Trends & issues in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 511 April 2016

Foreword | *Biometric technologies make use of an individual's unique biological characteristics to identify them in their dealings with government and business. Common biometrics include fingerprints, iris recognition, voice pattern recognition and facial recognition, among others.*

There has been a considerable increase in the uptake of biometric technologies by a number of organisations in recent years, as society looks for ways to safeguard personal information from potential misuse. For instance, fingerprint scanning—once the mainstay of forensic policing—is increasingly used as a means of verifying the identity of mobile phone and tablet users.

In 2014, the Australian Institute of Criminology conducted an online survey to gain a greater understanding of identity crime and misuse in Australia. The survey also asked a sample of Australian victims of identity crime about their experiences of, and willingness to use, biometric technologies.

This paper presents the results of the research, which indicate generally high levels of previous exposure to biometrics. It also presents some unexpected findings concerning those willing to take up biometrics in the future.

Chris Dawson APM

Use and acceptance of biometric technologies among victims of identity crime and misuse in Australia

Catherine Emami, Dr Rick Brown & Dr Russell G Smith

Biometric technologies use an individual's unique physiological or behavioural attributes to identify that individual (Unar, Seng & Abbasi 2014). Biometric technologies are diverse; some of the more common biometrics include fingerprint matching, facial imaging, signature recognition, retina and iris recognition and voice recognition. Other less widely used techniques include body-odour authentication (Gibbs 2010), gait recognition (Di Nardo 2008), ear geometry, vein-pattern analysis, and keystroke dynamics (Biometrics Institute; ALRC 2008). A recent survey of Biometrics Institute members found the technologies expected to dominate in the years ahead are fingerprint recognition (27%), facial recognition (24%), voice recognition (7%) and iris recognition (6%), with 22 percent of respondents anticipating that multi-modal approaches combining various biometrics would prevail in the future (Biometrics Institute 2015).

Biometric technologies are already used by a range of organisations in Australia to verify the identities of those they deal with. For example, the Department of Immigration and Border Protection (DIBP) collects biometric information, including fingerprints and facial images, from offshore visa and onshore protection visa applicants, immigration detainees and certain categories of airline passengers (DIBP 2013; Wilson 2007). Australian airports have facial recognition capabilities, known as SmartGates, that enable travellers from Australia, New Zealand, the United Kingdom, Switzerland, Singapore and the United States who hold ePassports to process themselves rather than undergoing the usual customs and immigration checks conducted by Australian Border Force officers (ACBPS 2014).

In addition to their use at airports or in the immigration and border protection context, biometrics are used to verify an individual's identity in a range of other settings. A number of Australian banks, for example, have introduced biometric technologies that allow banking customers to log on to mobile banking services using their fingerprints or voices (Head 2014a; Head 2014b; Bank of Melbourne 2014; Westpac 2015) instead of passwords.

Mobile phone companies have also increasingly adopted biometric technologies to allow users to log on to their mobile devices, releasing phones and/or tablets that owners can log on to by scanning their fingerprints (Phonegg 2014).

Previous research into user acceptance of biometric technologies

The successful implementation of biometric systems is heavily dependent on the degree to which those using the systems are willing to accept the technology. As the United Kingdom Biometrics Working Group (2002: 7) argued: '[U]ser attitude can make or break the implementation of a biometric system.' 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 that 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. Others may believe systems that scan irises or retinas may harm their eyes, despite clear evidence to the contrary. Accordingly, there is a need to educate users on why the system has been introduced and how it might benefit them. User concerns relating to the privacy and security of stored data must also be addressed, although emerging technologies such as biocryptography (Xi & Hu 2010) and cancellable fingerprint templates (Ahmad, Hu & Wang 2011; Rathgeb & Uhl 2011) have been proposed and are currently being developed in an effort to allay these concerns in future.

Research on public attitudes toward the use of biometric technologies has found that, while many Australians are comfortable with the use of these technologies for security purposes and to verify access to government services, there is much greater apprehension around the use of biometrics for marketing purposes, accessing public transport or enrolling in educational courses. Australians appear to be reasonably comfortable with the use of biometric technology in an airport security context, for instance, with a survey conducted for the biannual Unisys Security Index finding that 75 percent of Australian survey respondents were willing to provide biometric data (eg a photograph or fingerprint) to confirm their identity at an automated boarding gate when boarding a flight, and 71 percent were willing to provide this information to identify themselves as low security risk frequent travellers (Unisys 2014). These findings were based on a survey conducted by Newspoll in March 2014 using a randomly selected, nationally representative sample of 1,201 respondents aged 18 years and over. The survey results were then weighted in accordance with national demographic data from the Australian Bureau of Statistics (ABS; Unisys 2014).

Australians were considerably less enthusiastic about providing biometric data in order to receive customised retail offers at the airport, with only 33 percent of respondents willing to have their biometric data used for such purposes and 63 percent unwilling to have their biometric data used in this way (Unisys 2014). This reduced willingness to use biometrics in these contexts may be due more to the nature of the service being provided—namely, targeted advertising—than inherent concerns about the means of identification itself.

An earlier survey of 1,206 respondents aged 18 years and over, conducted by Newspoll in March 2012 as part of the biannual Unisys Security Index, asked members of the Australian public how acceptable they thought it was to use facial recognition technology in certain situations. The survey results were then weighted in accordance with national demographic data from the ABS. Almost all survey respondents (95%) supported the use of facial recognition by customs or immigration staff at airports as a means of identifying passengers on police watchlists. A large percentage of respondents (92%) also supported the use of facial recognition to assist police to identify people from video footage obtained from the public or from security cameras (Unisys 2012).

Respondents also expressed support for the use of facial recognition in the workplace to track which parts of a building had been accessed and by whom, although more than a quarter (29%) of respondents considered this an unacceptable use of the technology. Respondents were most concerned about the use of facial recognition by social media companies such as Facebook, with only 38 percent of respondents considering it acceptable for Facebook to use facial recognition to make it easier for users to identify friends in photographs, and 50 percent saying this was an unacceptable use of the technology (Unisys 2012).

In the public sector, Australians appear to be quite comfortable with the idea of providing biometric information including fingerprints, voice recordings and iris scans to access government services such as those provided by Medicare (81%) and the Australian Taxation Office (75%). Australian Unisys survey respondents indicated they would be willing to use these biometrics to access their bank records (69%), health records (68%) and welfare payments (63%), and to submit tax returns or access their tax records (65%). Respondents were less willing to use biometrics when enrolling in educational courses (36%), joining clubs (34%) or accessing public transport (29%; Unisys 2010).

Similar levels of public acceptance of biometrics were found in a nationally representative survey of 1,046 adults aged 18 years or over conducted in the United States in August 2002 (ORC International). It was found that 88 percent of respondents found the use of fingerprint scans to verify identity for passports to be very or somewhat acceptable, 84 percent supported scans to gain entry to government buildings, 82 percent supported scans at airport check-ins and 77 percent supported scans to obtain a driver's licence.

Survey results like this are subject to the usual limitations of this kind of research, including the use of small samples of the population which make the generalisability of results difficult, the possibility that the questions asked may suggest commercially attractive outcomes and the risk that respondents may have misunderstood or misinterpreted questions. Bearing these limitations in mind, the current study examined the previous experiences of a sample of Australians with the use of biometrics and sought to determine their willingness to use such technologies in the future to protect their personal information from misuse. It also attempted to discover if particular demographic groups may be more or less willing to use such technologies in the future.

Methodology

In September 2014, as part of the National Identity Security Strategy (AGD 2012), a survey was conducted to explore the perceptions and experiences of identity crime and misuse among a sample of the Australian public. Using an anonymous online format, the survey sampled 5,000 Australian residents registered with an online survey panel provider. The results showed a high proportion (68.1%) of respondents believed that misuse of personal information was very serious, and a further 28.2 percent believed it was somewhat serious. In terms of victimisation, 446 (8.9%) respondents reported having had their personal information misused in the preceding 12 months, and 20.4 percent of respondents reported misuse of their personal information at some time during their life (see Smith, Brown & Harris-Hogan 2015 for further details regarding the survey methodology).

As part of the survey, the 446 respondents who reported misuse in the previous 12 months were asked if they had ever used any of the following technologies in any way (not just to prevent misuse of personal information): passwords, signatures, voice recognition, fingerprint recognition, facial recognition and iris recognition. The question asked about the use of technologies rather than biometrics, as some respondents might have been unfamiliar with that term. They were also asked whether they would be willing to use any of these technologies in future to prevent misuse of their personal information.

For the study's purposes results relating to the use of signatures were excluded as, although technically a biometric, they are less likely to be perceived as such by the general public. In fact, 27 percent of respondents said they had not used signatures in the past, which may indicate that some people misunderstood what was meant by the term 'signature'.

One limitation of this methodology was that the questions on biometrics were asked only of those who had been victims of the misuse of personal information, and it is therefore plausible that those respondents' willingness to use biometric security measures was influenced by their experiences. It is therefore unclear to what extent the findings presented here are generalisable beyond this group. In addition, the questions about the use of security technologies were of a general nature rather than specific to any particular context (eg home computer use, mobile phone use, work activities, banking or international travel) and it is likely that different responses may have been given concerning these different applications.

Findings

Previous use of biometric security technologies

Overall, 95 percent of those who responded to this question reported having used at least one of the five forms of biometric security technology in the past (Table 1).

Table 1: Previous use of security technologies

Technology	n	%
Passwords	394	88
Fingerprint recognition	75	17
Facial recognition	30	7
Iris recognition	26	6
Voice recognition	25	6
Any	423	95

Source: AIC Identity crime and misuse computer file 2014

Note: Respondents were able to select more than one type of technology used, hence the total sample size will not sum to 446

Passwords were the most common form of security technology employed, with almost nine in 10 respondents having used such measures. This is unsurprising given the high level of computer usage in Australia, which invariably requires a password for access. In contrast, facial, iris and voice recognition had each been used by fewer than one in 10 respondents.

Chi square tests were undertaken for each of these security technologies to identify whether there were differences between previous use of biometrics and demographic characteristics such as gender, age, Indigenous status, language spoken at home, income, place of residence (whether capital city or otherwise) and hours spent per week on a computer—noting, however, that all differences between specific categories were based on an analysis of the adjusted residuals. A chi square is a simple type of bivariate analysis which tests whether there is an association or relationship between variables; these tests examine the statistical probability of the results occurring by chance. Further statistical tests were undertaken to determine whether the results for the four biologically-based biometrics (fingerprint, facial, iris and voice recognition), when grouped together, differed significantly in terms of the demographic variables considered.

Where passwords were concerned, only one variable demonstrated a statistically significant difference: those earning $180,000 or more per annum were found to be significantly less likely (51%, n=7) than other income groups to have used passwords in the past (χ^2 (5, n=446) =12.51, p<0.05). It is unclear why this was so, and future research is needed to examine this further. It is possible that individuals earning incomes of $180,000 or more may rely on other people, such as personal assistants, to log on to networks on their behalf and be responsible for user authentication in the workplace.

Seventeen percent of respondents had previously used fingerprint recognition. There was a significant difference between previous use of fingerprint recognition technologies and computer use (χ^2 (6, n=442)=18.56, p<0.01). Those using a computer for five hours per week or less were more likely to have used fingerprint recognition (46%, n=12), while those using a computer for 26 to 30 hours per week were less likely to have used this biometric

(10%, n=6). This may be because those respondents who indicated they use a computer for five hours or less per week may instead rely on their smartphones or tablets; a number of smartphones and tablets now use fingerprint identification to verify the identity of the person logging on.

A small number of respondents had used facial recognition (7%) and iris recognition (6%). In the case of facial recognition this is somewhat surprising, as 4.6 million people successfully cleared SmartGate kiosks at Australian airports in 2013–14 (ACPBS 2014). SmartGates use facial recognition technology in conjunction with ePassport chip data to verify travellers' identities (ACPBS 2014). It may be those using Smartgate terminals did not realise the terminals use a form of facial recognition or, alternatively, respondents to the present survey may not ever have used Smartgates.

Voice recognition had previously been used by just six percent of respondents. Those who lived in capital cities were significantly more likely to have used this technology (7%, n=23) than those who did not (1%, n=2) (χ^2 (1, n=446)=3.83, p<0.05).

Finally, when results for the four biological biometric technologies (fingerprint, facial, iris and voice recognition) were combined, it was found that 25 percent (n=111) of respondents had previously used at least one of these biometrics; but no statistically significant differences were found between use of any form of biometric and the demographic characteristics examined.

Willingness to use biometric security technologies in the future

Respondents were also asked to indicate their willingness to use biometric technologies in the future to protect their personal information from misuse. It was found that 96 percent (n=427) of respondents would be willing to use at least one of the specified technologies (Table 2). Respondents were most willing to use passwords and fingerprint recognition; they were least willing to use voice recognition.

Table 2: Willingness to use biometric technologies in future

Technology	n	%
Passwords	328	74
Fingerprint recognition	270	61
Iris recognition	182	41
Facial recognition	164	37
Voice recognition	139	31
Any	427	96

Source: AIC Identity crime and misuse computer file 2014

Note: Respondents were able to select more than one type of technology used, hence the total sample size will not sum to 446

Surprisingly, although 88 percent of respondents had used passwords in the past, only 74 percent indicated they would be willing to use them in future. It is possible respondents misinterpreted this question and, rather than reporting their willingness to use passwords in terms of acceptance of the privacy and other risks involved, instead were indicating their personal preference for usage in terms of convenience and efficiency. As a result, although more respondents reported actually using passwords, a smaller percentage indicated satisfaction with password use and might have preferred another system for user authentication. Further analysis of the responses of those willing to use passwords showed no statistical differences between demographic variables in terms of willingness to use this technology in the future.

Sixty-one percent (n=270) of respondents reported a willingness to use fingerprint recognition in the future. Statistically significant differences were found between willingness to use fingerprint recognition and age group, with older respondents being more willing to use this technology than younger respondents (χ^2 (6, n=446)=53.08, p<0.001). Indeed, 73 percent (n=64) of 55–64 year olds and 78 percent (n=58) of those aged 65 years and over were willing to use fingerprint recognition. By way of contrast, only 30 percent (n=6) of 18–24 year olds and 34 percent (n=31) of 25–34 year olds were willing to use fingerprint recognition. It may be that older people feel more familiar with fingerprint recognition systems (Biometrics Institute 2015), or perhaps younger people feel fingerprint recognition systems would delay or otherwise impede their use of smartphones and tablets. It is also possible older Australians may be more concerned about computer security than younger users (ACCC 2014).

There were also statistically significant differences between willingness to use biometrics and the language respondents spoke at home (χ^2 (1, n=446)=7.47, p<0.01). Those who spoke English at home were more willing to use fingerprint recognition in future (62%, n=260) than those who spoke another language at home (34%, n=10).

Four in 10 (41%) respondents were willing to use iris recognition in the future. As with fingerprint technology, there were statistically significant differences between age groups, with older respondents being more willing to use this technology than younger respondents (χ^2 (1, n=446)=7.47, p<0.01). Indeed, 52 percent (n=46) of those aged 55–64 years were willing to use iris recognition, as were 54 percent (n=40) of those aged 65 years and over. In contrast, only 23 percent (n=21) of those aged 25–34 years were willing to use iris recognition technology.

Similar age-related differences were found among those willing to use facial recognition technology (χ^2 (6, n=446)=41.20, p<0.001). Those aged 55–64 years (54%, n=47) or 65 years and over (52%, n=38) were more likely to be willing to use facial recognition than those aged 18–24 years (14%, n=3), 25–34 years (23%, n=21), or 45–54 years (31%, n=29). Willingness to use facial recognition also varied by extent of computer use (χ^2 (6, n=442)=19.00, p<0.01). Those who used a computer for five hours or less each week were less willing to use facial recognition in future (16%, n=4) than those who used a computer for 26–30 hours per week (60%, n=35).

Around a third of respondents (31%) were willing to use voice recognition technology in future. As with fingerprint, iris and facial recognition, willingness to use voice recognition varied with age, with older respondents being more willing than younger respondents to use this technology (χ^2 (6, n=446)=20.43, p<0.01). Those aged 55–64 years were more willing to use voice recognition in future (40%, n=35) than those aged 25–34 years (21%, n=19). Willingness to use voice recognition also varied with computer usage (χ^2 (6, n=442)=18.58, p<0.01). Those who used a computer for five hours or less per week (14%, n=4) or for 11–15 hours per week (18%, n=11) were less willing to use voice recognition in future than those who used a computer for 26–30 hours per week (46%, n=26).

Again, when results for the four biological biometric technologies (fingerprint, facial, iris and voice recognition) were combined, it was found that 68 percent (n=304) of respondents were willing to use at least one of these technologies in future. As with prior usage, there were statistically significant differences between age groups, with older respondents being more willing to use such technologies than younger respondents (χ^2 (6, n=446)=39.31, p<0.001). Those aged 55–64 years (80%, n=70) and 65 years and over (85%, n=63) were more willing to use such technologies, while those aged 18–24 years (33%, n=7) and 25–34 years (45%, n=41) were less willing.

Finally, the analysis examined whether willingness to use any of the four biological biometric technologies was affected by whether respondents perceived the risk of personal information being misused would increase or decrease in future. No statistically significant differences were found, suggesting that willingness to use any of these four technologies was not influenced by perceptions of risk.

Conclusions

As the use of digital technologies becomes more widespread and concern regarding potential criminal misuse of these technologies increases, the cybersecurity industry has sought ways to improve the efficient and secure authentication of user identity. Existing systems that rely on logon and password combinations have become problematic as criminals become more adept at compromising passwords, and many users fail to deal with passwords securely. The need for a large number of logon and password combinations has also made it difficult for users to manage this information without storing these details in insecure ways. Biometric technologies may provide a solution by allowing individuals to use their biological attributes to gain access to networks and data. This study sought to quantify the extent to which a sample of Australian victims of identity crime have made use of different biometrics in the past, and how willing they would be to use selected biometrics in future to minimise the risk of criminal misuse of their personal information.

With a rise in international security incidents, a balance must be struck between technologies that enhance personal security and minimise the risks of harm, and technological advances which may jeopardise individual privacy and the confidentiality of personal information. Understanding how the community perceives levels of risk, and whether it is willing to use technology as a security solution, is of critical importance in devising appropriate future policy measures that will be both effective and acceptable to the community.

This study found that, while the use of passwords is widespread among those whose personal information has been misused in the past year, relatively few had ever used other forms of biometric security technology including fingerprint, facial, iris or voice recognition. However, their willingness to use such technologies in future was high, with 96 percent indicating they were prepared to do so. While a willingness to use passwords and fingerprint recognition was most prevalent, a third or more of respondents were willing to use facial, iris or voice recognition to protect their personal information.

Interestingly, older respondents were more willing to use biometric security technologies in future than younger respondents. This result held for biometric technologies in general, as well as specifically for fingerprint, iris, facial and voice recognition. This could arguably indicate higher levels of concern among older people about the misuse of their personal information, resulting in a corresponding willingness to use more secure forms of identification to address the perceived threat. Alternatively, younger people might be reluctant to make use of apparently complex technologies if they believe these may impede their immediate access to the online world. These attitudes must be monitored to ensure future generations of users are willing to make use of any biometric security measures implemented.

Acknowledgements

This study was commissioned and funded by the Commonwealth Attorney-General's Department and forms part of the National Identification of Identity Crime and Misuse project, which has been implemented pursuant to the National Identity Security Strategy. The survey was developed with input and advice from the members of the National Identity Crime and Misuse Framework Working Group, led by the Attorney-General's Department. Their considerable expertise is gratefully acknowledged. Data collection was undertaken professionally and efficiently by i-Link Research Solutions, a market research consultancy firm that provided the panel of individuals, drawn from across Australia, who completed the survey. The willingness of the survey respondents and the time they spent in responding are also gratefully acknowledged.

The opinions expressed in this paper are those of the authors only and do not necessarily reflect the views or policies of the Commonwealth Government.

References

URLs correct at October 2015

Ahmad T, Hu J & Wang S 2011. Pair-polar coordinate-based cancelable fingerprint templates. *Pattern Recognition* 44(10–11): 2,555-2,564

Attorney-General's Department 2012. *National Identity Security Strategy 2012.* http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/National%20Identity%20Security%20Strategy%202012.PDF

Catherine Emami is a Research Officer, Rick Brown is Deputy Director (Research) and Russell G Smith is Principal Criminologist at the Australian Institute of Criminology.

General editor, *Trends & issues in crime and criminal justice* series:
Dr Rick Brown, Deputy Director (Research), Australian Institute of Criminology

Note: *Trends & issues in crime and criminal justice* papers are peer reviewed

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: aic.gov.au

ISSN 0817-8542

GPO Box 1936
Canberra ACT 2601, Australia
Tel: 02 6243 6666

Disclaimer: This research paper does not necessarily reflect the policy position of the Australian Government

Australian Competition and Consumer Commission (ACCC) 2014. *Targeting scams: Report of the ACCC on scam activity 2013*. https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2013

Australian Customs and Border Protection Service (ACBPS) 2015. *SmartGate*. http://www.customs.gov.au/smartgate/default.asp

Australian Customs and Border Protection Service (ACBPS) 2014. *Annual Report 2013–2014*. Canberra: ACBPS. http://www.border.gov.au/ReportsandPublications/Documents/annual-reports/ACBPS_AR_2013-14.pdf

Australian Law Reform Commission 2008. *For your information: Australian Privacy Law and Practice.* ALRC Report 108. http://www.alrc.gov.au/publications/9.%20Overview%3A%20Impact%20of%20Developing%20Technology%20on%20Privacy/biometric-systems

Bank of Melbourne 2014. Bank of Melbourne first to launch biometric technology in mobile banking. *Media release* 24 Sept. https://www.bankofmelbourne.com.au/about/media/archive/BOM-News-Article-65

Biometrics Institute 2015. Australian Federal Budget 2015 released. Good news for the biometrics industry but debate needed on the key issues. *Media release* 14 May. http://www.biometricsinstitute.org/news.php/179/biometrics-institute-media-release-australian-federal-budget-2015-released.-good-news-for-the-biomet

Biometrics Institute. *Types of Biometrics*. http://www.biometricsinstitute.org/pages/types-of-biometrics.html

Biometrics Institute 2015. *Biometrics Institute Industry Survey 2015*. Sydney: Biometrics Institute. http://www.biometricsinstitute.org/pages/industry-survey.html

Minister for Immigration and Border Protection 2015. *Speech to the Biometrics Institute Asia-Pacific Conference.* http://www.minister.immi.gov.au/peterdutton/2015/Pages/biometrics-institute-asia-pacific-conference.aspx

Department of Immigration and Border Protection (DIBP) 2013. *Fact Sheet 84: Biometric Initiatives*. Canberra: DIBP. https://www.immi.gov.au/media/fact-sheets/84biometric.htm

Di Nardo J 2008. Biometric Technologies: Functionality, Emerging Trends and Vulnerabilities. *Journal of Applied Security Research* 4(1–2): 194–216

Gibbs M 2010. Biometrics: Body Odor Authentication Perception and Acceptance. *SIGCAS Computers and Society* 40(4): 16–24

Head B 2014a. *St George leads biometric charge with fingerprint login for mobile banking*. *The Age* 22 Aug. http://www.theage.com.au/it-pro/business-it/st-george-leads-biometric-charge-with-fingerprint-login-for-mobile-banking-20140821-106xi7.html

Head B 2014b. Westpac launches fingerprinting access for online banking on iOs and Android devices. *The Age* 5 Dec. http://www.theage.com.au/it-pro/business-it/westpac-launches-fingerprinting-access-for-online-banking-on-ios-and-android-devices-20141205-120yr9.html

ORC International 2002. *Public attitudes toward the uses of biometric identification technologies by government and the private sector.* New York: ORC International

Phonegg 2014. *Cell phones with fingerprint scanner*. http://www.phonegg.com/list/182-Cell-Phones-with-Fingerprint-Scanner

Pidco GW 1996. Check Print: A discussion of a crime prevention initiative that failed. *Security Journal* (7): 37–40

Rathgeb C & Uhl A 2011. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Technology* (3): 1–25

Smith RG, Brown R and Harris-Hogan S 2015. *Identity crime and misuse in Australia: Results of the 2014 online survey*. Research and Public Policy series no.130. Canberra: Australian Institute of Criminology

Unar JA, Seng WC & Abbasi A 2014. A review of biometric technology along with trends and prospects. *Pattern Recognition* 47: 2,673–2,688

Unisys 2014. *Unisys Security Index Report Australia: Biometrics in Airports.* http://www.unisyssecurityindex.com/system/resources/uploads/113/original/In%20what%20circumstances%20are%20Australians%20willing%20to%20use%20biometrics%20in%20airports%20-%20May%202014.pdf?1400743365

Unisys 2012. *Unisys Security Index Report Australia: Facial Recognition.* http://www.unisyssecurityindex.com/system/resources/uploads/101/original/Australian%20support%20for%20facial%20recognition%20technology%20-%20May%202012.pdf?1338379115

Unisys 2010. *Unisys Security Index: Additional Research: Acceptable use of biometrics for security*. http://www.unisyssecurityindex.com/system/resources/uploads/70/original/In%20what%20circumstance%20do%20Australians%20support%20Biometrics.pdf?1337097045

United Kingdom, Biometrics Working Group 2002. *Use of biometrics for identification: Advice on product selection*. http://www.cesg.gov.uk/publications/Documents/biometricsadvice.pdf

Westpac 2015. Westpac launches Australian 'first': fingerprint sign-in for iPad banking app. *Media release* 7 Apr. http://www.westpac.com.au/about-westpac/media/media-releases/2015/7-april

Wilson D 2007. Australian Biometrics and Global Surveillance. *International Criminal Justice Review.* 17(3): 207–219

Xi K & Hu J 2010. Bio-Cryptography, in Stavroulakis P & Stamp M (eds), *Handbook of Information and Computer Security*. Verlag Berlin Heidelberg: Springer: 129–157. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.187.7410&rep=rep1&type=pdf