

BIOMETRIC SOLUTIONS TO IDENTITY-RELATED CRIME EVIDENCE VERSUS POLICY

Russell G Smith
Australian Institute of Criminology

Conference paper presented at:
Delivering crime prevention : making the evidence work
Carlton Crest Hotel, Sydney
21-22 November 2005



Australian Government

Australian Institute of Criminology



Crime Prevention Division
Attorney General's
department of nsw

This conference was organised by the Australian Institute of Criminology
in conjunction with the Crime Prevention Division of the New South Wales
Attorney General's Department.

<http://www.aic.gov.au/conferences/2005-cp/>

Note: copyright for these papers/speeches rests with the authors and the AIC accepts no liability for the material contained within them. These papers/speeches are not peer reviewed and in particular, speeches may not necessarily meet the standards of the AIC's formal publication series. Their presence on the AIC website should not be constituted as an endorsement of the views contained within them.

**Australian Institute of Criminology and
Crime Prevention Division, Attorney-General's Department, New South Wales
*Delivering Crime Prevention: Making the Evidence Work***

**Carlton Crest Hotel, Sydney
21 November 2005**

**“Biometric Solutions to Identity-related Crime: Evidence versus Policy
Russell G. Smith**

Introduction

Identifying people with certainty is both a time-consuming and costly activity for public and private sector organisations. Each year in Australia, government agencies need to identify and record approximately half a million new Australian residents (including births, permanent new arrivals and long-term visitors), 2.5 million enrolment forms need to be 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. On each occasion, evidence of identity is required.

Millions of people every day also log-on to computer networks, for work, to withdraw cash from Automated Teller Machines, 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 EFTPOS transactions in Australia, each of which required a customer to enter a PIN (Australian Payments Clearing Association 2005). There are also millions of occasions each year in which individuals have to be identified for access to buildings, travel purposes such as air, train, bus and tram travel, collection of highway tolls, and use of retail customer cards in shops and businesses.

In order to identify oneself, it is usual to produce or disclose something that you *have* (such as a card or other token), something that you *know* (such as a password or PIN), something related to *who* you are (such as a fingerprint or other biometric), or something indicating *where* you are located (such as an address or phone number). Of course, there are others, such as the use of a person's name, and a variety of behavioural and psychological characteristics that can be used to identify people. Depending upon the degree of certainty with which one needs to establish a person's identity, one or more of these various methods may be relied upon. Often only one method of information will be used, although so-called 'two-factor authentication' is now becoming the standard. Each, however, has its own vulnerabilities and risks, which are able to be exploited by those who want to act illegally.

Identity-related Fraud Risks of Knowledge-based and Token-based Systems

Recently, however, reliance on simple knowledge-based and token-based systems have created many opportunities for fraud. In the news media, reports regularly appear of credit card numbers and other personal information being taken from databases and misused. 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 and Barbaro 2005).

Cases continue to come before the courts of fraud facilitated through the misuse of computer passwords, and fraudulent identities have also been involved in the commission of a wide range of other criminal activities including obtaining finance dishonestly, opening bank accounts in false names, money laundering, car re-birthing, credit card skimming, obtaining family allowance benefits, obtaining security guard licences and shooters' licences, avoiding driving demerit points and producing TOEFL Certificates for immigrants. It has recently been estimated that identity-related fraud cost \$1.1 billion in Australia alone in 2002 (Cuganesan & Lacey 2003).

The precise way in which identity-related fraud is perpetrated, and the ease with which it can be carried out, will depend on the type of authentication system that is in place. In particular, it will depend on the nature of the data which are associated with individuals, and how easy they are to obtain and/or replicate. For example, to defeat knowledge-based systems it is necessary for an offender to ascertain and use the piece of information that the user knows (password). This information may be learnt directly from the user (who may share their password with friends or co-workers, or be tricked into revealing it through 'social engineering'), may be guessed or 'cracked' through the use of computer technology, or may be obtained through practices such as 'shoulder-surfing' (where an individual watches a person entering their password or PIN into a machine) or 'dumpster-diving' (where an individual searches through a person's rubbish for relevant information).

Different challenges are faced by those who seek to defraud a token-based system. As such systems rely on the association of people with a physical object, circumventing them will generally require an individual to acquire the required token. This can be done either by stealing or purchasing a legitimately manufactured token, or forging a copy. The ease with which such objects can be counterfeited will depend on the nature of the object, and any document security features (such as holographic images) that have been incorporated. Although the use of such security features may make it more difficult to defraud token-based systems, with advances in computer technology it is usually possible for a determined identity thief to bypass even the most secure systems and counterfeit documents containing the appropriate security features (Smith 1999). Even if documents cannot be successfully counterfeited, it may still be possible to buy or steal them.

Biometric Authentication

Due to the vulnerabilities of knowledge-based and token-based systems, a number of organisations and government agencies are moving to 'biometrics'. The United Kingdom Biometrics Working Group (2002, p.4) define biometrics as 'the automated means of recognising a living person through the measurement of distinguishing physiological or behavioural traits'. In other words, biometric systems are based on who a person is, rather than what a person has or what he or she knows. Whether by fingerprint, voiceprint, iris

pattern or a number of other characteristics, it is possible to measure individuals' personal attributes to help identify them. In Australia, for example, on 24 October 2005, a biometrically-enabled Passport was first made available in which the personal information currently recorded on the passport is now kept on a computer chip embedded in the centre pages of the Passport. Already some 2,500 e-Passports have been issued, and trials are being conducted involving airline staff and some others which enable them to use facial recognition technology in conjunction with the e-Passport to proceed through customs controls at airports (Nash 2005).

Biometric systems entail two processes: enrolment and matching. In the enrolment phase, an individual's biometric characteristic (such as a fingerprint) is acquired for the first time. The image acquired will usually be converted into a 'template', against which subsequent comparisons are made. In the matching phase, an individual's biometric characteristic is captured again. This 'live template' is compared against previously enrolled data, seeking a match. The key question for biometric systems operating in verification mode is 'are you who you claim to be?'. Other issues arise in the contexts of using biometrics for identification and 'watch list' checking, such as for border control and immigration purposes.

Evaluating Biometric Systems

The ways in which biometric systems can be evaluated differ depending upon the particular type of biometric technology to be tested, as well as the purpose for which it is being used - whether for identification or surveillance. No single test has been developed which can accurately measure all issues across different biometric devices, in a uniform way. Because of this multiplicity of ways in which biometric systems can be evaluated, it is not readily possible to determine which is the 'best' biometric, because some systems will perform well on one measure, but will be outperformed on others. The choice of which biometric system to deploy, if any, 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.

Policy makers are faced with a wide range of considerations when deciding whether or not to implement biometric solutions to identity-related crime. On the one hand, policy makers must evaluate a considerable and ever-increasing body of technical evidence relating to the performance of biometric technologies, while on the other hand a range of social, legal, and practical considerations need to be addressed including privacy, data security, user acceptance, and cost. Compelling evidence of performance should not, however, overwhelm these non-technological considerations. There are nine key issues to consider.

Enrolment

At the outset, it is important to bear in mind that the traditional ways in which identity is established will still be required during the enrolment phase. A person's biometric does not, by itself, provide evidence of identity: 'biometric systems can only confirm or

determine a claimed identity – one established upon a system at enrolment – as opposed to revealing a “true” identity’ (International Biometric Group 2003, p. 17). To this end, it is important to ensure that appropriate identification documents are still provided, and background checks made prior to enrolment as the integrity of a biometric system is only as good as the quality of the enrolment data (Dunstone 2003). If care is not taken in the enrolment phase, it will continue to be possible for a person to defraud the system, defeating the purpose for which biometrics are used.

Moreover, a real danger arises if a person can successfully bind their biometric data to a stolen identity, because this will allow them to continue using the stolen or fabricated identity for a variety of fraudulent purposes, with little risk of detection. It will generally be accepted that because a person can provide a biometric that matches the assumed identity, they must be that person. This may have a significant detrimental effect on the person whose identity has been stolen, and can take a long period of time to correct.

Some of the most difficult issues relate to the creation of databases of personal information, and the enrolment of individuals within them. The techniques of deception often reach back to the very creation of the records entailed in a system of identification. If a false identity can acquire the trappings of legitimacy from the very start, it makes a much more effective tool for the identity fraudster, being practically impossible to detect.

With established databases, such as those held by the Australian Taxation Office or state offices of Births Deaths and Marriages, there is an on-going 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. Others, however, are dishonest. In Australia, the Report of the House of Representatives Standing Committee on Economics, Finance and Public Administration (2000), *Numbers on the Run*, reported the finding of the Australian National Audit Office that there were 3.2 million more Tax File Numbers than people in Australia and 185,000 potential duplicate tax records for individuals. The ATO currently believes that there are over 25,000 duplicate tax file numbers which form part of 6.5 million inactive TFN records (Australian Taxation Office 2004, p. 6).

Performance

There are a number of ways in which the performance of biometric systems can be measured. These include collecting and analysing the:

- failure to enrol rate (FTER) – this measures the proportion of users who, for some reason, cannot enrol in a particular biometric system;
- failure to acquire rate (FTAR) – this measures the proportion of cases where a user seeks to provide a biometric to match against their previously enrolled template, but the system cannot acquire an image of sufficient quality;
- false match rate (FMR) – this measures the probability that a sample will be falsely declared to match the template of another person;
- false non-match rate (FNMR) – this measures the probability that a sample will be falsely declared not to match the template of the user who provided the sample;

- false accept rate (FAR) – this measures the proportion of cases in which an impostor is falsely accepted by a biometric system;
- false reject rate (FRR) – this measures the proportion of cases in which a genuine user is falsely rejected by a biometric system; and the
- equal error rate (EER) – this is usually the point at which the false reject and false accept rates are equivalent. In some cases, it can also refer to the point at which the false match and false non-match rates are equivalent.

It should be noted that while these measures are widely used, 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 biometric evaluation report closely before accepting its results. In addition, while each of the abovementioned measures can be used to evaluate biometric technologies, they are not the only possible ways of evaluating biometric systems. Some of the other issues that need to be considered are as follows.

Data Security

The implementation of biometrics in any case is not a simple matter, and the two models of storage of biometric information each offer their own challenges and risks. On the one hand, biometrics applications for verification may compare the individual's body – whether it be a fingerprint, face, hand, or iris – directly to the template recorded on a card or other *portable medium*. If this is the case then defeat of that medium's security features may allow replacement or alteration of the template, unbeknown to the system administrators. For facial recognition, depending on the model used, this might be as straightforward as photo substitution or as complex as cracking strongly encrypted data.

If, on the other hand, the comparison is to a template held on a *central database*, that database would represent a high-profile target for hackers, organised criminals and other parties. Securing that information, for example using public key encryption, and ensuring inside parties are not able to access and alter information inappropriately, represents a major challenge. In recent times, various large-scale information databases, including client details held by major credit card companies and respected commercial providers, have been defeated or compromised by outsiders and insiders alike. To anticipate the points of susceptibility to interference is the essential challenge of implementing biometric applications on a wide scale.

Spoofing

Spoofing refers to techniques developed or adapted to challenge the biometric in question. There are three main ways in which a system can be attacked (Thalheim et al. 2002): The first involves the creation of an artificial biometric. This involves putting artificially created data into the regular sensor technology of the system. For example, a fake finger could be used to deceive a fingerprint scanner, or a photograph used to deceive a facial recognition system. For this approach to work, it is necessary for the

impostor to obtain a copy of the biometric that they wish to use. This could be done, for example, by taking a photograph of the person to be imitated.

The second, known as relay attacks, involves the use of artificially created data. However, 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. This is a device which can be attached to the back of a computer (for example, in the USB port), which can obtain information as it is input into the computer. The data captured can then be replayed, to deceive the system. A researcher at the Australian National University in 2002, for example, demonstrated how fingerprint verifiers could be circumvented by presenting a template resembling that electronically stored in the device (Baker 2002).

Finally, 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 an external attack on the database (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. For example, a person could match his or her own fingerprint to a false identity, which could then be used for fraudulent purposes.

The first of these methods is the main focus of literature in this area, as it is the most likely avenue for spoofing. People are more likely to attempt to spoof a fingerprint recognition system by using a rubber finger, or a voice recognition system by using an audio recording, than they are to hack into the database itself. Many technology developers have attempted to create countermeasures to prevent such attacks.

The most common of these countermeasures is what is known as ‘liveness’ testing. Many systems have some form of technology capable of checking that the biometric characteristic being measured belongs to a live person. For example, fingerprint scanners may test the temperature of the finger, while iris scanners may search for a pulse or rapid eye movements. Such systems have a dual advantage: they can help to prevent spoofing, as well as potentially preventing some forms of crime displacement (see below). Unfortunately, there is little research on the steps that have been taken to prevent the less common forms of attack. There are also few evaluations that measure the ability of systems to repel concerted attacks. One of the few studies in this area was conducted by three German researchers who attempted to spoof a number of different devices (Thalheim et al. 2002). While some of the devices caused them slight difficulties, with a little persistence they managed to compromise each device investigated.

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, there have been reports that transplant surgery and immune system drugs may very soon enable faces to be transplanted. This might not currently be considered a realistic threat, and in any case is unlikely to occur on a sufficiently wide

scale to affect most systems. Yet, in view of the global awareness of how far terrorists may go in furtherance of their aims, such concerns need to be taken into consideration.

Privacy

While some have claimed that biometrics can be a privacy-enhancing technology (Biometrics Institute 2002), there is a general perception that the use of such technologies is likely to invade privacy. Some of the main privacy concerns include fears that biometric 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'); shared without explicit permission; or used to track people across multiple databases to amalgamate information for the purpose of surveillance or social control (General Accounting Office, United States 2002).

In recent times with ever-present concerns over terrorism, a number of countries have decided to 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; *South China Morning Post* 2002). A pilot program for a biometric ID card has also been implemented in Britain, in relation to asylum seekers (McAuliffe 2002).

Such proposals face vocal opposition from advocates of privacy who raise the grave consequences of essential information being misused such as occurred during the Nazi regime in the Second World War. One writer refers to 'the singular ease with which population registration systems have been mobilized for genocidal purposes' (Seltzer 1998, p. 544).

Any use of biometric systems needs to comply with privacy principles and privacy legislation (Crompton 2002). In Ontario, for example, policies were developed to govern the use of biometric systems designed to prevent welfare fraud. The following privacy protective provisions were included in the Canadian *Social Assistance Reform Act* (Cavoukian 1999, p. 5):

- any biometric information collected under the Act must be encrypted;
- the encrypted biometric cannot be used as a unique identifier, capable of facilitating linkages to other biometric information or other databases;
- the original biometric must be destroyed after the encryption process;
- the encrypted biometric information only can be stored or transmitted in encrypted form, then destroyed in a prescribed manner; and
- no program information is to be retained with the encrypted biometric Information.

The Act also required that systems should be unable to be implemented that could reconstruct or retain the original biometric sample from encrypted biometric information,

or that could compare it to a copy or reproduction of biometric information not obtained directly from the individual. These largely reflect the Information Privacy Principles that currently exist in Australia under the *Privacy Act 1988* (Cth).

User Acceptance

Past experience has shown that the efficiency and accuracy of biometric systems can be reduced if those required to use the system are not willing to accept the technology: ‘user attitude can make or break the implementation of a biometric system’ (United Kingdom Biometrics Working Group 2002, p. 7). 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 (see 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). Both end users and administrators of systems may be reluctant to make use of them. Accordingly, the need arises to educate users about the reasons why the system has been introduced and how it might benefit them. User concerns relating to privacy and security of data storage, as well as the safety of using some devices especially eye-based biometrics), would also need to be addressed.

Rectification

Another problem associated with biometrics arises from the fact that once a system has been compromised, it may be difficult to rectify the problem. While a new PIN can always be issued, new fingerprints cannot. Any error, corruption or systematic failure of the biometric identifier will be as permanent and irrevocable as the ‘correct’ identification is supposed to be. 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 (Biometrics Institute 2002). Meanwhile, the ostensibly greater security afforded by the use of the biometric may lead to overconfidence in its accuracy, which could make any cases of successful identity fraud that much more damaging.

Cost

There are a wide range of costs involved in the implementation and use of biometric systems. It is especially important to consider recurrent costs, which can often outweigh the costs of infrastructure and initial implementation. Often however, these differing cost considerations are grouped together and presented in simplistic charts, such as that contained in a Report from the International Biometric Group (2003) which seeks to compare a range of considerations relating to different biometrics in one chart. Although simple to read, it could be grossly misleading.

Displacement

Finally, the use of biometrics as a crime reduction strategy, like many other crime reduction techniques, carries with it the risk that displacement may occur. Displacement has been defined as: ‘a change in offender behaviour, along illegitimate means, which is designed to circumvent either a specific preventive measure or more general conditions unfavourable to the offender’s usual mode of operating’ (Gabor 1990, p. 66). One academic described the problem of displacement of crime as follows:

Fear of displacement is often based on the assumption that offenders are like predatory animals - they will do what ever it takes to commit crimes - just as a rat will do whatever it takes to steal food from the cupboard (Eck 1998).

If it is assumed that potential offenders act on the basis of some rational calculation in which they balance up the likely risks and benefits to be derived 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.

The use of biometrics for logical access control could result in offenders obtaining access to computers through bribery or coercion of IT personnel or other gatekeepers within organisations, or forcing users under threat of violence to permit the offender to have access by presenting their biometric under duress. We have already seen the occurrence of this with duress being used by offenders against users at ATMs to compel them to withdraw cash. Failure to comply has even resulted in users being killed in some countries.

Conclusions

This paper has identified some of the considerations that need to be taken into account when deciding whether or not to implement biometric systems. The concern is that the introduction of a new technology may make matters worse – either with respect to the specific crime problem sought to be addressed, or by creating new risks through the infringement of privacy or displacement to other forms of more serious crime.

Careful thought also needs to be given to what biometric 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 upon enrolment, then the subsequent use of a biometric authentication system may make identity-related crime easier to perpetrate, and more difficult to detect. Offenders may simply put their energies into creating a false identity and using that when enrolling in a biometric system.

The decision about which biometric technology, if any, to implement is not a simple one. There is a wide range of factors which need to be considered, including the performance of the system, its ability to be compromised, the ease of using such systems, and user concerns about issues such as privacy and security. In addition, the cost-effectiveness of rolling out a biometric system must be determined, with consideration given to both implementation and recurrent costs. These should be carefully weighed against the cost

of using other viable alternatives methods of identification, such as knowledge or token-based systems, in light of the particular security needs of the organisation.

Of great importance from the point of view of policy makers, however, 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 solely to focus 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 needs to be sought out and scrutinized concerning the range of other legal, social, and ethical considerations governing the use of any given system. Unfortunately, it is these aspects which have yet to be fully researched.

References

Australian Payments Clearing Association 2003, Payment Statistics
<http://www.apca.com.au>

Baker, L. 2002, 'Rule of Thumb: Don't Rely on New Security Systems', ANU Reporter, vol. 33, no. 9, 7 June, <http://www.anu.edu.au/pad/reporter/volume/33/09/acrobat.pdf>.

Australian Taxation Office 2004, Compliance Program 2004-05, Australian Taxation Office, Canberra.

Benitez, M. A. 2002, 'ID Card Contract Awarded', South China Morning Post (Hong Kong), 27 February, p. 2.

Biometrics Institute 2002, 'The Impact of Biometrics on Privacy', an Interview with Dr Roger Clarke, <http://www.biometricsinstitute.org/bi/interviews.htm>.

Cavoukian, A. 1999, Privacy and Biometrics, <http://www.ipc.on.ca/docs/pri-biom.pdf>

Crompton, M. 2002, 'Biometrics and Privacy: The End of the World as we Know it or the White Knight of Privacy?', presented at Biometrics-Security and Authentication Biometrics Institute Conference, Sydney, 20 March.

Cuganesan S. and Lacey D. 2003. Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent, SIRCA, Sydney.

Dunstone, T. 2003, The use of Biometric Technology in Airports
http://www.biometricsinstitute.org/bi/Articles/0303_AirportReview1.pdf

Eck, J. 1998, 'Preventing Crime at Places', in Sherman, L. W., Gottfredson, D., Mackenzie, D., Eck, J., Reuter, P. and Bushway, S. What Works, What Doesn't, What's Promising, National Institute of Justice, Washington.

Gabor, T. 1990, 'Crime Displacement and Situational Prevention', *Canadian Journal of Criminology*.

General Accounting Office, United States 2002, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174, November, Washington DC, <http://www.gao.gov/new.items/d03174.pdf>.

House of Representatives Standing Committee on Economics, Finance and Public Administration 2000, *Number on the Run: Review of the ANAO Audit Report No 37, 1998-99 on the Management of Tax File Numbers*, Parliament of the Commonwealth of Australia, Canberra.

International Biometric Group 2003, *Biometric Market Report 2003–2007*.

Krim, J. and Barbaro, M. 2005, '40 Million Credit Card Numbers Hacked', *Washington Post*, 18 June, p. A01. http://www.washingtonpost.com/wp-dyn/content/article/2005/06/17/AR2005061701031_2.html

McAuliffe, W. 2002, 'Asylum Seekers Get First UK Biometric ID Cards', *ZDNet Australia*, 5 February. <http://www.zdnet.com.au/newstech/security/story/0,2000024985,20263301,00.htm>

Nash, B. 2005, 'Utilising the Latest in Biometrics Technology to Enhance Your Forensic Capability', paper presented at the IIR Conference Combating Identity Fraud, 1 November, Sydney.

Pidco, G. W. 1996, 'Check Print: A Discussion of a Crime Prevention Initiative that Failed', *Security Journal*, vol. 7, pp. 37-40.

Seltzer, W. 1998, 'Population Statistics, the Holocaust, and the Nuremberg Trials', *Population and Development Review*, vol. 24 no. 3, pp. 511-552.

South China Morning Post (Hong Kong) 2002, 'ID Card Plans Raise Issue of Carrier Privacy', 17 January, p. 11.

Smith, R. G. 1999, 'Identity-Related Economic Crime: Risks and Countermeasures', in *Trends and Issues in Crime and Criminal Justice*, No. 129, Australian Institute of Criminology, Canberra.

Thalheim, L., Krissler, J., and Ziegler, P-M. '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 Kingdom, Biometrics Working Group 2002, *Use of Biometrics for Identification: Advice on Product Selection*, <http://www.cesg.gov.uk/site/ast/biometrics/media/Biometrics%20Advice.pdf>.