TRENDS & ISSUES
in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 324 September 2006

Identification systems: a risk assessment framework

Russell G Smith

Identity-related crime affects all sectors of society - and robust measures are needed to guard against its increase. There are various mechanisms used by organisations to verify the evidence of a person's identity and an important goal is to ensure that any system is as effective and efficient as possible. This paper provides a framework for assessing the competing factors that decision makers need to address when determining the effectiveness and efficiency of any proposed identity checking system. Ten groups of factors are identified, against which each system can be assessed, and a framework for quantitative analysis is provided. The adoption of any given solution must be driven by an objective assessment of evidence relating to all of these factors – not solely those governing technical performance measures.

Toni Makkai
Director

Identifying people with certainty is time consuming and costly for public and private sector organisations. Each year in Australia, government agencies need to identify approximately half a million new Australian residents, 2.5 million enrolment forms are processed by the Australian Electoral Commission, the Australian Taxation Office issues almost half a million new tax file numbers, Centrelink grants 2.8 million new claims for benefits, and the Department of Foreign Affairs and Trade issues over one million travel documents (websites listed in references). On each occasion, evidence of identity is required.

In addition, millions of people every day logon to computer networks, for work, to withdraw cash from automated teller machines (ATMs), or to use the internet for recreation or business. In 2005, the Reserve Bank reported that there were 772 million ATM withdrawals and 1,176 million electronic funds transfer at point of sale (EFTPOS) transactions in Australia (APCA 2006), each of which required customers to identify themselves by entering a personal identification number (PIN). There are also millions of occasions each year on which individuals need to be identified for access to buildings, travel purposes, and proof of age for purchasing alcohol and cigarettes.

Failure to have effective means of identification creates opportunities for criminal activity. It has recently been estimated that identity-related fraud alone cost $1.1 billion in Australia in 2002 (Cuganesan & Lacey 2003). This paper provides a framework for evaluating three principal approaches to identifying people for government and business purposes.

The 100 point system

The 100 point system of identification, which operates throughout Australia, relies on people submitting documents for inspection at government agencies or financial institutions. Each document is assigned a value depending upon its level of security. Primary documents (which carry 70 points each) include certificates of citizenship, passports, and birth certificates. Secondary

ISSN 0817-8542

ISBN 1 921185 19 8

GPO Box 2944
Canberra ACT 2601
Australia
Tel: 02 6260 9272
Fax: 02 6260 9293

For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: http://www.aic.gov.au

Project no. 0040

documents include drivers' licences (40 points), public employee or student ID cards (40 points), credit cards (25 points), Medicare cards (25 points), and council rates notices (25 points). There is a range of other documents that can be used to verify name and address, each carrying different numbers of points. At present under the Financial Transaction Reports Regulations 1990 (Cth), 100 points of documentation are required to open an account with a financial institution as well as for establishing identity for the most secure forms of electronic communications with government.

Biometrics

In recent years, biometric technologies have developed as a means of identifying people. Biometrics has been defined as 'the automated means of recognising a living person through the measurement of distinguishing physiological or behavioural traits' (Great Britain. Biometrics Working Group 2002: 4). In other words, biometric systems are based on who people *are*, rather than what they *carry with them* such as a card, or what they *know*, such as a password. Whether by fingerprint, voiceprint, iris or facial pattern, it is possible to measure individuals' physical attributes to help to identify them. In Australia on 24 October 2005, a biometrically-enabled passport was made available in which the personal information currently recorded on the passport is kept on a computer chip embedded in the centre pages of the document. Already some 2,500 e-passports have been issued, and trials are being conducted involving airline staff and some others to enable them to use facial recognition technology in conjunction with the e-passport to proceed through customs controls at airports (Nash 2005).

Identity cards

A third approach is to issue people with identity cards. It is now possible for plastic identity cards to contain a computer chip to hold personal data more securely than with ordinary magnetic stripe cards, which are vulnerable to compromise through skimming. To provide a further layer of security, computer chip cards can be activated through the use of a PIN, or even a biometric authentication system.

A number of countries issue compulsory identity cards, some of which include a biometric identifier. Hong Kong, for example, has developed multi-use ID smartcards which contain basic biometric information such as thumb prints and a photograph, and are capable of multiple functions including use as drivers' licences and as library cards (Benitez 2002). A pilot program for a biometric ID card has been implemented in Britain for asylum seekers (McAuliffe 2002). In Britain, financial institutions have also issued chip/PIN cards which must be used after 13 February 2006 when making card transactions.

Enrolment and matching

Each of these systems involves the use of two processes: enrolment and matching. In the enrolment phase, an individual's identifying information is acquired for the first time. Biometric images are converted into a template, against which subsequent comparisons are made. In the case of the 100 point system and identity cards, identity is checked against previously registered data held on databases of issuing agencies, or on a card which may or may not be secured by a PIN or other security measures. The Australian Government is currently implementing the National Document Verification System which will improve this process.

At present when people seek to carry out transactions, they simply produce their card, state their name or provide a signature. This can then be verified against previously held data. In the matching phase of a biometric system, an individual's biometric characteristic is captured again. This live template is compared against previously enrolled data, seeking a match. In the matching phase of a card-based system, the cardholder simply presents the card for matching against a variety of characteristics such as signature, photograph, or PIN (in the case of chip cards). Matching cards, of course requires the cardholder to hand over the card physically or at least to present it for scanning (for example in Hong Kong's transport system). Combinations of systems can be used, with matching undertaken in a series of steps from the simplest, such as checking a photograph, to the most complex such as occurs with biometrics.

Choosing the best approach

The ways in which these three systems can be evaluated differ depending upon the particular type of technology and security measures used, as well as the purpose for which the system is being used – whether for identification or for surveillance/watch list checking. The choice of system will depend on the particular needs and priorities of the organisation, including the location and purpose of the system, and the number and nature of the people who will be using it.

From the existing literature, it is possible to identify ten key groups of factors that policy makers need to assess when deciding whether to implement any particular solution to deal with identity-related crime (Table 1).

For each of the 34 considerations, it is possible to rate their effectiveness, which represents a balance between their benefits (the extent to which the system will overcome the problems sought to be addressed), and their harms (negative consequences associated with their introduction). Systems can then be compared in terms of a mean benefit/harm value determined using the following formula:

$$v = \frac{\sum(w(b) \times s(b))}{\sum(w(h) \times s(h))}$$

where: v = value
b = benefit
h = harm
w = importance weighting (1–5)
s = significance score (1–5)

Table 1: Evaluation criteria for identification systems
Enrolment
failure to enrol
false enrolment
Matching
failure to acquire
false match
false non-match
false accept
false reject
equal error rate
Efficiency
enrolment speed
matching speed
data overload
Data security
portable medium
database
Spoofing
artificial identities
relay attacks
database attacks
Privacy
no consent
function creep
unauthorised data matching
User acceptance
links to police
links to criminals
health and safety
Rectification
inability to rectify
cost
time to carry out
Cost
infrastructure
implementation
recurrent
Displacement
spatial
temporal
target
tactical
offence
perpetrator

To calculate the mean benefit/harm value for each identification system, a weighting is assigned from 1 to 5 according to the importance of each of the 34 considerations in terms of benefit (e.g. 5 = greatest benefit) or harm (e.g. 5 = greatest harm). A score is then assigned from 1 to 5 to determine the significance of the consideration, again in terms of both benefit and harm. Significance means simply the extent to which the system succeeds in achieving its objectives or the extent to which harms arise. Weighting values are multiplied by score values for each consideration, and the mean for each identification system is calculated. This will vary from 1 (least effective) to 25 (most effective).

When undertaking any such assessment it is important to compare specific rather than general approaches. Clearly, it would be inappropriate to compare biometric systems as a whole, in view of the widely differing performance of specific technologies. For example, comparisons could be made between the 100 point system used to open bank accounts; facial recognition biometric systems such as that being implemented by the Australian Customs Service; and the use of a computer chip identity card with PIN authentication. Confining the discussion in this way would permit greater comparability without the introduction of confounding factors. Ideally, assessments of this nature would draw on the results of empirically-based research, and/or be undertaken by informed stakeholders in the provision of the systems in question. The primary arguments applicable to each group of factors follow.

Enrolment

Each system requires users to identify themselves upon enrolment. At the outset, it is important to bear in mind that the ways in which identity is established under the 100 point system will still be required for biometric and card-based systems, although the electronic capture of a biometric image can be accomplished in seconds as opposed to the lengthy process of issuing and activating a card. Appropriate evidence of identity is required under each system, and may include background checks with referees or interviews. The integrity of any system is only as good as the quality of the enrolment data provided. Two primary measures of performance on enrolment are the failure to enrol rate, which measures the proportion of users who, for some reason, cannot enrol in a particular system, and the false enrolment rate, which measures the extent to which users are able to enrol using a false identity. A further measure concerns users who may be prevented from enrolment due to other impediments such as cost or disability.

Matching

The performance of matching processes can be measured in a variety of ways. Matching of identity cards raises few difficulties as cards are simply issued to eligible people, who can present them for matching when required. Difficulties will arise where those required to check photographs or signatures fail to do so either through lack of time or neglect. Chip/PIN cards involve certain performance issues which arise in common with biometric systems. The following measures can be used to assess matching performance:

- failure to acquire rate – where the system cannot acquire an image of sufficient quality for matching
- false match rate – where a sample is falsely declared to match the template of another person
- false non-match rate – where a sample is falsely declared not to match the template of the user who provided the sample
- false accept rate – where an impostor is falsely accepted by a biometric system
- false reject rate – where a genuine user is falsely rejected by a biometric system

- equal error rate – the point at which the false reject and false accept rates are equivalent.

It should be noted that while these measures are widely used in the biometrics industry, their use is not always consistent. Evaluations are also often carried out within the industry promoting the technology in question, casting doubts on the objectivity of some reports. This makes it vital for policy makers to inspect any evaluation report closely before accepting its results.

Efficiency

An important consideration for all identification systems is their ability to be used by agencies to deal with large numbers of individuals quickly. It is possible to assess speed in a number of ways. These include looking at the time taken to enrol a person, to acquire their characteristics, to verify information provided, or to conduct the matching process. Biometric systems vary considerably in relation to their processing speeds, although they are invariably quicker than manual processing of individuals in the 100 point system or when using plastic cards. Where systems fail for some reason, however, considerable time may be taken to rectify the problem. The problem of data overload also needs to be considered prior to implementing an electronic system on a national scale.

Data security

Data in both biometric and card-based systems can be stored in two ways. When cards are employed to verify individuals, biometric systems seek to compare individuals' recorded characteristics, such as their facial image, directly with a template recorded on the card or other *portable medium*. In this case, defeating that medium's security features may allow replacement or alteration of the template, unbeknown to the system administrators. For facial recognition, this might be as straightforward as photo substitution or as complex as cracking strongly encrypted data held in a chip/PIN card system. Even theft of card stock from manufacturers represents a risk for plastic card-based systems.

If, on the other hand, the comparison is with a template held on a *central database*, that database could represent a high-profile target for criminals. Securing that information, for example using public key encryption, and ensuring inside parties are not able to gain access to, and alter information inappropriately, represents a major challenge. Large-scale information databases have been defeated recently by outsiders and insiders alike. In the United States in May 2005, for example, the processor of payment card data, CardSystems Solutions Inc, had its database breached and credit card account information including magnetic stripe data and cardholder names relating to over 40 million accounts were stolen. Over 130,000 Australian cardholders were affected as a result (Krim & Barbaro 2005). With established databases there is also an ongoing need to cleanse the data to ensure that the information recorded about individuals is correct. Some changes that occur may be legitimate, such as changes of name on marriage or through formal change of name procedures, but others are not.

Spoofing (counterfeiting)

All three systems are susceptible to spoofing or compromise through counterfeiting or deceiving the security measures in question. Sometimes this may simply entail the theft and use of legitimate identifiers. In the case of card-based systems, circumvention entails an individual acquiring the required card by stealing or purchasing a legitimately manufactured card, or forging a copy. The ease with which cards can be counterfeited depends on the nature of the card, and any security features (such as holographic images) that have been incorporated. Although the use of such security features may make it more difficult to defraud card-based systems, advances in computer technology usually make it possible for a determined identity thief to bypass even the most secure systems.

In the case of chip cards, counterfeiting requires that the chip's encryption be defeated, which is beyond the ability and resources of most criminals. A simpler approach to defeat a chip card activated with PIN, is to ascertain the PIN. This may be learnt directly from the user or the user may be tricked into revealing it through social engineering. Alternatively, it may be guessed or cracked through the use of computer technology, or may be obtained through practices such as shoulder-surfing (where a person entering their PIN into a machine is watched) or by searching through rubbish for relevant information.

In the case of biometric systems, there are three main ways in which a system can be attacked (Thalheim, Krissler & Ziegler 2002). The first involves the creation of an artificial biometric by putting artificially created data into the regular sensor technology of the system. For example, a photograph could be used to deceive a facial recognition system. For this approach to work, it is necessary for imposters to obtain a copy of the biometric that they wish to use such as by taking a photograph of the person to be imitated. The problem of displaying this to the sensor in public then also needs to be addressed.

The second, known as relay attacks, involves the use of artificially created data. Instead of obtaining the relevant data by copying the biometric to be used, this method involves capturing the relevant data as they are input into the sensor, through use of a device such as a sniffer program, perhaps attached to a computer's USB port. The data captured can then be replayed to deceive the system. In 2002, a researcher at the Australian National University demonstrated how fingerprint verifiers could be circumvented in this way (Baker 2002).

Thirdly, there are database attacks which seek to compromise the databases in which the data are stored. This will usually need to be done by someone who has administrator rights over the database, although it could be done through hacking. One way such an attack could take place is where an individual who works on the development of the system forges user data that are reactivated at a later date to their advantage.

In developing technologies, however, manufacturers have attempted to create countermeasures, the most common of which is known as liveness testing. This ensures that the biometric characteristic being measured belongs to a live person. For example, facial recognition systems may require evidence of eye movements or the use of temperature sensors. Such systems have dual advantages in that they can help to prevent spoofing, as well as potentially preventing some forms of crime displacement (see below).

Little research has measured the ability of systems to repel concerted attacks. Facial recognition systems, for example, have yet to be tested against people seriously motivated to evade detection through prosthetic and cosmetic adjustments to their facial shape and size. Indeed, partial facial transplants have recently been performed which could affect template matching. In one study conducted by three German researchers, efforts were made to spoof a number of different biometric systems (Thalheim, Krissler & Ziegler 2002). While some caused slight difficulties, with a little persistence each biometric system investigated was compromised.

Privacy

Recording personal information and its retention in large databases raise some privacy concerns. While some have claimed that biometrics can be a privacy-enhancing technology (Clarke 2006), there is a general perception that such technologies invade privacy. The widespread implementation of identity cards or biometrics systems is opposed by advocates of privacy who raise the grave consequences of information being misused, such as occurred during the Nazi regime in the Second World War.

Some of the main privacy concerns affecting both biometric and card-based systems include fears that information will be gathered without permission or knowledge, or without explicitly defining the purpose for which it is required; that information may be used for a variety of purposes other than those for which it was originally acquired (function creep – a particular problem with government issued cards of various kinds); shared without explicit permission; or used to track people across multiple databases to amalgamate information for the purpose of surveillance or social control (United States. General Accounting Office 2002).

Any use of such systems needs to comply with privacy principles and privacy legislation (Crompton 2002). In the case of biometrics and chip/PIN identity cards, additional measures may be needed to mandate the use of specified levels of encryption for the capture, storage and transmission of data, to limit database matching except under close scrutiny by independent observers, to prevent the reconstruction or retention of the original biometric sample from encrypted biometric information, and to prevent comparisons with reproductions of biometric information not obtained directly from individuals. Some of these aspects may require amendments to privacy legislation, although simple verification checks with issuing agencies are unlikely to cause concern.

User acceptance

Experience has shown that efficiency and accuracy, particularly of biometric systems, can be reduced if those required to use the system are not willing to accept the technology. Some people may find the process of providing personal information in public distasteful. This was one reason given for the reluctance of retailers to make use of a cheque fraud prevention initiative which required customers to leave their fingerprint on cheques before they would be accepted by retailers (Pidco 1996). Similarly, users may associate fingerprints with policing and criminality and feel reluctant to use fingerprinting systems. Still others may believe that systems which scan irises or retinas may harm their eyes, despite clear evidence to the contrary. In the case of identity cards, citizens of some countries may feel less inclined to accept them than others, particularly when health information is included. Accordingly, the need arises to educate users about the reasons the system has been introduced and how it might benefit them.

Rectification

Another problem associated more with biometrics than identity cards is that once a system has been compromised, it may be difficult to rectify the problem. While a new card or PIN can always be issued (albeit sometimes after considerable effort), new facial images cannot, although it is possible to correct the information on databases. Even if the enrolment process remains error-free, a biometric is effectively a 'PIN you can never change', and compromised once, is compromised for all time.

Cost

Costs involved in the implementation and use of each system vary widely, and both biometric and chip/PIN systems have extensive initial implementation costs, including transitional costs from legacy systems. It is important to consider recurrent costs, which can often outweigh the costs of infrastructure and initial implementation. In evaluating systems, it is important to examine these different cost considerations separately, and to conduct evaluations of recurrent costs once implemented.

Displacement

Finally, the use of any highly secure identification system as a crime reduction strategy carries with it the risk that displacement may occur. If it is assumed that offenders act on the basis of some rational calculation in which they balance up the likely risks and benefits from a potential course of conduct, then as some types of crime are seen to become too difficult to commit, other, easier targets may be considered (Smith, Wolanin & Worthington 2003).

In the case of biometrics or chip/PIN cards, this could result in offenders obtaining access to computers through bribery or coercion of IT personnel, or forcing users under threat of violence to disclose their PIN or to permit the offender to have access by presenting their biometric under duress. This has already been seen with duress being used by offenders against users at ATMs to compel them to withdraw cash. In some countries, failure to comply has even resulted in victims being killed.

Conclusions

In deciding whether to implement different types of personal identification systems, policy makers need to ensure that the new technology achieves its intended security aims and does not make matters worse – either generally or by way of displacement or other unintended consequences. An example of how this might take place is the creation of the Access Card Consumer and Privacy Taskforce to address consumer and privacy issues related to development of the government's proposed Health and Social Services Access Card (www.humanservices.gov.au/access/consumer_privacy_taskforce.htm).

Careful thought needs to be given to what technologies cannot do. Of greatest importance is the fact that they cannot validate identity upon initial enrolment. If checks are not in place to validate the evidence of identity produced at enrolment, then the subsequent use of a biometric authentication system may make identity crime easier to perpetrate, and more difficult to detect.

Also of importance is the need to balance the evidence that exists in support of, and against any given system in relation to each of the various considerations outlined above. Policy makers should avoid the temptation to focus solely on the seemingly convincing evidence of technical performance provided by the industry concerned. Technical performance is only one criterion, and even this can be measured in a wide range of ways. Instead, evidence about the range of other legal, social, and ethical considerations governing the use of any given system needs to be sought out and scrutinised. Unfortunately, it is these aspects which have yet to be fully researched.

Acknowledgements

Former AIC analysts Jamie Walvisch, Dr Yuka Sakurai and Stuart Candy contributed research for this paper.

References

All URLs were correct at 18 July 2006

Australian Payments Clearing Association (APCA) 2006. *Payment statistics* http://www.apca.com.au/

Baker L 2002. Rule of thumb: don't rely on new security systems. *ANU reporter* 33(9) 7: 1

Benitez MA 2002. ID card contract awarded. *South China morning post* (Hong Kong) 27 February: 2

Clarke R 2006. Smart cards and biometrics: is a nightmare-free Australia card feasible? Presentation to ACT Society of Technology and the Law, Canberra, 23 March http://www.anu.edu.au/people/Roger.Clarke/DV/ID-ACTSTL-0603.html

Crompton M 2002. Biometrics and privacy: the end of the world as we know it or the white knight of privacy? Paper presented at Biometrics-Security and Authentication Biometrics Institute Conference, Sydney, 20 March

Cuganesan S & Lacey D 2003. *Identity fraud in Australia: an evaluation of its nature, cost and extent*. Sydney: SIRCA

Great Britain. Biometrics Working Group 2002. *Use of biometrics for identification and authentication: advice on product selection*. London: Biometrics Working Group http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricsAdvice.pdf

Krim J & Barbaro M 2005. 40 million credit card numbers hacked. *Washington post* 18 June

McAuliffe W 2002. Asylum seekers get first UK biometric ID cards. *ZDNet Australia* 5 February

Nash B 2005. Utilising the latest in biometrics technology to enhance your forensic capability. Paper presented at the IIR conference, Combating identity fraud, Sydney, 1 November

Pidco GW 1996. Check print: a discussion of a crime prevention initiative that failed. *Security journal* 7: 37–40

Smith RG, Wolanin N & Worthington G 2003. E-crime solutions and crime displacement. *Trends & issues in crime and criminal justice* no. 243 http://www.aic.gov.au/publications/tandi/tandi243.html

Thalheim L, Krissler J & Ziegler PM 2002. Body check: biometric access protection devices and their programs put to the test. *c't magazine* (Germany) no. 11 May http://www.heise.de/ct/english/02/11/114/

United States. General Accounting Office 2002. *Technology assessment: using biometrics for border security*. GAO-03-174. Washington DC: GAO http://www.gao.gov/new.items/d03174.pdf

Websites

Australian Electoral Commission
http://www.aec.gov.au/

Australian Taxation Office
http://www.ato.gov.au/

Centrelink
http://www.centrelink.gov.au/

Department of Foreign Affairs and Trade
http://www.dfat.gov.au/

Department of Immigration and Multicultural Affairs
http://www.immi.gov.au/

Dr Russell G Smith is Principal Criminologist at the Australian Institute of Criminology.

General editor, *Trends & issues in crime and criminal justice* series: Dr Toni Makkai, Director, Australian Institute of Criminology, GPO Box 2944 Canberra ACT 2601
Note: *Trends & issues in crime and criminal justice* papers are peer reviewed.

The AIC is a statutory body with a Board of Management comprising Australian, state and territory government representatives, administered under the *Criminology Research Act 1971*.