Biometric Technology in Driver Licensing

Guest Column by Ian Williams

An advocate of dignified secure human identification, articles relating to Ian's position on privacy and biometrics have appeared in *Business Week, Interactive Week, Biometric Digest, Biometric Technology Today* and the *Canadian Broadcasting Corporation production Undercurrents*.

Biometric technology is a useful tool in preventing identity theft, and ensuring that an individual securely accesses their personal privileges. Two years ago my daughter received as a gift an electronic portfolio that would open only for her. This toy used speech recognition, to prevent others from accessing her personal items. My daughter quickly learned she could protect her personal information with something that was unique to her, a biometric. Increasingly in Canada, everyday applications, including banking and e-commerce are using biometric technology; people embracing the benefits it offers and providers recognizing the technology as a privacy enhancement.

Biometric technology, defined by some as "automatically recognizing a person using distinguishing traits", was gaining popularity in identification applications prior to September 11th. A reason often cited was the need to ensure that a person could enroll for a benefit or privilege once only, using a single identity. An additional element of security added to a token or identification card, ensures that the person who claims a privilege is really the person entitled to that benefit. At the same time it ensures that an individuals' privileges will not be attained through identity assumption by modification to the original document.

The two scenarios above translate into what is commonly termed in the biometric community as either a ONE: MANY or a ONE: ONE comparison. To put these into a driver licence perspective, consider the following: Have I been issued a driver licence before, perhaps under a different name? The first scenario would then compare my biometric data against all other previously issued records, comprising the ONE: MANY aspect of identification. The second scenario, being a ONE: ONE, and as an example possibly at an airport counter, a comparison to see if I was indeed the person this driver licence was issued to, thus entitled to a privilege by authentication.

Various Biometric Technologies

There are about eighteen various biometric technologies. Some are well known and actively used. Others such as Unique Body Odour, Vascular Pattern and Gait are not. Of these technologies Finger Imaging, Facial Recognition, Iris Scanning, Retina Scanning, Hand Geometry, Voice and Signature Dynamics are leading.

Within the technologies mentioned above there are added considerations for decision. Facial recognition, for example, may involve another three sub categorical approaches. Some facial vendors use a physical geometry method of analysis on the facial features, others use an Eigenface approach which places each face into one of eight basic structures then studies characteristics, and others offer facial thermography which measures the relative heat patterns in the facial tissue. Finger imaging is no different, with some vendors applying optical technology to scan, others offering sound wave scanning, and many applying different extraction algorithms and binning techniques to improve search results.

With all these choices how can one make a qualified decision on a biometric technology for a jurisdiction? Which technology should be used? Which is the most accurate? What is the cost? Will the information be exchanged with other jurisdictions? Will political acceptance be possible?

Choosing a Biometric Technology

Many factors need to be addressed when choosing an appropriate biometric for an identification application enhancement. The four main factors are: accuracy, effort, intrusiveness and cost.

Accuracy – There simply is no point in implementing any biometric technology that will be used if it does not provide accurate results although studies have shown that biometric systems appearing to be "used" can deter the number of attempts at misuse even if they are not operational. Accuracy is key.

Effort – If the system continually requires modifications, operators will quickly tire and results will decline. If the enrollment process is too cumbersome, operator buy-in will not be achieved. From an end-user perspective, if the enrollment process is time-consuming and difficult the end-user may be dissatisfied and form a negative opinion affecting the success. Motor vehicle administrators are all too familiar with the issue of "long lines at the DMV".

Intrusiveness – This is probably the most important deciding factor, particularly for Canadians. If the system is seen as privacy invading or encroaching, public sentiment may cause the demise of the program. Any biometric system involving the public-at-large has to offer security and enhanced privacy. Certain biometric technologies are seen as being

Back to Contents

connected to law enforcement, others may be perceived as capturing more than required. However, there are demonstrated approaches that can alleviate public fears and show that the technology can be applied in a privacy conscious manner. Successful marketing may play a key role.

Cost – It was for a time, just a driver licence, now it's used for everything. Prior to September 11th, we really only dealt with individuals holding multiple driver licences to evade suspensions and bans or to commit fraud and theft. Today national security must be considered in determining an appropriate cost to implementing an improved identification system.

Other Factors

Interoperability – Some may want this, others may not. You may ask, why not? Several years ago I consulted on the design of a biometric identification system for a large metropolitan Canadian city that was trying to reduce welfare fraud. In this particular application, the government agency planned to collect biometric samples for the purposes of evaluating entitlement to welfare benefits. The system ultimately designed used standard biometric technology, which was modified such that the resultant stored biometric data did not match that in use by most police forces and therefore could not be exchanged or used in any comparison. The modifications ensured that the biometric sample could only be utilized for the purposes for which it was obtained. This perspective is currently incorporated into a European Union (EU) directive regarding the collection and dissemination of biometric data.

However, there are some benefits to jurisdictional exchange, and others may wish interoperability. There are several initiatives underway to allow jurisdictions the ability to exchange and compare data. The American Association of Motor Vehicle Administrators (AAMVA) has incorporated a Fingerprint Minutiae Template Standard as part of their latest Driver Licence Standard. The US based National Institute of Standards and Technology (NIST) has a Biometric Interoperability Workgroup that is researching methods of exchanging biometric data not only within a specific technology but also between systems using different technologies.

Where Do I find Information?

A great source of information is the Biometric Consortium website: www.biometrics.org. This website is the defacto source of information regarding biometric technology, and since it is government sponsored, it tends to be technology and vendor neutral.

Another source is the San Jose State University, where the US National Biometric Research Center resides. Led by Dr. Jim Wayman, many government bodies request testing of biometric technologies and devices for appropriate use in public sector applications. Additionally, the US Department of Defense conducts assessments of biometric technologies and offers these reports via their website: **http://www.dodcounterdrug.com/facialrecognition**.

Another source for information is the United Kingdom Biometrics Working Group which provides details on the process one should undertake when evaluating a biometric collection device. This document can be found at the following: **http://www.cesg.gov.uk/technology/biometrics**.

Summary

Adding biometric technology to the driver licence application will be a serious challenge for most Canadian jurisdictions. Careful planning and research will be a prerequisite before any decisions can be made. Additionally, buy-in at a public and political level will be essential to the success of the project. Consideration in deploying a biometric enhancement may be made by applying the technology as a voluntary enrolment initially, in order to gain public acceptance.

The main obstacles to a motor vehicle administration considering biometrics might not be the technologies, but overcoming media scrutiny and obtaining public approval. A jurisdiction that includes privacy and security designs as their primary objectives may have a better chance of success.

Remember, biometric technology is a useful tool in securing an identity and ensuring that a person and only that person can access their secured privileges. Privacy and security are the reward when used appropriately.

Back to Contents