Identity management and the application of biometric technology

Anne Trimmer, Minter Ellison[*]

Anne Trimmer is a partner at Minter Ellison in Sydney.

With the adoption of biometric technology for passport security, it is timely to consider whether there is a wider application of biometric technology in enhancing security for online banking and in the regulation of money laundering in Australia.

Biometrics is a generic term that refers to various means by which biological data can be measured and used for the purposes of identification and authentication. The most popular forms of biometric identification are retina scans, hand geometry, thumb scans, finger prints, voice recognition and digitised photographs. Recent media reports have also suggested that ear scans might be an accurate biometric measure. The use of biometrics is not new - the signature has been used for authentication purposes for a long time, as have fingerprints.

Biometric technology can be a convenient and secure mechanism for authentication of parties when conducting a transaction using a variety of service channels (eg. in person, by telephone, or online).

Biometric technology might act as an aide in enhancing security for online banking and against money laundering for several reasons, including:

- it operates as a privacy enhancing technology (PET) to promote an environment of trust and security among internal and external users of financial services;
- the high levels of authentication offered by biometrics satisfy an organisation's need to know who it is dealing with and mitigates against identity theft and fraud;
- it provides an audit trail; and
- existing methods of customer authentication are limited to a range of details that are provided by the customer but can be known, and used, by others.

The retention of personal data in computerised systems has led to the growing phenomenon of identity theft. This occurs where hackers gain access to the confidential details of potentially millions of people and utilise that information to initiate fraudulent transactions, complete an identity theft or simply on-sell that information.

A significant and costly problem arising in the context of identity fraud is 'phishing' via internet banking. Phishing involves the use of spam email to deceive customers into disclosing personal financial information including credit card numbers, bank account information, social security numbers, passwords and other confidential information. Customers receive emails from scammers masquerading as banks, requiring them to validate or to update their details on apparently legitimate websites.

Current procedures to curb the substantial losses sustained through identity fraud include the use of smartcards, public education into credit card fraud, and mechanisms for simply limiting access in particular websites. Biometric technology has been given increased attention as a mechanism to bolster the security of internet banking where a form of biometric data is used in conjunction with cards or details to gain access to bank accounts. Several large Australian banks have announced an intention to trial small 'proof of concept' identity management systems within the next two years.[1]

One bank executive commented that it is an area in which collaboration should be promoted, and not one that should be used to generate a competitive advantage for any particular bank.[2] Providing a biometric identification tool to every internet user is estimated to cost $700 million[3], though the devices will only be provided to a select number of individuals in trials. The implementation of such a system may prove to be uneconomical if the costs of implementation greatly exceed the losses sustained from phishing.

Apart from economic considerations, there are, of course, significant privacy issues that need to be considered under a biometric regime. A person's biometric data, once collected, is personal information contained in a record and must be managed in accordance with the *Privacy Act 1988* (Cth) and in particular the National Privacy Principles. Potentially the biometric data might also be used in legal proceedings and investigations.

While biometric technologies have the potential to be PETs, they are also perceived by many privacy commentators to be privacy invasive technologies (PITs). The former Privacy Commissioner[4] has concluded that the impact of biometric technology on an individual's privacy will depend on the way in which biometric systems are constructed and whether privacy issues (such as choice, openness and accountability) are built into the system at an early design stage.

Whether raw biometric data is 'personal information' for the purposes of the Privacy Act is uncertain. Personal information is defined as *information or an opinion (including information forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion.*

Without the necessary technology to read biometric data, a person's identity may not be ascertainable from raw biometric data, especially if it has been converted into digital form. Therefore, the question as to whether a biometric constitutes personal

information for the purposes of the Privacy Act may depend on who has possession of the biometric data and that person's capability to read it.

This issue has been considered by the Privacy Commissioner, who concluded that even though the use of biometrics generally involves a number of transformative processes that involve the manipulation of data, for example, the mathematical transformation of the information into an algorithm code, there is no reason why the digital representation of human characteristics (the biometric) would not remain personal information in most, if not all, stages of the processing and storage of that data.[5]

One argument in favour of applying biometric technology is that it can assist with requirements for authentication and non-repudiation. Authentication is the process for achieving certainty in the identity of the other party to a transaction, relying on one or more of the following:

- something you know (eg. a password or a PIN);
- something you have (eg. a smart card or hardware token); and
- something you are (eg. a biometric).

The application of an authentication process to an electronic (or other) transaction is designed to protect the integrity of dealings and to avoid unintended consequences such as an incorrect transfer of funds or the improper collection, alteration or disclosure of information. Biometrics can be a powerful form of authentication of parties to a transaction because of their uniqueness. It has uses not simply in the identification of an individual but as a means to verify a person's eligibility to access a service, particularly in online transactions.

Non-repudiation is an objective of authentication, with the aim of providing irrefutable evidence that an action took place. It is meant to protect one party to a transaction against a denial that a particular event took place and to protect parties from a false claim that a record was tampered with, not sent or not received. The risk is that, if something goes wrong, the individual will not be able to repudiate the transaction or repair the situation.[6] An organisation using biometrics for authentication and non-repudiation purposes needs to implement a process by which an individual can challenge a transaction, but not to the extent that the high level of authentication offered by biometrics is undermined.

Furthermore, the use of biometrics in identity management technologies can be used advantageously in limiting access to data centres and web-based resources, preserving the privacy of consumers. This has particular ramifications in relation to bank phishing. Biometric technology has the added requirement of a person being physically present for authentication, unlike conventional password or identification card systems where that data can be exchanged easily and entered through remote access.

A problem however lies in the permanent nature of biometric identification. Whilst passwords and pins can be regularly altered and updated, a person's physical make up is largely incapable of drastic modification. The accidental release or theft of such information can have even more severe consequences for consumers than conventional security measures, simply due to the inability to substantially modify biometrics. This potential danger however can be prevented by ensuring all data is encrypted and not provided in raw form. At the same time, any scanning recognition systems must be flexible enough to cater for slight changes in physical structure, and yet be conservative enough not to generate false acceptances.

A privacy risk raised by any inaccuracy inherent in the collection of biometric information through false acceptances or false rejections may corrupt personal information. An organisation using biometric information must anticipate that this may occur and develop mechanisms to allow it to correct the problem. False acceptances can lead to unauthorised access and the perpetuation of identity fraud, whilst false rejections will lead to inconvenience and irate customers.

As with other security systems, there is also concern over the theft and misuse of biometric information, particularly in the context of bank phishing. For example, fingerprint images are converted to approximately 40 unique points of the finger which are then encrypted and stored on a computer system, and the original fingerprint image is discarded. At this stage, it is said that it would not be possible to reverse-engineer those points into a fingerprint or to match the points of the finger to the owner.[7] Databases may incorporate algorithms that can only be generated from the original image. Ultimately, the effectiveness of the systems will depend on the manner in which the data is stored and the mechanisms for retrieving that information.

While biometric technology has significant capabilities as a PET, there is scope for it to function as a PIT, as biometric data may be retained for purposes other than identification and authentication. The information may reveal particular physiological or genetic conditions, potentially threatening a person's privacy. Medical information may be derived and subsequently used in identifying particular groups as target markets or result in discrimination[8]. This is an example of 'function creep'[9], where biometric data collected for a stated purpose is subsequently used or disclosed for an alternative purpose without the knowledge and/or consent of the individual. This issue may be addressed through the appropriate encoding of raw data such that the additional information can no longer be discerned.

Other concerns include the means by which biometric data may be obtained. Unlike credit card and bank account applications where consumers consciously submit their details and elect passwords, biometric data can be obtained covertly without a person being aware that that information is being collected. This may compromise their privacy and their desire for anonymity. The Privacy Commissioner however has stated that measures in the Privacy Act, the Information Privacy Principles and the National Privacy Principles will adequately protect against this.[10] They prohibit the covert collection of such information and require an organisation to take reasonable steps

to inform a person that such information is being gathered.

The Biometrics Institute has submitted a draft Privacy Code[11] for approval by the Privacy Commissioner with the intention of facilitating the protection of identified information provided by biometric systems and to promote biometrics as privacy enhancing technologies. The Principles in the Code provide for the appropriate collection, use, disclosure and maintenance of biometric data. The main limitation imposed on organisations collecting such data is that it must be done in a fair and lawful manner and must be necessary for the performance of its functions or activities though there is scope for this to be modified. Ultimately, biometrics presents as an appealing security tool, although its success depends on the establishment of appropriate control regimes.

This article is based on one originally published in Technology News, a client newsletter of Minter Ellison.

---

* This article was written with the assistance of Li Yen Chen.

1 see Australian IT, *Westpac mulls bio-banking*, 16 September 2005, http://australianit.news.com.au/common/print/0,7208,16622385^16123^^nbv^,00.html (last viewed 5 December 2005)

2 Connors, E. and Moullakis, J., *High-tech blitz on bank fraud*, The Australian Financial Review, 16 September 2005, p 1

3 ibid

4 Former Privacy Commissioner Malcolm Crompton, *Biometrics and Privacy, The End of the World As We Know It or The White Knight of Privacy?*, Biometrics Institute Conference, Sydney, 20 March 2002, p 2

5 ibid, p 15

6 ibid, p 11

7 Chu, K., *Will that be cash, credit – or finger?*, USA Today, 12 January 2005, http://www.usatoday.com/tech/news/techinnovations/2005-12-01-cash-credit-finger_x.htm?csp=N016 (last viewed 5 December 2005).

8 Prabhakar, S., Pankanti, S., and Jain, A., *Biometric Recognition: Security and Privacy Concerns*, IEEE Security & Privacy, March/April 2003, p 41

9 as defined in the Biometrics Institute: Draft Privacy Code.

10 Former Privacy Commissioner Malcolm Crompton, *Biometrics and Privacy, The End of the World As We Know It or The White Knight of Privacy?*, Biometrics Institute Conference, Sydney, 20 March 2002, p 9

11 Draft Privacy Code of the Biometrics Institute, http://www.biometricsinstitute.org/associations/4258/files/Biometrics%20Institute%20Privacy%20Code%20Revised.doc (last viewed 5 December 2005)