

A similar outcome is achieved through the EU's EURODAC AFIS fingerprint system as applied to asylum seekers. In this case, the EU is concerned with providing fair and equal treatment of all asylum seekers and preventing fraudulent duplicate asylum applications. According to EU policy, an individual seeking asylum must apply once and only once to the first EU Member State they enter. However, given the open borders policy of the EU and the lack of a centralized asylum seekers' registry, many individuals routinely filed multiple applications. Upon rejection of a claim, applicants would simply move to another EU Member State and begin the asylum process again. The proliferation of multiple applications was diverting resources away from new applicants, creating an undercurrent of fraud and increasing the costs of managing and administering these programs.

In 2003, the EU deployed a centralized Automated Fingerprint Identification System (AFIS) database for asylum seekers. This centralized database has enabled government officials to determine – during

the interview process- whether or not the individual they are interviewing has submitted a prior application in any EU Member State. As with the UNHCR example, the only information contained in the database are fingerprints. No other personal information is required

Each of these applications is based on a centralized database where one to many searches are performed. However, because the biometric data is stored independently of any personal information or links to any personal information, it increases rather than diminishes the privacy of the individuals applying for and receiving aid. The database application simply returns a hit or no hit response indicating whether or not a given individual's biometrics reside in the database. This anonymous identification scenario can be used for many similar types of benefits or welfare programs as well as for checking against criminal or terrorist watch lists at borders or ports in a way that enhances rather than diminishes the privacy of the individuals required to furnish their biometric.

Function Creep

One of the biggest privacy fears is that biometric data will be subject to the same kind of function creep that has made the Social Security number the defacto identification number in the US for everything from library cards, to bank accounts, health records and retail incentive programs. There is no question that commercial enterprises in particular will be tempted to link volumes of personal data to biometrics which left unregulated could lead to re-use by unauthorized third parties for their own purposes. This scenario is even more frightening in regards to government agencies where this third party spillover might well lead to use by various branches of law enforcement and justice organizations.

One of the best ways to combat this type of privacy threat is to create a legal framework and a systems architecture that from the initial stages is designed to thwart this

kind of use and abuse. In this regard use of the Social Security number is an excellent example of an identification scheme that was never actually thought of as an identification scheme and was therefore not subjected to the rigorous legal and systems analysis required to safeguard against function creep.

Is Big Brother Watching?

It is true that no technology is infallible. Errors abound in the world of digital data and malicious sabotage in the form of viruses, worms and compromised security systems is an almost daily occurrence. While this tends to lend credence to the argument that further exacerbating the situation through the use of biometrics is a move in the wrong direction. However, there is a tremendous opportunity to use this highly personal data to decrease rather than increase numerous threats in the real and virtual worlds. Biometrics can provide a key to lock information in such a way that only the rightful owner has the ability to unlock it. Biometrics can provide a non-reputable audit trail that may indeed prevent unauthorized access and use in a way not previously possible.

The bottom line for biometrics, as is true with many new technologies, is that the technology itself is neutral. Though biometrics are unique in their intensely personal nature, they can be used well or they can be used poorly. The challenge is to define the constraints in a way that from both a legal and operational standpoint they are truly designed well. Then biometrics will serve the interests of privacy, not violate them. ■

C. Maxine Most is the Principal of Acuity Market Intelligence (www.acuity-mi.com), an emerging technology market research and analysis firm and the Editor of Biometrics Market Intelligence (BMI) (www.biometricsmi.com), a quarterly report providing market insight and analysis for the biometrics industry. For more information Ms. Most may be reached at cmxmost@acuity-mi.com.