Australian Government
Australian Institute of Criminology

AIC reports
Research Report 20

Changing perceptions of biometric technologies

Christie Franks
Russell G Smith

ISSN (Online) 2206-7280
ISBN 978 1 922478 14 6 (Online)

Published by the Australian Institute of Criminology
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6268 7166
Email: front.desk@aic.gov.au
Website: aic.gov.au

Please note: Minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

All publications in the Research Report series are subject to peer review–either through a double-blind peer review process, or through stakeholder peer review. This report was subject to double-blind peer review.

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

General editor: Dr Rick Brown, Deputy Director, Australian Institute of Criminology

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at **aic.gov.au**

Contents

Figures

Tables

Acknowledgements

This study was undertaken as part of the Australian Government's National Identity Security Strategy. The Australian Institute of Criminology's annual identity crime survey was developed with input and advice from the Department of Home Affairs and the Attorney-General's Department. Quantitative data collection was undertaken professionally and efficiently by i-Link Research Solutions, a market research consultancy firm that provided a panel of individuals drawn from across Australia who were asked to complete an online questionnaire. The qualitative survey platform, i-Discuss, was also provided by i-Link Research Solutions and the online interviews were moderated by Footprints Market Research, who also conducted a preliminary qualitative analysis of the findings. The time and willingness of those who completed the surveys and participated in the online interviews are also gratefully acknowledged. The AIC is also grateful to the Biometrics Institute and the Ada Lovelace Institute for their willingness to permit use of their survey findings in the present report. The opinions expressed are those of the authors alone and do not necessarily reflect the views or policies of the Australian Government or the research and industry organisations involved.

Acronyms

AGD	Attorney-General's Department
AI	artificial intelligence
AIC	Australian Institute of Criminology
BaaS	biometrics-as-a-service
FRaaS	facial-recognition-as-a-service
NFC	near-field communication
PIN	personal identification number
RFID	radio frequency identification
SaaS	software-as-a-service

Abstract

Identity crime and misuse cost the Australian economy an estimated $3.1b in 2018–19 (Smith & Franks 2020). Protecting individuals' personal identification information and finding secure ways to verify identities has become an increased priority as the impact of identity crime continues to grow in Australia and worldwide. Biometric technologies for identity verification provide an enhanced security solution, although implementation of biometric systems within Australian society has met with varying degrees of acceptance. Since 2013, the Australian Institute of Criminology (AIC) has conducted online surveys to gain a greater understanding of identity crime and misuse in Australia. These surveys have asked about respondents' experience of identity crime and also their previous use of, and future willingness to use, biometric technologies to safeguard their personal information. This report presents both qualitative and quantitative research findings obtained from a sample of respondents in the most recent surveys concerning their experiences of biometrics and perceptions as to its role in identity security.

Executive summary

Identity crime and misuse cost the Australian economy an estimated $3.1b in 2018–19 (Smith & Franks 2020). Protecting individuals' personal identification information and finding secure ways to verify identities have become increased priorities as the impact of identity crime continues to grow in Australia and worldwide. Biometric technologies for identity verification offer an enhanced security solution, although implementation of biometric systems within Australian society has met with varying degrees of acceptance. The Australian Institute of Criminology's (AIC) online surveys aim to gain an enhanced understanding of identity crime and misuse in Australia, through quantifying respondents' experience of identity crime and also their previous use of, and willingness to use, biometric technologies to safeguard their personal information. This report presents both qualitative and quantitative research findings obtained in the AIC's most recent surveys, conducted in 2018 and 2019 (reported in Jorna, Smith & Norman 2020 and Franks & Smith 2020 respectively).

Methodology

Annually since 2013 (with the exception of 2015), the AIC has administered online questionnaires to a research panel of Australians drawn from all states and territories. A sampling frame of more than 300,000 individuals was provided by the market research company i-Link Research Solutions, which also hosted the online questionnaire and provided raw, de-identified data for the AIC to analyse. Sampling was completed once a quota of 10,000 respondents had been satisfied. No other quotas were employed as the sample was sufficiently large to ensure good representation from urban and regional areas across Australia.

Survey results were weighted by age and gender to represent the spread of the population in Australia. Australian Bureau of Statistics data from the 2016 Census were used to develop the weighting matrix for the sample. Questions on biometrics were asked of all respondents, not only those who had reported previous misuse of personal information. All respondents answered questions about their prior use of biometrics and their willingness to use biometrics for specified purposes.

Extended online interviews were conducted with 99 individuals who had participated in the AIC's online survey in 2018 and who had agreed to participate in further research. These interviews were moderated by Footprints Market Research using the i-Discuss online platform provided by i-Link Research Services. Interviews canvassed four selected topics that enabled responses of the original survey respondents to be examined in greater depth. These qualitative results are the focus of the present report.

In order to provide data on certain other aspects of biometrics, the findings of two other surveys were presented. One was conducted for the Ada Lovelace Institute in the United Kingdom on public attitudes to facial recognition technology and the other was conducted for the Biometrics Institute to ascertain the views of its membership regarding the biometrics market globally. These are presented by way of comparison with the AIC's quantitative survey and qualitative interview research findings.

Background

Identity crime and misuse

Identity crime is a ubiquitous form of criminal activity worldwide and is the most prevalent crime type in Australia at present. It affects millions of individuals, businesses and government agencies annually, with one in four Australians reporting that they have previously fallen victim to misuse of their personal information (Franks & Smith 2020).

In 2012 the Council of Australian Governments reviewed and revised the National Identity Security Strategy on the basis that 'the preservation and protection of a person's identity is a key concern and a right of all Australians' and it was concluded that an updated strategy document was needed in response to the evolving nature of identity crime in Australia (Department of Home Affairs 2020a). The Council of Australian Governments review recommended the creation of a longitudinal measurement framework for identity crime and misuse that could be used to measure the effectiveness of policy and practice throughout Australia (Department of Home Affairs 2020a).

Biometric technologies and identity security

As part of the 2012 update of the National Identity Security Strategy (AGD 2013) a National Biometric Interoperability Framework was identified as an implementation goal. The framework was developed to ensure consistent collection, use, disclosure and management of biometrics across the Commonwealth, state and territory governments in Australia (AGD 2013).

Biometric technologies use unique physiological or behavioural attributes of people as a means of personal identification. Types of biometrics currently in use include fingerprint scans, facial recognition, iris and retinal scans, voice matching, DNA and signature analysis. Human microchip implantation has also become increasingly available, although it is not technically a biometric technology but an implanted radio frequency device that can be used for a variety of identification and geolocation purposes. Facial recognition has become the method of most interest globally and the one predicted to experience the largest growth rate over the next few years (Biometrics Institute 2019). Of the AIC 2019 survey respondents, 73.2 percent of the total cohort stated their willingness to use facial recognition technology and this percentage increased to 81.2 percent of those who had experienced previous misuse of their identity credentials (Franks & Smith 2020).

The Australian Government currently employs biometrics in various agencies in an effort to address challenges from the increasing volume of travel and trade, the enhanced sophistication of criminal activity and the complexities of a digitally connected world (Department of Home Affairs 2020b). For example, the Australian Border Force establishes the identity of citizens and non-citizens through biometric technology as they pass through border controls while the Australian Federal Police uses biometrics to proactively support all phases of law enforcement operations including criminal investigations, disaster victim identification and location of missing persons (Department of Home Affairs 2020b).

In addition, private sector use of biometric technologies has increased dramatically with the development of smart devices. Most mobile phones and tablets have fingerprint scanners and reverse cameras for enhanced facial scan security features. Many financial institutions are also turning to biometrics for increased security of financial transactions. The Commonwealth Bank of Australia announced in 2019 that it was in negotiations with federal agencies to make use of government facial biometric holdings when conducting customer verification checks required by Know Your Customer regulations (Bajkowski 2019).

Use and acceptance of biometric technologies

Results of the AIC 2019 identity crime survey, AIC 2018 identity crime survey and online interviews, and consulted international publications, demonstrate a generally high level of previous exposure to biometrics, with an increasing willingness to use biometric technologies in the future, especially among previous victims of identity crime. Simple username and password combinations are becoming obsolete as offenders have become more adept at compromising these user authentication processes. The constant requirement of network security to reset these combinations has made it challenging for users to manage access to devices without resorting to insecure ways of remembering passwords. Biometrics offer a more secure solution by enabling individuals to use their biological attributes as a means of identifying themselves.

The AIC's research has shown that previous use of specified biological biometrics is strong, with three out of four respondents stating they have used at least one form of the technology in the past (Franks & Smith 2020). Franks and Smith (2020) also reported that future willingness to use biometrics as a security solution remains consistently strong, with at least 71 percent of all respondents willing to use some form of biometric for identification purposes, increasing to 76 percent for recent victims of identity theft. Recent victims were also more than twice as willing as non-victims to try having a computer chip implanted under their skin as a future security option (42% vs 20% respectively; Franks & Smith 2020). Generally, recent victims of identity crime were more willing than non-victims to use all of the biometric technologies mentioned; however, recent victims were four percentage points less willing than non-victims to continue using the less secure option of passwords (Franks & Smith 2020). The top three preferred biometrics among the cohort interviewed by the AIC in 2018 were fingerprint scans, facial recognition and voice recognition.

Respondents to the AIC surveys have shown a general approval of the use of biometric technologies by government authorities for law enforcement and national security reasons and as a means of obtaining access to government services. Feelings towards the use of biometric technologies for public surveillance, personal reasons and by private industry are mixed. Privacy, ethical use, data access and storage security were some of the main concerns expressed by both AIC and comparison survey participants.

Results of the Biometrics Institute (2019) survey of industry experts were consistent with 2018 in predicting facial recognition technology as the area of greatest potential growth by 55 percent of Biometrics Institute respondents. AIC and Ada Lovelace Institute (2019) survey respondents stated their acceptance of the use of this technology in the form of crowd surveillance for national security and community safety but were less willing when considering it for commercial use. Survey participants were generally willing to use all biometric systems monitored by government entities and far less willing to use those issued by private organisations.

Most of the survey cohort had limited knowledge of how their personal information was being used, stored and protected, and expressed disappointment in the degree of information provided by both government and industry. The Biometrics Institute (2019) cohort ranked 'data sharing concerns' as the second highest key market restraint, with 'privacy/data protection concerns' ranked at number one.

Respondents from both the AIC and Ada Lovelace Institute surveys and the AIC online interviews were concerned about privacy issues and the ethical use of biometrics data—these included concerns about inaccurate matching leading to false identification/prosecution by law enforcement. Individuals were most comfortable with biometrics when they were afforded freedom of choice but accepted enforced use in situations where their security was at risk; however, support was not unconditional. The capture and storage of information without user consent was not justifiable for most.

Conclusion

Identity crime and misuse of personal information remain ongoing concerns for those in the Australian community. Despite advances in verification of credentials and improvements in online authentication procedures, victimisation continues to increase. Financial losses also continue to rise, along with the equally harmful non-financial consequences including damage to credit ratings, being wrongly accused of crime, and a range of psychological and emotional harms.

This report presents the findings obtained in online interviews with selected AIC 2018 survey participants as well as the results of the latest AIC identity crime survey, conducted in 2019. The results of relevant international publications that demonstrate previous exposure to biometrics in Australia and overseas are also presented by way of comparison. This report also examines the increasing willingness of individuals to use biometric technologies in the future, advantages, challenges, future developments and the restraints of implementation including expense, privacy and ethics considerations.

Introduction

As part of the Australian Government's National Identity Security Strategy (AGD 2013), a sample of 10,000 Australians was surveyed about their experience of identity crime and misuse. In addition to determining how prevalent misuse of personal information was, the survey investigated how willing respondents would be to use various biometric technologies to protect their personal information in the future. This report presents the results of extended online interviews with 99 selected members of the 2018 survey cohort for a more intensive analysis of the following topics:

- individual knowledge of biometric technologies and how they are used;
- individual perceptions of advantages and problems with systems currently in use;
- attitudes towards the use of facial recognition; and
- willingness to have a computer chip implanted beneath their skin for digital identification purposes.

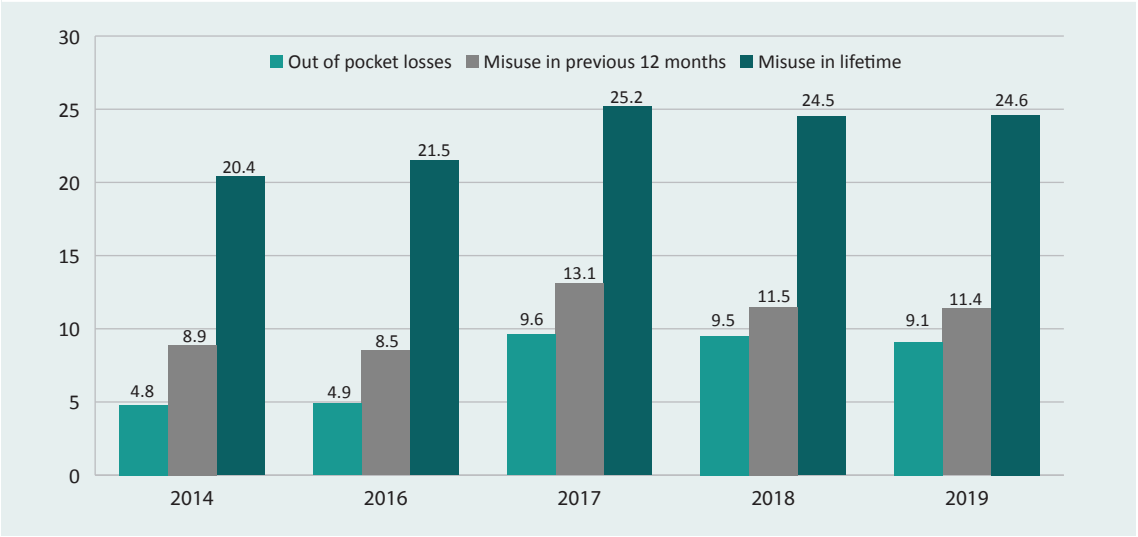
This report also presents the findings of the AIC surveys conducted in both 2018 and 2019 (Jorna, Smith & Norman 2020 and Franks & Smith 2020 respectively) that relate specifically to previous use of biometrics and willingness to use biometrics in the future.

Background

Prevalence

One-quarter of respondents to the AIC 2019 survey (25%) reported having experienced misuse of their personal information at some point in their lifetime, the same proportion as in 2018 (Franks & Smith 2020). Just over 11 percent of respondents reported having had their personal information misused in the last 12 months, also consistent with 2018 findings (Franks & Smith 2020). Franks and Smith (2020) also found that the majority of survey respondents (97%) believed identity crime and misuse in the Australian community was a serious issue, with nearly two-thirds (63%) of the cohort perceiving the risk would increase within the year (Figure 1).

Figure 1: Lifetime victimisation rates of respondents (weighted data) (%)



Source: Identity crime surveys 2014, 2016, 2017, 2018 and 2019 [AIC data files]

Costs

The estimated direct and indirect cost of identity crime in Australia in 2018–19 was $3.1b—17 percent more than for 2015–16 (Smith & Franks 2020). Even accounting for inflation over the three years of 5.4 percent (1.8% per year; Reserve Bank of Australia 2020), this increase is considerable. The total includes losses suffered by government agencies, Australian businesses and individuals. Respondents to the AIC 2019 survey alone reported $3.6m in losses, a substantial 80 percent increase over the $2.0m reported in 2018 (Franks & Smith 2020).

Impact on victims

In addition to the direct and indirect cost of identity crime, over 15 percent of respondents to the AIC survey in 2019 who reported misuse of their personal information stated that they experienced mental or emotional distress as a result, an 11 percent change over 2018 results (Franks & Smith 2020). Franks and Smith (2020) also found that victims required 34 hours on average to deal with the consequences of their personal information being misused, consistent with 2018 findings, and almost all respondents (94%) reported changing their behaviour in some way as a result.

Biometric technologies and identity security

With rapidly developing technology increasing the speed and capabilities of computer processing, as well as increasing the variety of devices and applications available, improved security measures have also been developed that go far beyond password-based authentication systems. Biometric identification is rapidly becoming the primary authentication system in the digital realm. Biometrics refers to the measurement of biological systems. Biometric technologies conduct and use those measurements to confirm matching of data samples against previously collected digital information from users. Biometrics identify people by measuring some aspect of individual anatomy, physiology, a skill, a behaviour or a combination of these things (Anderson 2020).

Facial recognition is probably the oldest identification mechanism of all, with human cognitive functioning evolving to provide efficient ways of recognising other people's facial features and expressions (Anderson 2020). Handwritten signatures appeared as far back as classical China but since the Electronic Signatures in Global and National Commerce Act of 2000 (15 USC 96, 114 Stat 464) came into effect in the United States, contracts can now be legitimised by simply ticking boxes on web pages (Anderson 2020).

In ancient Babylon, fingerprints were used for business transactions. Using fingerprints to identify people was discovered under varying circumstances around the world, mentioned as early as the seventeenth century following the invention of the microscope in Europe (Anderson 2020). Anderson (2020) also tells of 225 Irish citizens using their fingerprints to sign a petition in 1691 asking for reparations following the siege of Londonderry by King William.

Facial recognition is considered to be the biometric technology most likely to increase in use over the next few years, as reported in the findings of the Biometrics Institute's annual surveys of members and stakeholders. These surveys have been conducted since 2010 and all Biometrics Institute members and stakeholders worldwide are invited to participate. A record 453 individuals responded to the Biometrics Institute (2019) survey, a 46 percent increase over the 2018 survey response (310). Respondents represented suppliers of biometrics (50%), users (34%), universities (8%), international organisations (6%), regulatory bodies (3%) and other interested parties (7%; Biometrics Institute 2019).

How biometrics work

Biometric authentication, unlike the use of passwords or token-based authentication systems (key card, fob, photo ID), relies on unique biological characteristics to verify an individual's identity. It is generally more convenient for users to not have to remember passwords or carry a physical identification document that can be easily lost or stolen. The authenticator is also a definable part of the individual and therefore much more difficult to forge.

Signatures

Handwritten signatures have a high forgeability and are a fairly weak security method, despite being used for centuries prior to digital technology. Initially, signatures were required on the backs of credit cards for additional verification until the adoption of the PIN by smartcard industries (Anderson 2020). Online signature firms are now able to generate through cloud services legally binding signatures that are basically machine-written on electronic documents (Anderson 2020). However, handwritten signatures are still used for most legal contracts and photo identification and require witness verification and/or notarisation by a government-appointed official.

Fingerprints

One of the first recorded cases of law enforcement using fingerprint recognition occurred in Buenos Aires, Argentina, where police used a latent fingerprint to solve a double homicide in 1892 (Aware 2020). Police agencies around the world began using fingerprints to solve crimes shortly after, with the New South Wales Police taking up the technology in 1903 (Sydney Morning Herald 2003).

Fingerprint recognition is now used for many applications outside of law enforcement that include mobile authentication, physical access control, onboarding, and both private and government identification. In countries with high levels of illiteracy, fingerprints are used by banks to identify customers. Aadhaar is the national system created by India that maintains both fingerprints and iris codes of most residents; it was initially designed to support welfare payments but is now used to open bank accounts, register mobile phones and facilitate crime scene forensic investigations (Singh 2018).

Like most biometrics, fingerprint algorithms compare features from an original registration template sample with a newly collected sample. A fingerprint record can include data from a single finger, multiple fingers and palms (Aware 2020). Automatic fingerprint identification systems look at the pattern of ridges that cover the fingertips, classifying branches and end points of those ridges, with some also looking at the pores in the surrounding skin (Anderson 2020).

An advantage of fingerprint authentication is that it is a technology most people are familiar with and use regularly to access their mobile devices. It is relatively cost effective and easy to use across systems; however, the variance of technology can be a disadvantage, with cheaper systems having increased rates of false negatives and false positives (Anderson 2020). Errors have also occurred due to age, birth defects, injury or other type of surface damage.

As Anderson (2020) has explained, fingerprint identification systems can be attacked in many ways both electronically and through physical manipulation of the fingers being scanned or order of the fingers being scanned. Despite their varying limitations, the presence of a fingerprint identification system can itself be a deterrent for identity fraud.

Voice recognition

Voice recognition analyses a person's voice to verify their identity. Airways and soft-tissue cavities, as well as the shape and movement of the mouth and jaw, influence voice patterns to create a unique 'voiceprint' (Aware 2020).

A primary use of voice recognition is for hands-free mobile authentication, a safe driving alternative when facial recognition, fingerprint recognition and other forms of biometric authentication are unsafe. Government services and private organisations are also using voice recognition for over-the-phone identity verification that unlocks specific account holder functions. In forensic phonology, used for criminal investigations, a recorded voice is compared with speech samples of all viable suspects (Anderson 2020).

Voice recognition offers some advantages:

- accessible for authentication on all digital devices with microphones;
- cost effective, convenient and familiar;
- contactless, less invasive and more hygienic; and
- useful for phone-based business such as customer service call centres.

Voice recognition also has disadvantages:

- not as accurate as some other biometric technologies;
- requires liveness detection to verify sample authenticity; and
- background noise can impact the sample and matching.

Facial recognition

Facial recognition applies biometrics to the human face using algorithms that map out feature points such as eyes, eyebrows, nose, mouth, cheekbones, chin and ears. The same template versus sample comparison method applies, sometimes using liveness detection to ensure that the sample is not a digital or paper reproduction (Aware 2020).

Law enforcement agencies use facial recognition technology primarily to search for criminals and identify persons of interest. Extended government use includes customs and border security, fraud prevention and personal identification. In the private sector, mobile authentication has become the most common use of facial biometrics as a password alternative. Healthcare organisations have also begun taking advantage of the technology to enhance patient identification.

Facial recognition does have some advantages over other biometric security solutions. There is a considerable amount of digital facial image data freely available from public sources to train algorithms using machine-learning techniques (Aware 2020). With the proliferation of smartphones, tablets and computers with built-in cameras, the convenience of collecting live samples is also a benefit. Creating images can also be performed at the same time as other verification processes such as voice recognition, fingerprint scan or keystroke patterns (Aware 2020).

There are some obvious challenges with facial recognition such as the effect of lighting, ageing, and the presence of glasses or facial hair, extending to include arguments of racial and ethnic bias. Camera technology can also lead to conflicting matching results occurring. A challenge for facial recognition technology is the number of images available online through social media and other website profiles, giving criminals the means to access potential fraud victims via free, online public access to their posted and shared photos. More sophisticated facial recognition systems, such as those used for airport passenger verification, require multiple images for enrolment rather than a single stored image, and more complex matching processes.

Iris scans

The iris, an eye muscle that regulates pupil size, contains patterns unique to each individual. This led to the development of iris recognition technology for identity verification in the 1990s (Aware 2020). Iris pattern recognition has the best error rates of any automated biometric system measured under lab conditions, with patterns different even for identical twins and between both eyes of a single individual. (Anderson 2020). The speed and accuracy of iris recognition technology made it more commercially available as a form of biometric identification dating from 2005, when the original patents expired and gave rise to private industry competition (Anderson 2020).

Iris recognition is used for a variety of identity verification purposes ranging from mobile phone authentication to border management programs and physical access control for both private and government organisations. Iris biometrics need no physical contact when scanning and can be captured from a fair distance with advanced equipment, producing extremely accurate matching. The human iris also appears to be relatively stable throughout a person's lifetime and is very difficult to forge (Anderson 2020).

Disadvantages of using iris data are the expensive equipment required for the most accurate results and it can be traumatic for some individuals to have their eyes scanned. It must also be noted that iris recognition is different from retinal recognition, which establishes uniqueness using the arrangement of blood vessels on the retina at the back of the eye. For the purpose of this report, retina scans will not be discussed further.

DNA

Deoxyribonucleic acid (DNA) is the hereditary material in animals that has become a valuable tool for crime scene forensics and verifying child parentage. Although able to achieve much more precise verification of identity than other biometrics, some argue (eg Anderson 2020) that DNA is too slow and expensive for commercial use, and it also faces opposition from privacy advocates. There are also human error factors to consider such as careless collection and management of samples of DNA, and poor laboratory procedures and record-keeping in certain cases. For example, the United Kingdom maintains one of the largest DNA databases in the world (6 million records) but it has been alleged that approximately half a million of those records have misspelled or completely wrong names associated with DNA samples (Anderson 2020).

Human chip implant technology

Arguably adjacent to biometric technology is biohacking, or the modification of human bodies with the use of technology. Developing from wearable devices such as fitness trackers, these technologies have been extended to include human microchip implantation as one of their services. Individuals and businesses are hosting 'implant parties' where groups of people have small chips similar to those used for pets inserted under the skin, usually in the hand between the thumb and forefinger (Ma 2018). These chips are used in the same way as a key card to unlock locations or services, waving a hand in front of a scanning device instead of using a physical identifier.

While some large, multinational companies are in discussions with biohacking organisations to enrol their employees with microchips, human rights and privacy groups are concerned that employees could be coerced into using the technology under threat of termination of their employment unless they consent to the procedure (Kollewe 2018).

Despite concerns, the technology is spreading and gaining popularity around the world, including in Australia. Human microchip and implant services began several years ago, with Sydney-based company Chip My Life (2020) currently offering both a radio frequency identification (RFID) implant ($83) and a near-field communication (NFC) implant ($155), with an additional charge of $75 for the implant procedure. An RFID implant can be used for simple data transmissions of things such as account numbers/verification and is read at short range via radio waves powered by the reader (Hoffman 2016). The NFC implant has evolved from the RFID technology and is a method of wireless data transfer where one chip detects then enables another in close proximity to transfer small amounts of data (Faulkner 2017).

Use and misuse of biometric technology

It was generally perceived by those who were interviewed as part of the AIC's qualitative research that biometric technologies were not without problems and could be compromised by offenders and misused by government entities or private organisations. The issues of secure data storage, data access and privacy were also found to be important to those interviewed. In the United Kingdom, the Ada Lovelace Institute (2019) survey reported that people fear the normalisation of surveillance, support police use of biometrics only with limitations and do not trust the private sector to use facial recognition technology. Function creep (using technology for purposes not previously disclosed) is a repeated worry for individuals who believe an opt in/opt out policy with full user consent should be the accepted norm.

The Biometrics Institute's (2019) survey of industry experts reported that the most important development in the use of biometrics is in the areas of border control/security and mobile identity managed by smart devices. These findings are consistent with the results of both the AIC and Ada Lovelace Institute surveys, which demonstrate overall support for government use of biometrics for national security purposes and technology offered as security for smart devices such as fingerprint scans and facial recognition.

Advantages

There are many advantages to using biometric technologies as security solutions to identity crime. Conventional user-authentication systems such as passwords or PINs have become impractical and subject to the ever-evolving techniques of cybercriminals to compromise and misuse personal information. The need to constantly change passwords/PINs has led users to complacent actions such as keeping paper copies of codes or relying on electronic files and password keeper apps, which themselves can be compromised and make one ineligible for compensation if fraud occurs (Smith, Gannoni & Goldsmid 2019). Scammers also target devices that use passwords and PINs for skimming such as ATMs and EFTPOS machines. Biometrics have faster processing times and can be easily integrated with other authentication processes. They do not require users to remember a phrase or number code as it is their own individual characteristics that unlock the security feature, making it much more difficult for criminals to falsify. With rapidly developing technology, and the recent introduction of biometrics-as-a-service (BaaS) options, the overall costs of biometric technologies are decreasing, making them more readily available.

Challenges

As with all technology-based systems, there is always a risk of failure due to hardware malfunction, software corruption or human implementation error. Environmental conditions can also upset machine-based devices, especially those capturing biometrics: dust, noise, vibration, lighting and humidity are the most common problems.

Some of the biggest challenges when implementing biometric technologies to identify individuals relate to the associated risk to privacy and the potential for unauthorised tracking of transactions or user locations. Many are concerned about governments exceeding their authority by using biometrics to identify individuals for data-matching, identification and surveillance purposes (Smith, Gannoni & Goldsmid 2019; United States Government Accountability Office 2002). Smith, Gannoni and Goldsmid (2019) argue that the efficiency of biometric technologies makes allegations of intentional function creep more legitimate than with conventional authentication systems.

Some biometric systems also have difficulty in matching data for some subjects. Anderson (2020) found that the elderly and manual workers often have damaged or abraded fingerprints and people with dark eyes/large pupils have difficulty using iris recognition systems. Rhue (2018) argues that a person's race influences how facial recognition software interprets facial expressions, and a lack of uniformity in this software means that bias may be introduced through various mechanisms. Additional challenges stem from fraudulent enrolment in biometric systems. If a false or fabricated identity is used to enrol in a government or business biometric system, it would be difficult to detect the fraud, challenge the enrolment and locate the individual responsible (Smith, Gannoni & Goldsmid 2019). Rowe et al. (2013) and Smith, Gannoni and Goldsmid (2019) identified various crime displacement risks associated with biometric technologies, raising concerns that individuals could be threatened with violence unless they present themselves to allow access to secure buildings/terminals or withdraw funds from ATMs or banks. End-user resistance to the use of biometrics due to health, security or privacy concerns is another challenge that has emerged from the present research. Biometric systems are also very expensive to implement and maintain; however, this problem is now solvable for smaller organisations with BaaS, discussed in more detail later in this report.

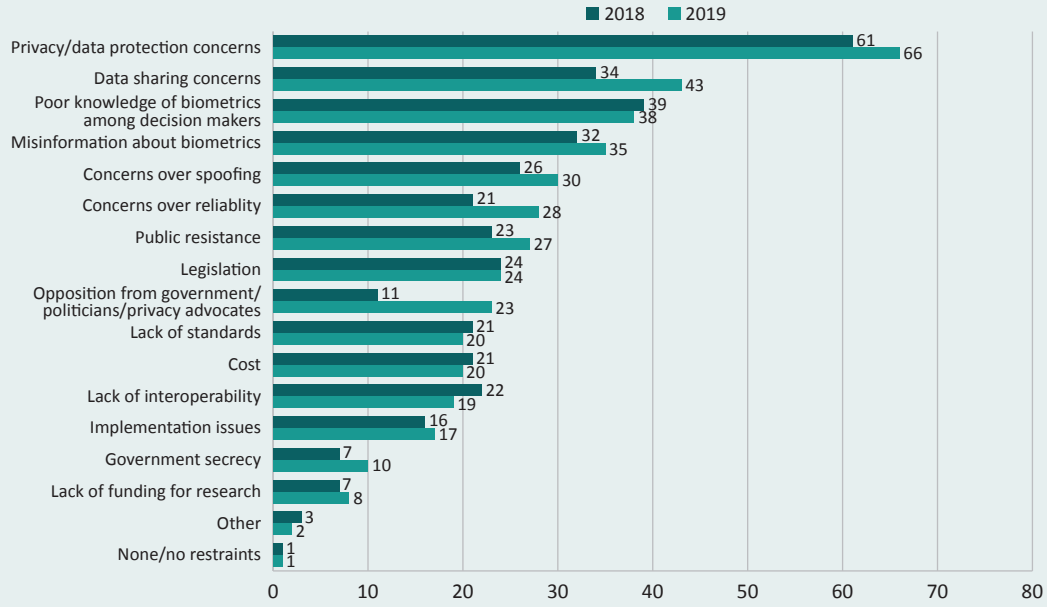
Attitudes towards biometrics

When reviewing prior research investigating people's willingness to use biometric technologies to minimise the risks of identity crime and misuse, Riley et al. (2009) discussed how cultural differences should be considered during design and implementation of biometric systems. Semnani-Azad et al. (2019) considered the importance of societal acceptance and trust, and the impact of cultural norms on trust levels. Indeed, public trust is a primary factor in the acceptance of biometric technologies, as is confirmed by survey results discussed in this report.

Results of the AIC surveys found that most participants were comfortable with biometrics being used for security purposes, or to access buildings, personal devices or government services (Franks & Smith 2020; Jorna, Smith & Norman 2020). The Ada Lovelace Institute (2019) undertook a survey to determine public attitudes to facial recognition technology in the United Kingdom and found majority support when there was a demonstrable public benefit; however, there was limited, conditional support for police deployment and substantial mistrust in private sector use.

The Biometrics Institute (2019) survey of industry stakeholders reported the biggest market restraint to the technology as relating to privacy/data concerns at 66 percent in 2019. Similarly, data-sharing concerns ranked as the second largest market restraint at 43 percent (Biometrics Institute 2019; Figure 2).

Figure 2: Market restraints for biometrics, 2018 versus 2019 (%)



Source: Biometrics Institute 2019

Purpose of this report

This report examines the changing perspectives of users towards the use of biometric technologies in Australia and overseas. It investigates current public knowledge and awareness of biometrics and the willingness of individuals to use the various technologies in specific circumstances. It also examines the benefits and challenges associated with the use of biometric systems and the associated costs and restraints of implementation such as ethics considerations, privacy issues and data-sharing/security concerns.

Methodology

AIC surveys—research design and definitions

The AIC identity crime surveys employed a quantitative, cross-sectional survey design, examining identity crime and misuse of personal information among a sample of Australian residents in varying age groups ranging from 15 to 24 years of age up to over 65 years of age. This methodology has been replicated annually since 2013 (with the exception of 2015; see Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018; Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman 2020; and Franks & Smith 2020).

The definition of identity crime and misuse of personal information used in the surveys was:

> obtaining or using your personal information without your permission to pretend to be you or to carry out a business in your name without your permission, or other types of activities and transactions. This does not include use of your personal information for direct marketing, even if this was done without your permission.

Personal information was defined as including:

> name, address, date of birth, place of birth, gender, driver's licence information, passport information, Medicare information, biometric information (eg fingerprint), signature, bank account information, credit or debit card information, Personal Identification Number (PIN), Tax File Number (TFN), Shareholder Identification Number (HIN), computer and/or other online usernames and passwords, student identification number and various other types of personal information.

Survey questions

A questionnaire was administered online that contained a mix of closed-response and open-ended questions on the following topics:

- demographic and other characteristics of respondents including age, gender, usual place of residence, income, language spoken at home, Aboriginal and Torres Strait Islander status and computer usage;
- experience of misuse of personal information and method of victimisation;
- actual financial losses, funds recovered and other consequences of victimisation;
- whether and how respondents reported misuse of personal information and their satisfaction with the responses;
- behavioural changes arising from the misuse of personal information;
- awareness of the availability of court-issued Victims' Certificates;
- perceptions of the seriousness of misuse of personal information;
- perceptions of the risk of identity crime over the next 12 months; and
- use of security measures, including biometric technologies, in the past and willingness to use them in the future to reduce the risk of identity crime victimisation.

The questions were replicated between surveys so that direct comparisons could be made with earlier findings. The questions were developed by the AIC in consultation with the Department of Home Affairs.

The questions spanned a number of reference periods. Demographic questions (eg usual place of residence, age and income) related to respondents' circumstances at the time of responding. Other questions asked about lifetime experience of identity crime and misuse, as well as identity crime and misuse in the 12 months prior to completing the survey. The most recent survey was available for completion from mid-December 2019 to early January 2020 (hereafter referred to as the 2019 survey). The survey had 40 questions in total and took approximately 10 to 15 minutes to complete.

Qualitative research by the Australian Institute of Criminology

In the AIC 2018 survey, respondents were asked if they would be interested in participating in further research in the form of online interviews. Of the 9,911 survey respondents, 4,903 (49%) expressed a willingness to participate in further research concerning four topics (below). Of those willing to participate, 30+ members of each group were randomly selected , with 99 individuals in total eventually able to complete the online interviews. The 99 individuals who completed the interviews provided 117 unique responses, as some multiple group participation was required due to participant withdrawal:

- Group 1 (31 participants): knowledge of biometrics and how they are used;
- Group 2 (28 participants): use and misuse of biological biometrics (advantages and problems with current systems);
- Group 3 (30 participants): opposition to facial recognition (unwilling to use facial recognition to prevent misuse of personal information); and
- Group 4 (28 participants): willingness to have a computer chip implanted for ID verification, what government agency, organisation or individual should cover the costs, and perceived associated risks of human microchip technology.

In Group 4 only 11 new individuals initially completed these interviews, and in order to boost the numbers a further 17 were recruited from those who had already participated in the other groups of questions, making a total of 28 who completed the questions in Group 4.

The selection of interviewees was undertaken by i-Link Research Solutions in 2019, the company that undertook the online survey in 2018. The online interviews were then moderated by Footprints Market Research, as contracted by the AIC, using the i-Discuss online interview platform provided by i-Link Research Solutions. The AIC provided additional questions to i-Link to be used on the i-Discuss qualitative boards in three-hour blocks to allow for real-time researcher response. Members of each group were interviewed over a three-day period for a combined fieldwork period of 12 days.

As with the initial AIC survey, participation was voluntary, with the subjects offered incentives from the external provider (i-Link) in exchange for completing the survey. It was acknowledged that while risk of psychological distress associated with the research was minimal, there was a possibility that a participant might feel uncomfortable answering questions about victimisation and as a result withdraw from the interview at any time. A plain language statement was also provided explaining the nature of the research and contact information for those participants who felt they might need victim support.

Because the total number of 99 individual interviewees was only one percent of all those who participated in the AIC survey in 2018, the question arises as to how representative the interviewees were of all survey participants. I-Link Research Services provided information on the demographic characteristics of the 99 interviewees and whether or not they had been victims of identity crime, to enable the AIC to compare these findings with the full online survey sample of 9,911.

Of the 99 interviewees, 31 percent had experienced identity crime at some point in their lifetime and 10 percent in the previous 12 months, both comparable with the AIC online survey cohort of 2018 (25% and 12% respectively; Jorna, Smith & Norman 2020). However, 62 percent of interviewees were women, a significant 11 percentage points more than the proportion of women recorded by Jorna, Smith and Norman (2020) in the 2018 survey (51%; N–1 $\chi^2(1)=4.574$, $p<0.05$).

Generally, the 99 interviewees had largely similar demographic characteristics and demonstrated similar willingness to use biometrics when compared with the AIC survey cohort in 2018. The only significant differences recorded between the survey participants and the interviewees were in previous use of voice recognition and human microchip implants as well as future willingness to use voice and facial recognition technologies. Some 34 percent of interviewees stated they had previously used voice recognition technology compared with 20 percent of the AIC 2018 survey cohort (N–1 $\chi^2(1)=12.682$, $p<0.001$). No interviewees had previous experience of human microchip implants, compared with seven percent of the 2018 survey cohort (N–1 $\chi^2(1)=6.990$, $p<0.01$). In considering future willingness to use biometrics, those interviewed were less willing when it came to both voice recognition (63% vs 72%; N–1 $\chi^2(1)=4.700$, $p<0.05$) and facial recognition (61% vs 72%; N–1 $\chi^2(1)=11.906$, $p<0.001$) technologies. These relatively small differences between the interviewees and the 2018 survey respondents should be taken into consideration when interpreting the following qualitative findings.

Ada Lovelace Institute survey

The Ada Lovelace Institute is an independent research and deliberative body dedicated to ensuring that data and artificial intelligence (AI) work effectively for people and society. Its core belief is that the benefits of data and AI should be justly and equitably distributed for the purpose of enhancing both individual and societal wellbeing.

In 2019 the Ada Lovelace Institute commissioned YouGov in the United Kingdom to undertake an inaugural survey to understand public attitudes in Britain regarding the emerging public and private sector deployment of facial recognition technology. A sample of 4,109 adults from across the United Kingdom captured the public's initial response to a range of scenarios outlining specific applications of facial recognition technology in different sectors and for various purposes (Ada Lovelace Institute 2019). Areas of discussion included individual awareness and consent, police use, the normalisation of surveillance, government and private sector applications, and public trust.

Biometrics Institute surveys

The Biometrics Institute was founded in 2001 to promote the responsible and ethical use of biometrics and biometric analytics as an independent and impartial international forum for biometrics users and other interested parties. The Biometrics Institute distributes an annual survey to thousands of members, key stakeholders and media contacts to provide an insight into trends and developments in the biometrics industry.

In its tenth year, the Biometrics Institute's 2019 survey registered a record 453 individual responses from around the globe, an increase of 46 percent over 2018 (*n*=310), and included a combination of supplier organisations, government organisations, banks, airlines, universities, regulators and other non-government organisations (Biometrics Institute 2019). The survey offers a gauge of industry attitudes towards biometrics implementation, market restraints and legislation as well as future trend predictions.

Biometrics Institute 2020 survey

Shortly before the release of the present report, the Biometrics Institute published its eleventh survey of industry stakeholders (Biometrics Institute 2020). (For access to the full survey results, contact nicky@biometricsinstitute.org.) This survey was distributed in May 2020 at the height of the international restrictions caused by the COVID-19 pandemic. As a result, the Biometrics Institute revised the questionnaire and included questions specific to the impact of the coronavirus pandemic. The survey was circulated to more than 7,000 individuals across the globe, with responses received from 326 industry professionals. Undoubtedly a result of worldwide coronavirus restrictions, the survey response was nearly 40 percent less than for the 2019 survey (*n*=453: Biometrics Institute 2019).

Notable changes were seen between the findings of the Biometrics Institute's surveys in 2019 and 2020, particularly concerning the results of questions about the most significant areas of development in biometrics over the previous 12 months. Respondents identified 'digital identity' (17% of responses in 2020) as the most significant area of development, followed by 'mobile identity' (12%), 'privacy and ethical issues' (11%) and 'biometrics capture via smartphone' (10%).

'Digital identity' was also seen as the top area in which respondents expected to see the most significant developments over the next five years, followed by 'artificial intelligence' and 'biometrics and hygiene issues'.

In response to questions about the impact that the COVID-19 pandemic would have on the way in which biometrics are used and implemented, 60 percent indicated that such changes would occur, with the majority of responses referring to the likely move towards contactless/touchless modalities. The overall survey results demonstrate how societal changes can quickly alter perceptions of and affect future developments in biometric technologies.

Findings: Knowledge and use of biometrics

Awareness of biometrics and how they work

Biometric technologies are currently used by government agencies, businesses and individuals across Australia for various identity verification purposes, ranging from passport identification and Centrelink access to digital payment verification and mobile device logon. Biometrics are a rapidly growing technological solution with robust identity security capabilities. With the increasing prevalence of identity crime in Australia and abroad, it is imperative to understand public perceptions of these technologies and how they operate. The rapid development of the biometrics industry has also seen a growth in public mistrust of these technologies due to concerns over privacy laws and ethics policies that need to be explored. Public trust plays a central role in the acceptance of any new technology and more information is needed on the vulnerabilities of systems to bias, fraud and misuse. Further research is also needed on the roles of facial recognition, AI and the normalisation of surveillance.

Public awareness of biometric technologies has generally been high since the introduction of fingerprint and facial scanning applications on personal mobile devices. Franks and Smith (2020) found more than three-quarters (76%) of respondents had previously used some form of biometric technology. In the United Kingdom, only 10 percent of the Ada Lovelace Institute (2019) survey cohort admitted to not knowing anything about facial recognition technology.

Uses of biometrics

It emerged from the extended interviews with the AIC 2018 survey cohort that interviewees understood biometrics to entail the use of an individual's unique biological characteristics (facial, iris, fingerprint) as a means of conducting personal identification. Those interviewed understood the purpose of biometrics as being to enable access to devices, accounts or locations with the aim of preventing personal identity theft and ensuring general safety for the community. Some of the interviewees also mentioned the use of biometrics to track people of interest (ie by law enforcement), with the objective of strengthening the safety and security of communities. For example, one interviewee said:

> Biometric technologies may be used for identification purposes, controlling access to devices and systems, tracking individuals that are under surveillance.

The three principal uses of biometrics as described by interviewees were:

- accessing technology including smartphones, tablets and computers/laptops together with apps, programs and account information accessible through these devices;
- border control/airports, using facial recognition; and
- voice recognition to access government services such as Centrelink.

Some people also described a world in which biometrics would be all-pervasive. One interviewee noted:

> I believe biometrics can be used in endless situations. Government services like Centrelink/Medicare could use it for quickly accessing a customer's information including form lodgment. Courts could use it to scan people in and direct them to the right court. I believe the future will have all our info networked for security reasons so even if the technology is just used to check that we are not illegals, overstaying visas, or on criminal watchlists most companies will use this tech for this purpose in the future.

When questioned specifically about how biometric systems work, most were able to describe the enrolment and matching processes but few understood how biometrics work for watch-list matching except for what they had seen on digital entertainment:

> I have seen this done on some TV shows where they have a photo of a person then scan a crowd to find that person.

Of the more than 4,000 respondents to the Ada Lovelace (2019) survey, which focused specifically on facial recognition, 90 percent were aware of the technology but only 53 percent stated they knew specifics about its deployment. Thirty-six percent said they were aware but did not know anything specific about facial recognition systems and 10 percent said they were not aware of the technology at all (Ada Lovelace Institute 2019). The Ada Lovelace Institute (2020) survey found few respondents were aware that facial recognition was used outside of policing and airports, with less than 15 percent realising deployment has reached workplaces, shops and commercial premises. The Biometrics Institute (2019) survey cohort are all industry stakeholders and maintain a strong knowledge of the available systems and their functions.

Data storage, security of information and misuse

All human interaction with digital technologies results in an assemblage of data, including biometrics. Personal digital data stored on mobile devices are self-managed by the owner of that device; however, cloud technology has moved storage from devices to servers that offer larger storage capacity and up-to-date security software (Lupton & Michael 2017). The majority of the AIC interviewees did not concern themselves with what happens to that data and assumed that data were secured by the service provider. Lupton and Michael (2017) argue that these data assemblages are sometimes procured by outside actors and agencies, including hackers and cybercriminals.

AIC interviewees had little understanding of data security and assumed biometric data were stored in one of three conventional ways:

- government and/or police databases;
- commercial organisation using the biometric data (eg banks); or
- local storage on a personal device (eg mobile phone).

Based on the responses received from those interviewed, data storage and security were topics where specific information was unknown; however, most maintained low levels of concern. There was also an overall sentiment that the government and hackers could potentially access data:

> “I would assume it is stored in a large digital database that was secure with limited/few people having access to this sensitive information. It’s always a concern regardless of any place or business: the risk of sensitive digital information being accessed or hacked by the wrong people and used for identify fraud.

Interviewees recognised the value of their data for national security purposes, controlling crime and so on but also realised that their data had a commercial value. Interviewees also noted the need to balance security interests with privacy concerns:

> I personally feel that biometrics in the future would be more common and I don't really feel comfortable with that. I already feel that Big Brother is watching every movement we make and this is just next level.

General misuse of biometrics was described by interviewees based on what they had seen in movies such as tricking iris scanners with a printed contact lens. The majority of those surveyed did not express personal concern over this type of misuse:

> I have only seen it on fictional TV programs where someone has produced a contact lens that has someone else's eye details on it.

> It doesn't concern me on a personal level, but as a country I do believe that our security is always at risk.

> I'm not particularly concerned at the moment but possibly in the future as technology seems to be becoming more advanced and security for technology is moving more towards biometrics rather than a password.

When asked which biometrics were most vulnerable to misuse, the top three responses provided by interviewees were fingerprint, voice and facial recognition. The Ada Lovelace Institute and Biometrics Institute surveys did not directly consider questions of user awareness of data storage, security of information and misuse.

Surveillance of public spaces

Surveillance technologies, including camera-based facial recognition, have redesigned physical public space as government, business and anyone with a mobile device can combine to create complex interactions of surveillance. Political and ethical problems associated with surveillance of public spaces have been an ongoing area of research and debate. Hall (2017) discusses how scholars have been tracking intensive and extensive expansions of surveillance in the name of risk management.

When asked about the process of law enforcement using biometric technology to search for individuals listed on government watch-lists, the AIC interviewees were generally knowledgeable about the concept of camera surveillance in public spaces but knew little of the specific procedures involved:

> I am aware of the plans to introduce cameras into public areas but I'm not sure how many are operating at the moment. I presume the relevant authorities would be able to scan through the pictures to find the match they were looking for.

There was a general acceptance of crowd surveillance for identifying known offenders but there were concerns held by interviewees regarding misuse and error:

> This sounds like it is exactly what this technology should be used for. Therefore, no objections whatsoever. Whoever is on the database has already demonstrated that they should be there.

> [Criminals] may have already paid for the previous crimes to society and they still get harassed when they haven't done anything.

With the exception of using biometrics for identifying known offenders, there was a general lack of acceptance of public crowd surveillance shown by the interviewees:

> Don't think this would be a great idea, I guess you could use it for monitoring but I feel like your privacy would be impeded as an individual going about your daily life.

> I feel our sense of privacy would vanish as we would be constantly watched wherever we go if everyone was subject to facial recognition.

Overall, around two-thirds of the AIC survey respondents considered government use of facial recognition was acceptable for the following purposes: detecting terrorists by government agencies (67%), airport security (66%) and detecting criminals by police (64%; Franks & Smith 2020).

Public support for facial recognition in the United Kingdom is similar to that found in Australia and conditional on public safety, with 71 percent of Ada Lovelace Institute (2019) participants agreeing to police use in public spaces provided it helps reduce crime. The Ada Lovelace Institute (2019) survey concluded that, although the general public fear the normalisation of surveillance, there is acceptance of the use of facial recognition technology when there is a clear public benefit. The majority of those surveyed (70%) agreed that the police should be allowed to use the technology in criminal investigations.

Access to information on biometric systems

Public understanding of biometric technologies and how biometric systems work is often lacking. The AIC interviewees felt the Australian Government has not supplied the public with adequate information on biometric technologies or how their personal information is being used, stored and protected:

> The government hasn't really communicated this to the community, has it? I have no recollection that the Commonwealth Government has made any effort to tell me what it does with my information.

A general view of those interviewed was the need for communication through multiple channels that was easy to understand across all demographics. The Ada Lovelace Institute (2019) survey did not address user opinions about biometrics information access.

The Biometrics Institute survey results were not directly comparable as they represented government, educational and private sector entities that are directly involved in the biometrics industry. For this reason, all survey participants had a general understanding of biometric technologies and their current usage. Interestingly, two factors considered to be restraining the biometrics market as listed in the Biometrics Institute (2019) survey were 'poor knowledge among decision makers' (38%) and 'misinformation about biometrics' (35%).

Understanding use of biometrics among different demographics

The AIC survey data were weighted by age and gender using census data from the Australian Bureau of Statistics (2019) to reflect the spread of the Australian population. Respondents included individuals aged from under 25 years to 65 years of age and over. The distribution of survey respondents by usual place of residence closely aligned with the Australian Bureau of Statistics (2019) demographic data and almost all survey respondents (93%) indicated that English was the language most often spoken at home. Four percent of survey respondents self-identified as being of Aboriginal or Torres Strait Islander descent or both. Respondents most commonly reported having an income of between $37,000 and $80,000 (31%), with time spent on computerised devices averaging 36 hours per week (Franks & Smith 2020).

The AIC interviewees were presented with research findings about biometric usage being more prevalent among older people (55 and over) than younger people (24 and younger) and asked to provide possible reasons for this. It was found that interviewees thought that older users tend to prefer using biometrics rather than remembering passwords, and emphasised national security reasons and the prevention of identity theft as additional justifications. Many were surprised by this information, citing reasons such as:

- older people favouring the ease of biometrics over remembering passwords, placing greater importance on identity theft and national security; and
- older people being less informed and/or more trusting about the use of biometrics.

> “I wonder whether more mature people are more conscious of crime and feel that this way will help eliminate the chance of people getting their information.

> “I would assume that older people (aged 55 years or more) would feel more secure using biometrics than a traditional ‘password’. It could also be the case that they are unaware of the cyber risks associated with biometrics.

Interviewees also thought that younger users were less inclined to embrace biometrics, stating that:

- young people are less trusting of the technology/less willing to share their biometric data and have no problem setting up and remembering passwords; and
- young people do not have the time or patience to enrol their biometric data, and may be complacent about its use even with greater exposure to media (films, TV) depicting the issues around cybercrime and identity theft.

> “Young people are probably in a hurry and can’t be bothered to set up the technology.

Many interviewees suggested that biometrics would be less popular for non-native English speakers who may not trust governments to keep biometric data secure due to the following:

- cultural barriers, depending on country of origin, where there may be a mistrust of providing biometric data, particularly to government departments. This includes a perceived lack of control over the use of biological biometrics; and
- language barriers causing difficulties with English-based voice recognition and in understanding the use of biometrics in general if instructions are not available in their native language.

For example, interviewees commented:

> Depending on their history – if they're here as political refugees or are from a country where they do not trust their leaders, they have learnt a healthy distrust of authorities being able to trace them through fingerprints etc.

> Or perhaps it just comes down to finding it hard to follow instructions in English about how to set up and use biometrics.

The other two surveys consulted did not present findings in terms of demographic variables.

Previous use of biometric technologies

In the AIC interviews, one participant commented on previous and frequent use of biometric technologies as follows:

> I currently use biometric technology everyday with my smartphone and tablet. Fingerprint access is quick and convenient for me along with the iris technology to access more personal/private folders within the smartphone. Biometric technology has been such a great welcome in terms of enhanced safety for individuals as well as for companies etc. I've previously tried this form of technology when coming back from an overseas trip and having a machine scan my face at the airport as opposed to waiting in line for customs to check my passport. It is convenient, efficient and fast and makes it great for places like an airport where security can't be compromised yet [there is] the need for quicker movement of people day in and day out, taking the stress out of workers.

AIC survey respondents were asked whether they had ever used particular security measures and how frequently they had used those security measures in the past—for any purpose, not just to prevent misuse of personal information. The most common security measure selected was the non-biometric option, with 97 percent of respondents reporting having used passwords, 86 percent frequently. The most commonly used biometric technology used was a signature, at 76 percent, followed by fingerprints at 63 percent. The least commonly used security measure was a computer chip implanted under the skin, although 10 percent of respondents did report having used this measure (Table 1).

Table 1: Frequency of use of security measures in the past (weighted data)

Security measure	How frequently security measures used (%)			
	Frequently	Occasionally	Rarely	Never
Passwords	85.6	8.6	2.6	3.2
Signatures	28.3	29.7	17.7	24.2
Fingerprint recognition	33.4	16.8	12.6	37.3
Facial recognition	15.5	11.2	14.3	59.1
Voice recognition	7.4	16.6	21.8	54.2
Iris recognition	5.2	6.7	10.0	78.2
Computer chip implanted under your skin	3.1	3.7	3.1	90.0

Source: Franks & Smith 2020

The Ada Lovelace Institute (2019) study, focusing on facial recognition, found that 48 percent of participants claimed some knowledge of the technology, with only five percent stating that they knew a lot of detailed information about it. In comparison, in the AIC 2019 survey 41 percent of respondents stated they had previously used facial recognition technology (Franks & Smith 2020).

Biometrics industry stakeholders who participated in the Biometrics Institute (2019) survey represented a vast majority (87%) who were comfortable as users of the technology as well as suppliers. Surprisingly, 13 percent of industry players surveyed by the Biometrics Institute (2019) stated that they were uncomfortable using biometrics themselves.

Body scans

AIC interviewees were asked about their experience with body scans during security screening. Most of the participants were familiar with the use of body scanners in locations such as government offices, court houses, prisons, police stations, hospitals, banks and airports:

> The airport is one I know of and have used in the past but am also aware some businesses would use this technology too to gain access into secure buildings etc. I would assume the government in some way or another would utilise this technology as they would have a significant amount of data/information that would require the utmost security and only be accessed by the right people.

Comparing biometrics with passwords/PINs

AIC interviewees were divided in their views when comparing biometrics to traditional passwords/PINs. While some agreed biometrics were both easier and more secure, others felt that the technology should be reserved for certain services and products only.

Overall, the AIC interviewees were most comfortable using biometrics for government purposes and mobile device access as opposed to tasks such as shopping, financial transactions and building access. Again, privacy is an issue:

> Biometrics technologies are better at securely identifying you than passwords or PINs as these can be easily hacked into, and you don't have to remember them. Definitely governments would find biometrics more secure as it would be a more effective and efficient way to identify people. Accessing one's phone and gaining access to buildings would be more secure with biometrics instead of passwords or PINs as it saves remembering them and regularly needing to change them. I don't feel that it is necessary for shops and banks to use biometrics. Our personal privacy would be invaded if that happens.

Some individuals felt that they had more control over their personal identification information by maintaining their own passwords/PINs. They were concerned about potential misuse by third parties and felt biometric data being stored on external servers via cloud technology was insecure, open to misuse and limited their access and control:

> I am not comfortable with the government using this technology to control our access. At least with a password/PIN, I have total control over it. But once my facial recognition is stored with the government, I lose total control of my own identity and security. Same argument as communications, shopping/financial transactions/building access…my facial data will be in the hand of private and government hands. Who is going to guarantee that my data is secure?

Previous use of passwords by AIC 2019 survey respondents was, predictably, high at 97 percent; however, future willingness to use passwords dropped to 93 percent for recent victims of identity crime (95% for non-victims; Franks & Smith 2020). These figures demonstrate what appears to be a waning in confidence in the use of passwords. Biometrics offer stronger security and without the necessity of remembering/changing multiple passwords across multiple devices.

Future willingness to use biometrics

AIC interviewees were generally more willing to use biometrics operated by government departments than private sector businesses as they felt their information would be more secure. However, some felt that government agencies were more inclined to misuse data collected for non-disclosed purposes or be targets for hackers while private organisations' concern for branding guarantees more robust security features. Respective interviewee comments are listed below:

> I am more willing to use biometrics by government departments because I feel that usage would have stricter guidelines and regulations and that it would less likely to be misused without actively being beneficial to the individual.

> I don't feel more confident with government biometrics as I think they would be a great target for international hackers. In saying that I would use a Smart Gate if it meant I go through more efficiently. I have had to use numerous in other countries going through customs, and there is no option to NOT use!

All AIC survey respondents were asked whether they would be willing to use various security measures in the future to protect their personal information, with 98 percent stating that they were willing to use at least one of the measures listed. As with the results on previously used security, the security measure that respondents were most willing to use in the future to protect their information was passwords (95%). The most popular biometric technology that respondents were willing to use in the future was fingerprint recognition (83%), closely followed by signatures (81%). Facial recognition ranked the third most popular biometric, at just over 74 percent. Surprisingly, 23 percent of those surveyed stated that they would be willing to use a computer chip implanted under their skin (Franks & Smith 2020; Table 2).

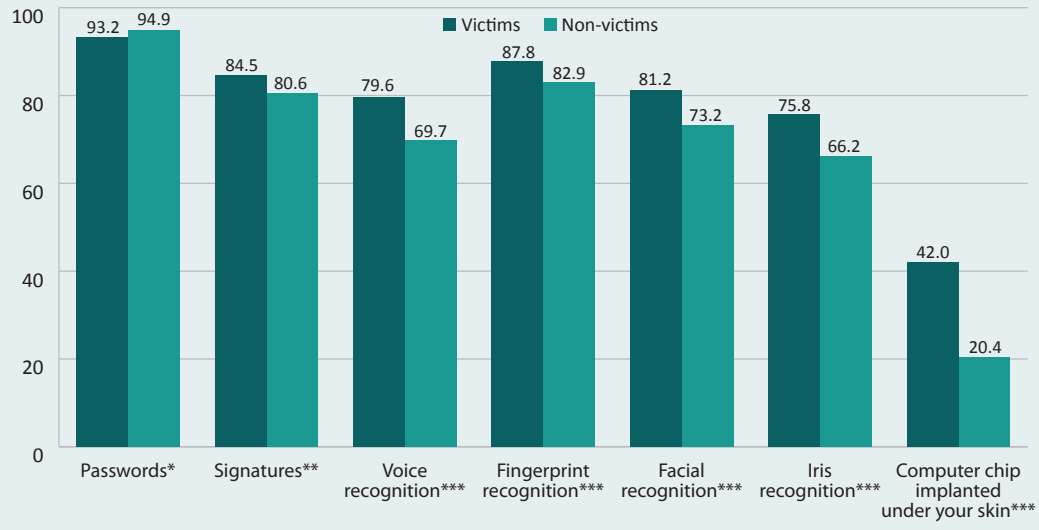
Table 2: Willingness to use security measures to protect personal information in the future (weighted data) (%)

Security measure	2018	2019	% change
Passwords	94.7	94.7	0.0
Fingerprint recognition	84.7	83.4	–1.5
Signatures	81.6	81.1	–0.6
Facial recognition	75.6	74.1	–2.0
Voice recognition	72.4	70.8	–2.2
Iris recognition	68.6	67.3	–1.9
Computer chip implanted under your skin	22.3	22.9	2.7
Any of the above	97.9	98.0	0.1
None of the above	2.1	2.0	–4.8

Note: Respondents could select multiple responses
Source: Franks & Smith 2020

Additional analysis of AIC survey responses examined whether willingness to use security measures in the future to protect personal information was associated with experience of personal information misuse in the previous 12 months. Recent victims were more willing than non-victims to use all suggested security measures with the exception of passwords (Figure 3). Passwords are generally the primary method of digital security for individuals. Once compromised, victims will look for alternative methods that they perceive to be potentially more effective, making them significantly more willing to try technologically advanced biometric options and computer chip implants.

Figure 3: Willingness of victims and non-victims of personal information misuse to use security measures to protect personal information in the future (weighted data) (%)



***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$
Source: Franks & Smith 2020

Overall, the majority of AIC survey respondents expressed a greater willingness to use biometric technologies issued by government departments and for public safety (Franks & Smith 2020). These sentiments were consistent with the Ada Lovelace Institute (2019) survey cohort, who declared an overall distrust (70%) of private sector usage of facial recognition technology and suggested that user consent and an opt in/opt out (46%) policy be required for all implementation. The majority of biometrics industry experts concur, with more than half (56%) admitting that there are too many instances where informed consent for biometrics use has not been obtained (Biometrics Institute 2019).

Trust and concern for ethical usage are recurring themes among all the survey participants. The Biometrics Institute (2019) survey found that 79 percent of industry professionals agreed that biometrics will increase security but 74 percent acknowledged that privacy concerns were holding back the market.

Signatures

Opinions expressed by the AIC interviewees were conflicting on whether or not signatures could be classified as biometrics. Many were concerned at the easy forgeability of signatures, with some feeling a digital/scanned signature would be more secure:

> I do not believe that a signature on paper is a biometric ID. Frankly, it might be far too easy for an unauthorised person to find my signature and paste it into a document that isn't mine. Fingerprints, eye scans, facial recognition and other body parts are (for the most part) far more secure.

Signatures were the second most popular biometric security method, overall, reported by AIC survey participants, with 81 percent of respondents stating a willingness to use the technology, increasing to 85 percent of recent identity crime victims (Franks & Smith 2020).

Fingerprint recognition

Most AIC interviewees were familiar and comfortable with fingerprint scanning technologies:

> On my phone I can store fingerprint profiles; when adding a profile, it will ask me to place my chosen finger on the scanner in various positions until it has scanned a sufficient amount of my fingerprint. When I want to unlock my phone, I just place my saved finger onto the fingerprint scanner and it will unlock it.

Fingerprint recognition was the most popular biometric security measure with the AIC 2019 survey cohort, with a strong 83 percent majority of users willing to use the technology in the future (88% of recent victims; Franks & Smith 2020).

Voice recognition

Voice recognition was not as popular or deemed as reliable as fingerprinting by most of the interview cohort; however, the benefits of the technology were still recognised:

> For a government department having voice recognition saves both them and us a lot of time.

The willingness of the AIC 2019 survey cohort to use voice recognition technology has declined by 2.2 percentage points since 2018, making it the fourth most popular biometric technology (70%). Recent victims of identity crime as recorded by the AIC survey were much more willing than non-victims to consider voice recognition technology (80%) and most other biometric options (Franks & Smith 2020).

Facial recognition

The AIC interviewees were generally unwilling to use facial recognition technology to prevent misuse of their personal information, giving the following reasons:

- concern that the individual may have their access denied if the technology does not recognise the user's facial imprint;
- uncertainty about the reliability of the technology—for example, the robustness of identification if people's facial appearance changes (facial injury, stroke, plastic surgery etc);
- concern over how the data are stored and subsequently used;
- general malaise about biometric identification, preferring to maintain individual privacy as much as possible and against what they see as increasing control and invasion by government into an individual's privacy;
- lower level of trust in the system's integrity when there is no active involvement from the individual (eg entering a password); and
- concern over identity theft if others are able to force a person to access their accounts (eg at an ATM).

One of the interviewees shared their concerns about data breaches:

> One – I am not 100 percent confident that the face recognition technology can perfectly identify me, and not mistake me as someone else (or the opposite, identify me instead of someone else). This is not likely, but can happen. Second reason – I don't trust that the information is secured. I mean, I know that there would be great attempt to secure private information, but there are always leakages – technical, human error, or people who intentionally try to steal information.

Although there were some concerns expressed about using facial recognition technology to identify criminals and terrorists, those interviewed were more willing to use biometrics to ensure individual and community safety. Many believed that criminals would already have profiles listed in law enforcement databases but also expressed their distrust in the accuracy when considering that individuals could change their appearance to avoid recognition:

> The main concern that I have is the effectiveness of the system. Personally, I have nothing to hide, but a criminal who knew of the existence of the system would surely try to dupe it? Anything is available for the right price, so I assume that criminals etc would happily undertake facial surgery to change their appearances. It is nothing nowadays to get facial implants or have nip and tucks done to alter the [sic] appearance.

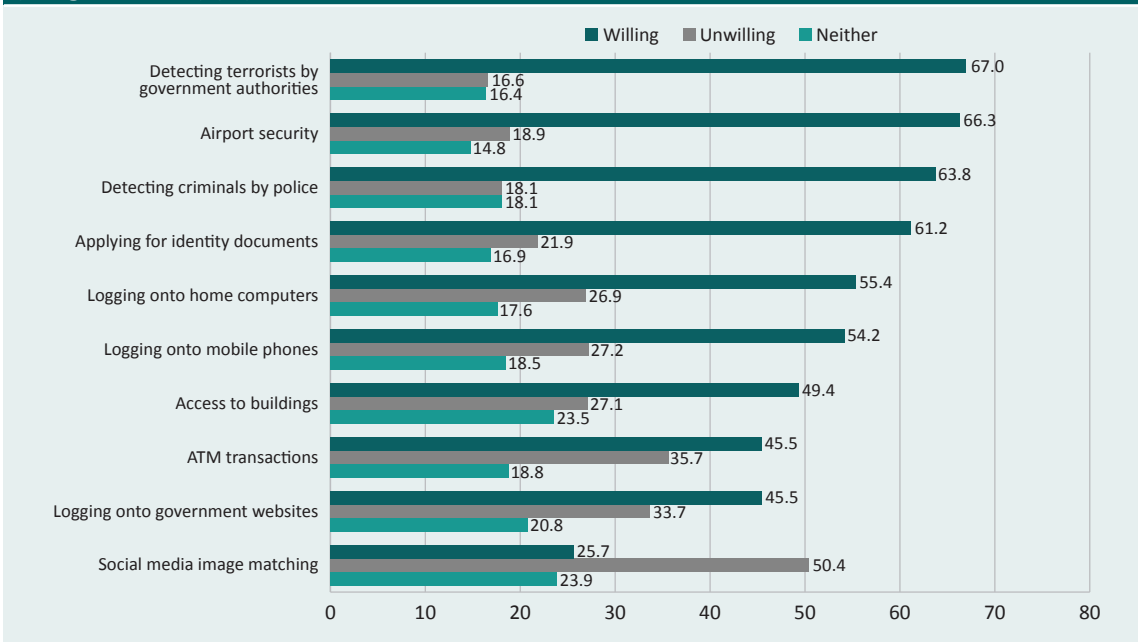
The AIC interviewees expressed similar sentiments about the use of facial recognition at border control as long as the focus was to identify known criminals or terrorists and not to log their personal identification information. Again, interviewees expressed concerns about privacy and the ability of a person to change their appearance to avoid detection:

> What if a person had cosmetic surgery and again the software failed to pick out or wrongly picked someone? How many levels of security are needed, where does privacy start and end? I understand there needs to be ways to stop wrong elements but where is the end point?

Future willingness to use facial recognition technology by AIC 2019 survey respondents has declined slightly (–2%) since 2018. To explore perceptions of facial recognition, the AIC cohort were asked how willing they would be to use the technology in various scenarios via a five-point Likert scale with the following response options: (1) extremely willing, (2) willing, (3) neither willing nor unwilling, (4) not willing and (5) extremely unwilling.

As with most biometrics, users were most willing to employ facial recognition technologies for government purposes such as identifying terrorist suspects (67%) and maintaining airport security (66%). The least acceptable purpose for using facial recognition technologies was for matching images on social media (50%; Figure 4).

Figure 4: Acceptability of using facial recognition technologies for specific purposes (weighted data) (%)



Source: Franks & Smith 2020

The Ada Lovelace Institute (2019) survey found that its participants were also willing to use facial recognition technology when there was a clear public benefit. Use by police in criminal investigations (70%), smartphone security (54%) and airport passport security (50%) received the strongest support from the Ada Lovelace Institute (2019) survey cohort. All options for using facial recognition technology without clear public benefit received less than 10 percent of the supportive vote (supermarkets (7%), schools (6%) and candidate recruitment (4%; Ada Lovelace Institute 2019).

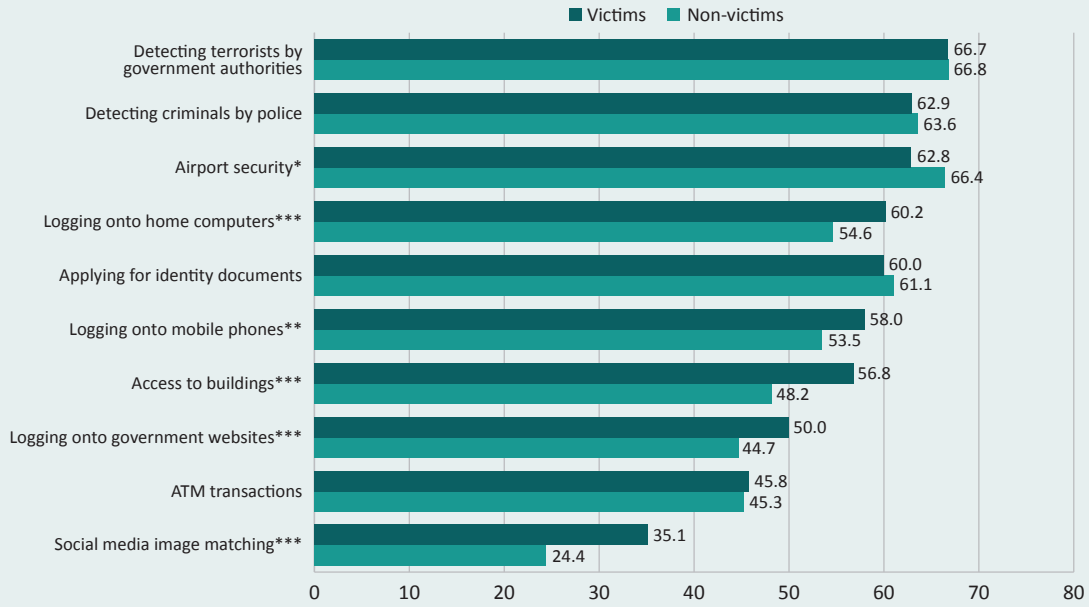
Victimisation and willingness to use facial recognition technology

Franks and Smith (2020) found that recent AIC survey victims of identity crime and misuse were significantly more willing than non-victims to use facial recognition for the following purposes:

- logging on to home computers (60% vs 55%; $\chi^2(1, 9{,}968)=13$, $p<0.001$);
- logging on to mobile phones (58% vs 54%; $\chi^2(1, 9{,}968)=8$, $p<0.05$);
- access to buildings (57% vs 48%; $\chi^2(1, 9{,}968)=30$, $p<0.001$);
- logging onto government websites (50% vs 45%; $\chi^2(1, 9{,}968)=11$, $p<0.001$); and
- social media image matching (35% vs 24%; $\chi^2(1, 9{,}968)=61$, $p<0.001$).

Surprisingly, recent victims of identity crime were less willing than non-victims to use facial recognition technology for airport security (63% vs 66% respectively; $p<0.05$). However, there was little difference between recent victims and non-victims in the perceived acceptability of using facial recognition for government purposes such as protecting Australians by detecting criminals/terrorists and applying for and using evidence-of-identity documents (Figure 5).

Figure 5: Perceived willingness to use facial recognition for specific purposes among recent victims and non-victims of personal information misuse (weighted data) (%)



***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$
Source: Franks & Smith 2020

Government databases with facial recognition

When questioned about their willingness to use facial recognition to enrol in government services, responses from AIC interviewees ranged from completely supportive of the use of the technology to completely opposed to the idea. Many people expressed concerns over data storage, security, privacy and the limitations for those with less access to technology:

> I definitely do not like the idea of having to use facial recognition for accessing government services. I feel that once a department has my data then every department will have it whether I want them (agree to it) to or not. This makes me feel very uncomfortable and that I have no degree of privacy at all anymore.

Half of the AIC 2019 survey participants who had previously experienced identity crime stated that they would be willing to use facial recognition technology to log onto government websites (50% victims vs 45% non-victims; Franks & Smith 2020). The Ada Lovelace Institute (2019) survey did not directly assess the public response to the use of facial recognition technology for logging onto government services. The Biometrics Institute (2019) survey also did not directly assess this question; however, just over a third (34%) of industry professionals agreed that significant developments were made in the deployment of government-issued identification, with further developments made in government/public transactions (15%).

Facial recognition and crowd surveillance

Public safety is an underlining reason the AIC interviewees gave for their acceptance of facial recognition to identify people recorded in law enforcement databases in a crowd. However, accuracy and misuse by authorities as well as privacy remain issues of concern:

> If the technology and hardware is already in place to do this, there is nothing stopping other people being added to the database without the public's knowledge. Call me sceptical, but I think once the hardware is set up and is available to use 'for identifying people in a crowd who are already recorded on official police and border control databases' it can now be misused. It also means anyone that has committed even a petty crime as a teenager, even if it was dismissed, would be in there.

When the scope of the question was expanded to include identification of the general public in a crowd, willingness declined and the interviewees felt this was far less acceptable. The issue of privacy was emphasised as well as reliability and data storage. However, some felt that if people with prior criminal convictions were monitored, it was only fair that the general public data be included in the database as well to ensure fairness:

> I still have grave concerns about accuracy, who has access to that data, where and how it is stored and what happens if compromised. I believe the potential to identify criminals and terrorists is great, but so much more thought, development and regulation has to be put in place to safeguard this highly personalised data. Perhaps it could be used to scan crowds for those criminals held in police and border control databases, but then be instantly destroyed for safety against privacy and fraudulent compromisation [sic].

The most popular use of facial recognition technology, as surveyed by the AIC 2019 cohort, was for 'detecting terrorists by government authorities' (67%), closely followed by 'detecting criminals by police' (63%; Franks & Smith 2020). This is consistent with findings in previous AIC and other surveys that, in general, individuals are much more comfortable knowing that biometrics are employed for national and community security.

Police trials of facial recognition in public spaces in London and Wales have created increased public debate about the ethical use of the technology by law enforcement. Respondents to the Ada Lovelace Institute (2019) survey, however, were in support of using facial recognition for a 'demonstrable public benefit' as long as there are appropriate safeguards in place.

Improvements in facial recognition systems

When asked about potential improvements that the government and biometrics industry could employ to make people more willing to use the technology, AIC interviewees wanted to feel more confident in the reliability of the matching process as well as understand more about the security around the use and storage of data and access to it:

> My concerns about facial recognition at present is [about] mistaken identity. The government needs to communicate to the general public, how it works, how does every person in Australia get facial recognition done, why we should trust it, what studies have been conducted with it, what issues are being identified with it. My concerns would be less if the general public were more educated and we could ask the experts any concerns we have; they also need to address how such a system will be implemented.

The Biometrics Institute (2019) survey asked industry suppliers and users which biometric method they believed was increasing in popularity, with a majority (55%) citing the face biometric as their primary selection, up eight percentage points over the 2018 survey (47%) and 17 percentage points over the 2017 results (38%).

Penalties for misusing facial recognition systems

Large numbers of identity crimes are reported annually and yet only a small proportion of incidents result in police investigation and prosecution. AIC interviewees were generally unaware of the penalties associated with the misuse of facial recognition technology but felt that they should be on the same level as those for identity theft and fraud and not exclude imprisonment if warranted:

> I don't know what courts currently impose and have not heard of any cases being successfully prosecuted. It would seem to me that any criminal activity such as using this technology to steal from someone by fraudulent activity should be penalised in the same way as any fraud. The same would apply to any other criminal activity. I oppose creating new laws where existing ones can be used or modified to cover new versions of the same crime.

The other surveys consulted did not address this topic.

Iris recognition

When asked about the potential dangers of using biometric technologies, the AIC interviewees only related potential danger to iris scans. Those who were skeptical admitted not knowing enough about the technology to have an informed opinion. It is imperative that information about biometric systems is more widely distributed:

> Eyes possibly…depending on how bright the identification system is. I don't know this…it's an assumption. Not sure whether you can be harmed via fingerprint or voice, iris appears more viable.

Franks and Smith (2020) found that the willingness of AIC survey participants to use iris scans declined slightly (–2%) between 2018 (69%) and 2019 (67%). Recent victims of identity crime were significantly more willing to use the technology (76%) than non-victims (66%; N–1 $\chi^2(1)=45.76$, $p<0.001$).

DNA

When asked about the use of DNA matching, the AIC interviewees only expressed concern over potential fraudulent transfer of DNA as they have seen depicted on television and in the movies:

> In criminal circumstances I think it can be misused – especially with DNA, it can be transferred without your knowledge onto something or somewhere to incriminate people.

The AIC surveys do not currently assess respondents' willingness to use DNA technology as this is not a biometric designed for individual use and is predominantly for law enforcement or parent verification purposes only.

Human microchip implantation

There was a general understanding among the interviewees that human microchip implantation may be an inevitable part of the future, with most willing to partake in this technology for government purposes only, as long as privacy, data security, and health and safety were guaranteed:

> With the security and crime issues the world is experiencing, I'd be happy to have a chip implanted, it would make it easy to prove my identity for financial, travel and medical services, but I would have to be assured that my identity was protected from fraud.

However, as with overall biometrics usage, interviewees preferred government-issued over private sector–issued technology based on the belief that businesses may not possess adequate ethics policies, have verifiable credentials or maintain security robust enough to ensure safe access and storage of their data:

> I think in principle, I would be willing to have a computer chip implanted for identification purposes with governments, as long as I can choose the details/level of details the computer chip provides. I am a little more hesitant to allow it for businesses, as it could be argued there is a lower level of security, and the 'computer chip' could be manipulated and your data/information may be on-sold.

When asked about their willingness to use a human-implanted microchip, nearly a quarter (23%) of AIC survey respondents stated they would try the technology, a slight increase over 2018 (22%; Franks & Smith 2020; Jorna, Smith & Norman 2020). Interestingly, Franks and Smith (2020) described how recent victims of identity crime were more than twice as willing as non-victims to have a microchip implant to secure their information (42% vs 20% respectively). The willingness of recent victims to consider human microchip technology experienced a four percentage point increase over AIC 2018 survey results (38%; Jorna, Smith & Norman 2020). Increasing interest in what some consider extreme methods of personal security is one of the motivations for this research.

Microchip implantation and removal

When enquiring further about the willingness of the AIC interviewees to have a microchip implanted under their skin, several issues were considered. Medical professionals were expected to be used for the implantation procedure, with an IT professional present to test the implant performance:

> I would only trust a doctor that has significant information about the technology to implant it and I would want someone, such as an IT person that has an expertise in the technology, to be there to oversee the procedure.

Additional information was deemed necessary before the majority of the interview participants would seriously consider a human microchip implant, namely:

- how the chip works/maintenance/replacement;
- health implications; and
- privacy.

> I should be informed of absolutely every single bit of detail about it beforehand.

Previous usage of the device was also important. Some interviewees stated they would require evidence of research and human trials prior to adopting the technology:

> I think that you should be given a large amount of information. It's a foreign object in your body, so warning signs of malfunction, infection, rejection etc. Also, any potential known dangers of having it in your body. How to care for and maintain the chip. The expected lifespan, if any, and the procedures to have it removed or replaced. Cost. The functions that it is capable of performing. Check-ups – when, where, how often?

Age of consent and advantages over other technology options were also considerations as well as cost, maintenance and removal. General consensus was that chip implantation should be reserved for adults only (over 18); however, some viewed parental consent was sufficient for younger members of the population. Multiple interviewees suggested implantation at birth but only if the technology and government regulations were in place:

> It would first come down to whether government was prepared to make it legal and necessary by putting new policies in place. Then I would be putting implants in at birth. However, initially till this occurs, we should at the very least be implanting serious criminal offenders so law enforcement agencies can keep abreast of their movements.

Some advantages of chip implants were described as follows:

- convenience of not having to remember/update passwords;
- reduces hacking and identity theft;
- faster and easier than providing 100 points of 'paper' identification;
- easier than biometrics enrolling and matching process; and
- if extended to driver licence and bank card information a wallet is no longer needed.

> Technology is moving at a pace that will see this becoming the norm in the future anyway. So, to reject it now to me is only delaying the inevitable. Also remembering passwords for everything now is impossible and time is wasted contacting companies to reset passwords which will eventually be forgotten as well. We write them down but then lose the paper we wrote them on. As for biometrics, I have always wondered what would happen in the case of injury and disfiguration and or damage to fingertips, facial features and blindness. Does this then prevent you being recognised by biometrics? I don't know the answer but certainly believe that implants seem to be an easier and more effective way to go.

The costs of technology are always a factor. Most of the interviewees believed that human microchips should be a government-implemented program and therefore subsidised by the government. If the implants were required by private industry employers, logic states that it would be the expense of the company offering this technology to their employees:

> I think the government should subsidise the payment of chip implantation, via Medicare or another funding model – I think that the individual should pay a proportion of getting the chip implantation. It could also be rolled into the 'passport' process, or actually replace the application fee for obtaining a passport, for example. I think the government should subsidise because it is an important initiative and makes better sense from a security point of view (from the government's perspective).

The costs associated with chip removal and maintenance are again believed to fall on the person or entity who instigates the action. If removal is required for health reasons or upgrade/maintenance, the expense is expected to be covered by the original payment source whether that be government, private industry or the individual:

> Ideally, it would be fantastic for this to be covered by the government or organisation that initially is using the information but with most if not all procedures done medically, the individual usually signs a contract/waiver taking ownership and responsibility of any risks/dangers and thus, taking ownership of any costs afterward involving any adverse health risks or other effects. So I don't have much confidence that the people who should be liable are in the end.

Overall, there was surprising support for human chip implant technology from the AIC interview cohort:

> It is a great way to confirm the identity of each person, especially when it comes to situations around deaths, missing persons, crime and fraud.

Multi-modal systems

The European Union was due to adopt a multi-modal immigration policy from 2020, a combination of four fingerprints plus facial recognition that non-residents will need to submit/verify before gaining entry to a member country (Anderson 2020). It is unclear at this time how the COVID-19 pandemic has affected this policy. Digital identity solution organisations, such as UK-based Yoti (2020), are offering multi-factor biometric authentication options to their digital identity application customers.

When presented with the concept of multi-modal biometric systems, the AIC interviewees could not describe an instance when they had been asked to provide more than one biometric verification. However, the majority agreed that they would welcome a biometric version of multi-factor authentication if it was user friendly and provided a greater level of security without compromises. Less willingness was expressed for multi-modal systems to be used for low-risk security requirements such as unlocking a mobile phone. As with all biometric technologies, users were concerned about privacy and data storage/management:

> For my own personal devices – no. I don't think I really need it. But if this was offered in terms of where I do my banking and important places who I have my information with such as the government or ATO I would be more than willing to use a multi-modal system as this type of information is not one I would love to be leaked/accessed or shared with anyone else. It's harder to do damage control than prevention in my view.

The Biometrics Industry (2019) survey participants listed multi-modal systems as their second largest area of development (61%), an increase of three percentage points over 2018 survey results (58%). The previous AIC surveys did not address the use of multi-modal biometric systems; however, this topic will be included in future surveys.

Preferred biometrics

When asked about their preferences for different biometrics, AIC interviewees were more inclined to use fingerprint matching than other biometrics. The perceived reliability of both facial recognition and voice recognition was a deterrent of use:

> I prefer using a fingerprint for devices that I own. I also prefer using fingerprints for entry/exit from the country (instead of facial where I must remove my glasses). I would be happy to use fingerprints for access to my bank.

User preferences were, of course, based on user experiences. Some common issues reported by interview participants included:

- fingerprints—can be difficult to match when they are wet or dirty, or there may be a general failure to recognise this biometric method, causing people to revert to passwords/PINs;
- facial—can be difficult to match in low light situations or when wearing glasses; and
- voice—can require a few attempts to match successfully and be impacted by background noise.

> With fingerprint I've had problems with recognition at times when my fingers are moist. With facial, I've had problems when wearing sunglasses or I'm unshaven, with voice, there are problems when there is cough.

When examining the results of the Biometrics Institute (2019) survey, industry leaders demonstrated only 40 percent confidence in any future developments of the public-preferred technology, fingerprint, consistent with 2018 findings. Facial recognition technology topped the list in 2019 for development potential by biometrics industry leaders for the second year in a row, up seven percentage points from 2018, with future developments set to address criticisms mentioned by the AIC interview cohort such as lighting and face accessory issues (Biometrics Institute 2019).

Concerns about biometric technologies

The AIC interviewees generally had a broad understanding of the potential problems associated with biometric technologies including their reliability, accuracy of matching, security of information, storage issues and associated costs. One interviewee said:

> I can only imagine that current systems are not yet perfected and that there might be a degree of inaccuracies occurring which might make false identifications. It's also possible that current technologies have incomplete databases, so the biometrics only work for less than 100 percent of the customers wanting access to a system.

Others expressed concerns about being wrongly identified by biometric systems either through system failures or interference:

> The main concern that I have is the effectiveness of the system.

> I still have difficulty believing that security software could not be tricked in some way.

One interviewee thought that criminal misuse of facial recognition systems was inevitable:

> My concerns about using facial recognition at airports is the collection of personal data. I do not believe the authorities are in the position to guarantee the safety of such data. If criminal elements accessed such data, they would be able to identify individuals visually. This could lead to targeted crime.

As with all technology, assumptions were made about the likelihood of systems improving over time as well as the possibility of increased criminal interference:

> I don't think they are getting worse or better at the moment but as people learn to use them more, they could become worse as other people can hack and then use them for other things than what they are collected for. They could also become better as more safety measures are put in place.

There was little knowledge about how the government and biometrics industry are acting to improve systems and how much they cost. Consumers interviewed were more knowledgeable about computer and mobile technology and felt that improvements were inevitable:

> Technologically, some of this has been ground-breaking. There would be huge dollars in this. The higher-level security applications couldn't afford these systems to get it wrong. To me this means these systems will be trialled and trialled for repeatability and reliability and therefore will be very expensive systems to buy, install and support. Getting it wrong would not be an option so I think the tech companies involved would be throwing everything at it.

The AIC 2018 questionnaire also asked respondents about their concerns with specific uses of biometric technologies. Table 3 presents these results.

Table 3: Concerns about the use of biometric technologies (weighted data) (%)

Concerns	Extremely concerned	Somewhat concerned	Not very concerned	Not at all concerned
Protection of my privacy using biometrics	48.8	34.2	13.0	4.1
Costs associated with biometrics	33.4	42.2	19.3	5.2
Risks of losing my biometric data	41.7	37.4	16.3	4.6
Risks of losing my money	43.1	35.5	16.8	4.5
Inconvenience of having to enrol in biometric systems prior to using them for the first time	21.5	40.0	30.8	7.7
Fixing problems if biometric systems fail	41.3	41.5	13.4	3.8
Physical injury to myself through using biometrics	24.9	28.9	32.4	13.9
What to do if my biometric data are compromised	50.7	35.7	10.3	3.3
Someone using my biometric data to pretend to be me	49.2	32.1	14.2	4.4
Police taking action against me by mistake through biometric matching	40.5	35.6	19.3	5.7
Forcing me to use biometrics without my free consent	47.0	34.3	14.2	4.5
Having to use multiple different biometric systems for different purposes	31.1	44.2	19.8	4.9
Government surveillance of me	38.2	33.2	21.5	7.1

Source: Jorna, Smith & Norman 2020

Individuals who responded to the Ada Lovelace Institute (2019) survey on facial recognition technologies in the United Kingdom were mostly concerned about the possibility of infringement of privacy and the need for law enforcement to use biometrics ethically. These concerns are reflected in other research. Rhue (2018), for example, describes how companies are developing facial recognition software to scan faces in crowds to determine whether any of the individuals pose a public safety threat because of their apparent emotional states. Rhue (2018) argues that if an AI system mistakenly identifies an individual as a threat, then that person could be detained, followed, placed on a no-fly list or some other life-altering consequence as a result of potential bias or inaccuracy in the systems. AI Now (2019) warns of bias in facial recognition systems causing continuing race and gender disparities via techniques such as affect recognition, which claims to 'read' emotions by interpreting physiological data such as micro facial expressions, tone of voice or gait. Crampton (2019) agrees that surveillance is no longer simply observation of identity but a process of assigning identity: you are not seen but rather are seen as whatever the system determines you to be (terrorist, threat, of colour, etc; Crampton 2019).

Findings: Privacy, ethics and data sharing

The Australian Government's National Identity Security Strategy (Department of Home Affairs 2020b) states that the government's use of biometric data is prescribed by law and consistent with obligations under the *Privacy Act 1988* (Cth), Australian Privacy Principles and the *Archives Act 1983* (Cth). The National Biometric Interoperability Framework describes how 'government agencies in Australia should expressly recognise and consider the role of privacy when engaging in the collection, use, disclosure, management and disposal of biometric data' (Department of Home Affairs 2020b).

The framework (Department of Home Affairs 2020b) also states that the use of biometric technologies should be appropriate and cost effective while considering any impact on the privacy of consumers as well as any security risks involved in collecting and holding personal identity information. Collection is guided by legislation and the Australian Privacy Principles, which require that consumers are notified of that collection. When technology and systems are used in ways beyond their original purpose, particularly when the new purpose results in invasion of privacy, function creep occurs. One AIC interviewee agreed, commenting:

> "I don't think anything in this computer age is 100 percent safe. I am sure that this data can be misused by people accessing or working with the data, [or by] the government using it for many things other than what it was collected for. Hackers can still get into computers.

Nearly three-quarters (74%) of Biometrics Institute (2019) survey participants agreed that privacy concerns are the leading market constraint for biometrics implementation. When asked about their perception of privacy, ethics and controls within the biometrics industry, both suppliers and users agreed in a 66 percent majority that 'privacy/data protection concerns' is the greatest market restraint for the biometrics industry, up 10 percent from 2018 (60%; Biometrics Institute 2019).

Facial recognition technology, and its use in public spaces for policing purposes, has raised many privacy concerns and ethical issues. Questions of accuracy, potential bias and ambiguity about the nature of deployments are areas in need of further exploration (Biometrics and Forensics Ethics Group 2019).

The Biometrics Institute (2019) cohort ranked 'data sharing concerns' as their second key market restraint (43%) behind 'privacy/data protection concerns'. The Australian Government's National Identity Security Strategy (Department of Home Affairs 2020b) proposes a collaboration between government and industry to develop a best practice for sharing biometric data that meets international standards. A majority of industry suppliers and users responding in the Biometrics Institute (2019) survey agreed that interoperability of border management systems requires revision of trust frameworks (79%), although 71 percent expressed the view that a single, global approach is unlikely.

Accountability, legislation and user consent

In a globalised digital economy, personal information is constantly generated by individuals through their use of digital technologies and their movements around physical environments. Highly publicised events and concerns reported by government whistleblowers have drawn attention to the use of people's personal data by other actors and agencies, both legally and illicitly (Lupton & Michael 2017). The AI Now Institute, an interdisciplinary research facility at New York University focusing on the social implications of AI technologies, argues that the emergence of globally-oriented data protection approaches, such as the European Union's General Data Protection Regulation, motivates policymakers to design ethical frameworks to answer the call for legislative accountability.

The AIC interviewees felt there was a need for more openness and transparency from both the government and the biometrics industry. The general sentiment of those interviewed was that enhanced communication of information was necessary to increase public willingness to use these technologies:

> My concerns about facial recognition at present is [about] mistaken identity. The government needs to communicate to the general public, how it works, how does every person in Australia get facial recognition done, why we should trust it, what studies have been conducted with it, what issues are being identified with it.

> Government could be required to advise you if it had captured and stored your image and linked it to your identity, how long it would be retaining it for, to what purpose it was putting it, and to destroy it if requested by you.

> The biometric industry needs to communicate what experiments they have done to improve facial recognition, analyse their results, identify problems that arise and release publications and provide documentaries on the topic to the general population.

Instances of biometrics use without informed consent are common, with over a third (39%) of the Biometrics Institute (2019) survey respondents agreeing that stricter regulations would not limit innovation and investment. Another third (33%) of these respondents felt the opposite, stating that stricter regulation would definitely decrease innovation and investment while the remaining 27 percent were unsure (Biometrics Institute 2019). The Ada Lovelace Institute (2019) survey respondents described how recent high-profile deployments of facial recognition technology have highlighted gaps in regulation for commercial use of biometrics and reiterated the need for policy upgrades to ensure trustworthy governance.

The Biometrics Institute (2019) also asked its industry survey respondents whether they believed that the current legislation covering the use of biometrics was strict enough. Nearly half (44%) stated 'no, not strict enough', with another 32 percent undecided. Less than a quarter (24%) believed current biometrics legislation is sufficient, although only 17 percent of those in the Australia and New Zealand region shared this view (Biometrics Institute 2019).

Numerous regulatory attempts have emerged to address the privacy, discrimination and surveillance concerns associated with biometrics motivated by the European Union's General Data Protection Regulation. In Australia the Parliamentary Joint Committee on Intelligence and Security's inquiry into the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019 ordered a temporary pause on the use of a national facial recognition database while legislation is developed to ensure proper and ethical management guaranteeing citizens' rights (Martin 2019). The Parliamentary Joint Committee on Intelligence and Security (2019) recommended that:

- the regime should be built around privacy and transparency, and subject to robust safeguards;
- the regime should be subject to parliamentary oversight and reasonable, proportionate and transparent functionality;
- the regime should be one that requires annual reporting on the use of the identity-matching services;
- the primary legislation should specifically require that there is a Participation Agreement that sets out the obligations of all parties participating in the identity-matching services in detail; and
- the Australian Passports Amendment (Identity-matching Services) Bill 2019 be amended to ensure that automated decision-making can only be used for decisions that produce favourable or neutral outcomes for the subject, and that such decisions would not negatively affect a person's legal rights or obligations, and would not generate a reason to seek review.

Freedom of choice

In relation to the need for freedom of choice about the use of biometrics, the AIC interviewees were generally comfortable with current uses of biometrics, based on their own understanding and non-invasive experiences of the technologies. Interviewees believed that people in Australia enjoy freedom of choice concerning biometrics used in connection with their personal devices and also in workplace settings, with employers usually having an opt in/opt out policy on the use of biometrics. Enforced use of biometrics for border security and in situations where the collective security of the nation is at risk was thought to be acceptable:

> I believe that biometric systems are optional at this stage. I can't think of any departments or organisations who give no options for using a biometric system. For example, at border security, there are pathways that do not use biometric security, to pass through border security. Similarly, on mobile phones, you have the option to use a 'password' or 'PIN' security settings. If biometrics was mandatory and the only option, I would want strict privacy and control on the data use, and most likely, only government departments being able to control this.

Many interviewees had conflicted views about the balance between public safety and freedom of choice in relation to biometrics, with sentiments such as the following being expressed:

> I believe we do not have free choice and that we have been forced to use biometric services. An example of this is Australian border and passport control. For the greater 'good' of our society I don't have an issue with this. I am opposed to supermarkets using biometric scanning for pure profit, market and sales purposes.

> I do not believe that biological biometric data should be captured without the individual's knowledge. However, for societal safety and security reasons we should capture biometric data without people's knowledge if it assists in law and order.

Although a certain level of acceptance was found for the compulsory use of biometrics in the interests of public safety, the capture and storage of biometric information without the individual's consent was not considered to be acceptable by all interviewees:

> It's the breach of privacy if without my knowledge something is stored. There has to be an option of choose or not to choose whether personally I want something to be stored. I don't want to compromise my security and privacy to anyone regardless of the reason.

> I feel it is very impersonal, intrusive and open to abuse by the authorities.

The Biometrics Institute (2019) survey found that 56 percent of participants felt that there were repeated instances in which informed consent for the use of biometrics had not been obtained, an increase of 10 percentage points over the 2018 survey results (46%). Nearly half of the Ada Lovelace Institute (2019) survey respondents (46%) believed the public should be able to either provide their consent for the use of facial recognition technology or be excluded by choice. Consent and/or exclusion were more strongly supported by ethnic minority respondents who experience less accuracy in facial recognition matching than other individuals (Ada Lovelace Institute 2019). For some, further implementation of biometric systems threatens invasion of privacy, particularly the use of cameras in public spaces.

Perceptions regarding surveillance

AI Now (2019) reports that there has been an increase in instances in which privately-owned technological infrastructures have been integrated with public systems that expand surveillance capabilities with limited transparency, accountability and oversight. Partnerships between governments and private technology companies have emerged that extend surveillance from public environments into private spaces such as private properties and residences (AI Now 2019). An example of these partnerships is the CAPTURE (Community Assisted Policing Through the Use of Recorded Evidence) program in Alberta, Canada, which was designed to share information from private security cameras installed at commercial businesses and personal residences with local police under the guise of improved community safety (AI Now 2019). Similar projects are being developed in other countries.

Overall, the AIC interviewees supported government and law enforcement use of biometric surveillance for the protection of the nation and individual communities, but when prompted began thinking more about their individual rights to privacy and ethical usage:

> I think it is important to keep us and our country safe, making these ways appropriate, but it can also be an invasion of privacy. You can't do anything without being spied on, like with cameras photographing you entering shopping centres etc… It is unfair for all the honest good people in the country but it is good for the criminals and terrorists who make it bad for the rest.

Similar results were found in the Ada Lovelace Institute (2019) survey, with participants expressing fear of the normalisation of surveillance. They were, however, more flexible in their acceptance of facial recognition when there was a clear public benefit. There is a saturation of CCTV cameras in the United Kingdom, with approximately one camera installed for every 14 people (Hall 2017), and as a result the Ada Lovelace Institute (2019) respondents are very familiar with public surveillance. The majority, however, believed that facial recognition should only be permitted for criminal investigations (70%) and in airports (50%).

Unconditional versus conditional support

There was consistent support for law enforcement and government use of biometric technologies among the AIC interviewees, but, as mentioned above, the support was principally in connection with maintaining public safety. Most interviewees expressed concern over privacy and unethical uses of biometrics. Support was rarely unconditional:

> Facial recognition is being used in large crowded areas to enable law enforcement officers to identify individuals and to quickly screen them using other security systems (ie terror watch-lists) to see if they are a security threat.

> Especially with terrorism having such a terrible impact on our lives, having airports and so on with safety precautions like this could deter future events from happening.

Overall, Australian survey respondents and interviewees were more willing to trust systems provided by government agencies than private sector organisations:

> I have more trust in government agencies. I believe the government is legally and morally responsible to ensure the safe and secure storage and access to my biometric information. I don't have the same level of trust in privately operated businesses.

The Ada Lovelace Institute (2019) respondents had high expectations that government regulations and a demonstrable impact on crime would provide adequate justification for the use of facial recognition systems. Nearly a third (29%) of those surveyed, however, were uncomfortable with police use, citing infringement of privacy (68%), lack of consent (62%) and concerns over ethical use (60%) as their reasons (Ada Lovelace Institute 2019). The Ada Lovelace Institute (2019) concluded that further, in-depth research is needed to understand these concerns more fully, specifically in relation to minority groups who have reported increased levels of discomfort with biometrics.

Private sector use and public trust

Regarding the use of biometrics by private sector organisations, the AIC interviewees felt that private sector use of biometrics was somewhat problematic:

> I don't object to it being used to identify criminals or terrorists but unfortunately once we go down the path of facial recognition, the ability to control it, [as with] other forms of identification, will be difficult. Tracking people for the purpose of shopping habits, checking up on where they go and what they do will no longer be private. As much as we believe it will only be used for good, once the database is set up and the technology is out there, it can also be accessed for the wrong reasons by the wrong people.

Some AIC interviewees, however, believed that private sector providers would be motivated to take steps to protect the security of personal information because of the economic and reputational interests at stake, arguably more so than the government sector:

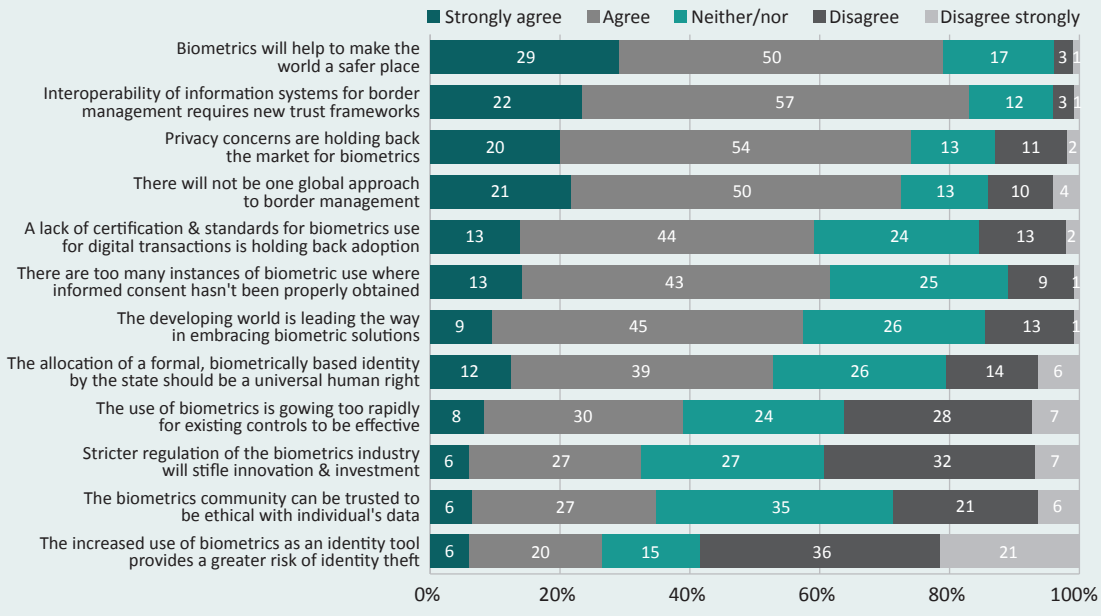
> Sometimes I think that the private sector will do a more reliable job of securing personal information, especially if their brand is critical to their business running.

AIC survey respondents were far less willing to accept the use of biometric technologies for private sector applications, particularly online, than for government uses. For example, half of the cohort specifically stated they would be unwilling to use biometrics for social media (Franks & Smith 2020). Public attitudes to private sector use of facial recognition technology in the United Kingdom were generally unfavourable, with 70 percent of Ada Lovelace Institute (2019) survey respondents lacking confidence that companies would use the technology ethically. It was perceived that if the technology were being used for commercial benefit, then the motivation for misuse would likely be high. The Ada Lovelace Institute (2019) concluded that further dialogue is needed between the public and private sectors to increase awareness and to help reduce the lack of trust in policymakers expressed by individuals in the community.

International standards and certification

Participants in the Biometrics Institute (2019) survey were asked to indicate the extent to which they agreed or disagreed with a number of views that had been expressed at various Biometrics Institute meetings over the preceding years. More than three-quarters believed that biometrics would help to make the world a safer place, with most of the remainder holding neutral views and only four percent disagreeing with this statement. Fifty-seven percent of the Biometrics Institute (2019) survey respondents indicated that the absence of standards and certification in the biometrics industry was holding back adoption of these various technologies. Some of the cohort (38%), particularly those from Australia and New Zealand, felt that the use of biometrics was growing too rapidly for existing controls to be effective (Biometrics Institute 2019; Figure 6).

Figure 6: Biometrics industry attitudes (%)



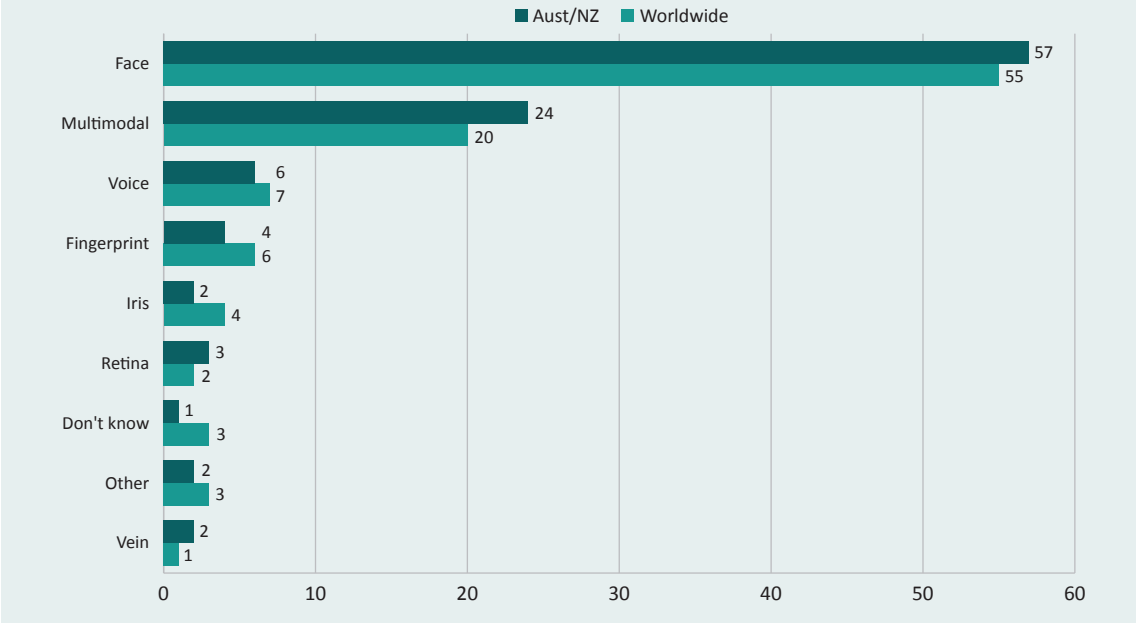
Source: Biometrics Institute Survey 2019

The majority (51%) of Biometrics Institute (2019) participants believed that the allocation of a state-supported, biometrically-based identity solution should be a universal human right and 54 percent felt that the developing world is leading the way in embracing biometric solutions. Government-supported national biometric identity systems that generate an individual identifier for each person as a link to government resources are growing in popularity and are encouraged in the developing world in support of 'ID4D' and fulfilling the UN Sustainable Development Goals (AI Now 2019). Residents in many countries are now required to use digital methods to access a range of services, as with the aforementioned Aadhaar program in India. Demographic information and biometrics (fingerprints, iris scans or facial scans) are being used for enrolment into an identification database or as a continuing means of authentication and are often marketed as a benefit to the individual while sometimes appearing to more directly benefit state and private interests (AI Now 2019).

The future of biometric technologies

The Biometric Institute (2019) survey participants predicted that the largest growth area of the technology will be in the facial recognition market (55%)—this relies heavily on AI technology for facial analysis. Figure 7 shows respondents' views regarding the Australia/New Zealand and worldwide markets for each modality.

Figure 7: Biometric most likely to increase in use over the next few years (%)



Source: Biometrics Institute Survey 2019

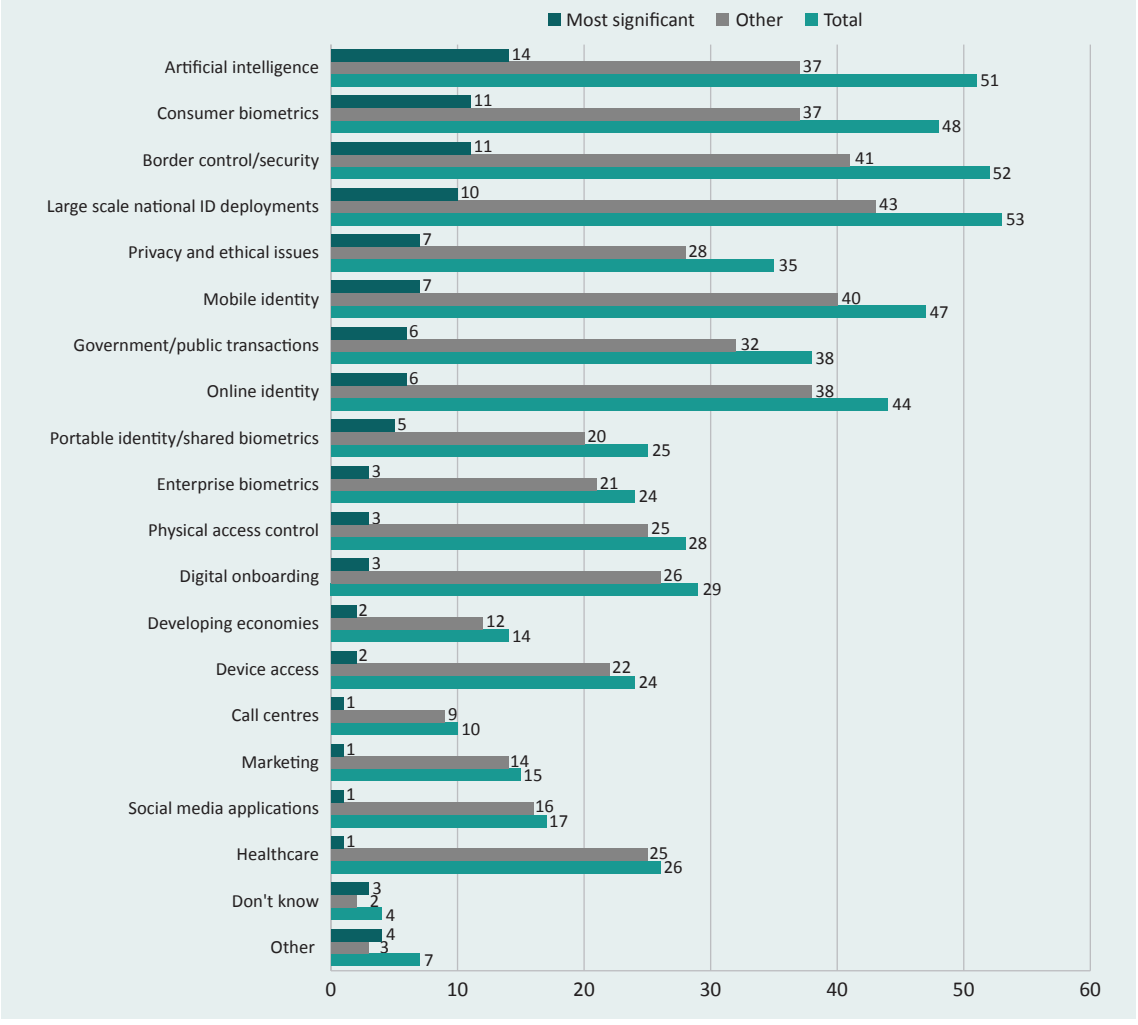
When first and second rankings were combined, facial recognition technology achieved support from 97 percent of respondents in 2019, an increase of seven percentage points over the 90 percent recorded in 2018 (Biometrics Institute 2019). AI Now (2019) warned, however, that rapid expansion of facial recognition technology without adequate regulations in place would cause unnecessary risks and recommended expanding biometric privacy laws in both the public and private sectors.

Future developments in biometrics

In 2016 the European Union invested €4.5m in a research program to strengthen border control technologies. The preferred consultant, iBorderCtrl, proposed the use of AI-driven avatars to conduct interviews with travellers while assessing facial biometrics for truthful answers (Crampton 2019). Trials of iBorderCtrl's automated deception detection system began in 2018 and was based on an earlier system called 'Silent Talker' to uncover 'biomarkers of deceit' that reveal a person's true feelings no matter how much they try to control their facial expressions (Crampton 2019). The iBorderCtrl project demonstrates 'platform biometrics' which employs affect recognition and expands on physical identification of individuals to detect and draw conclusions about formerly private attributes such as emotion, intent and social bias (Crampton 2019).

The Biometrics Institute (2019) industry survey ranks AI (14%) as its most significant area for increased use of biometric technology over the next five years (Figure 8).

Figure 8: Developments in the use of biometrics during the next five years (%)



Source: Biometrics Institute Survey 2019

Facial recognition technology works via AI machine learning, which teaches algorithms desired outputs of identifying and extracting patterns from datasets (Crampton 2019). AI Now (2019) warns of the dangers of AI systems that may be vulnerable to mass surveillance from faulty recognition, lack of scientific evidence and irresponsible ethics. It has encouraged developers and researchers to consider who their technologies benefit and/or harm when planning future projects.

Biometrics-as-a-service

Software-as-a-service (SaaS) is a delivery and licensing model under which software is centrally hosted by a service provider who then on-sells the software via a cloud-based subscription service (International Data Group 2018). The International Data Group offers global expertise on technology and industry trends and estimates that nine out of 10 companies will have at least part of their infrastructure 'in the cloud' by 2019, with the rest to follow by 2021 (International Data Group 2018).

With the increasing popularity of SaaS as a cost-effective way for organisations to limit overhead expenses while still maintaining the most up-to-date technology, biometrics-as-a-service (BaaS) has emerged as a viable approach. BaaS has recently been developed to capitalise on the well-established benefits of SaaS and offer a cost-effective solution to organisations without the resources to implement expensive in-house biometric systems.

Aware (2020) reports that BaaS allows a company to benefit from subscription services instead of larger, upfront capital expenditures. BaaS also offers businesses an affordable option for contracting multiple biometric modalities to fully implement multi-factor authentication that is future-proof (Greene 2020). There is also less risk involved for the contracting organisation, with hardware, software, maintenance and security all managed by the BaaS provider as part of the subscription. The BaaS market is projected to be worth $2.9b by 2022 (Aware 2020).

In an extension of BaaS, AI firm AIH Technology has teamed up with Microsoft Partners Network to plan and launch facial-recognition-as-a-service (FRaaS) on the Microsoft Azure platform (Pascu 2020). The availability of FRaaS will expand the market and make private access to facial recognition technology far more accessible. This also increases the potential urgency of international legislation and policy reform to address bias concerns and ensure individual privacy rights are maintained.

Self-managed user profiles and government access

With the digital private sector turning to subscription service providers, the topic of government subscription services continues to be of relevance. If biometric profiles are self-managed by their owners, identification-issuing authorities such as passport and motor vehicle licensing agencies could move away from printed documents to more manageable and less costly digital alternatives. The process of verification would not change but instead of, for example, a physical passport that could easily be lost or compromised, a digital profile maintained by biometric security methods would be held in some sort of digital wallet by the owner. The issuing organisation could then charge a nominal verification and subscription fee, potentially saving millions on specialised printing products and anti-forging technology.

Australia's Digital Transformation Agency (DTA) announced its digital identity solution GovPass in 2017, promising online access to all government services without having to repeatedly provide 100 points of identification to each agency (DTA 2020). In late 2018 the DTA launched the first live pilot for GovPass and its adjoining program, myGovID mobile app, under the government's Trusted Digital Identity Framework, employing facial recognition technology via selfie to access Australian Taxation Office services as an alternative to AusKey (Bushell-Embling 2018). It was announced in 2019 that the myGov authentication system would also move to myGovID in 2020 (Burt 2019a) which was successfully implemented. GovPass is also gaining momentum, with the DTA appealing to the public through this expansion in the hopes that all government services will become available through digital channels by 2025 (Hendry 2020).

Australia Post has also recently had its digital identification series, Digital iD, approved as a 'trusted identity service provider' under the Trusted Digital Identity Framework as part of the GovPass framework, offering a 'fast, easy and secure digital identity solution' (Australia Post 2020; Burt 2019b).

Internationally, the Dutch National Office for Identity Data, in partnership with Delft University of Technology (TU Delft), began public testing of a digital passport application in late 2018 (Stokkink & Pouwelse 2018). TU Delft are blockchain research leaders and their resulting technology, Trustchain, is at the forefront of both government and private sector use worldwide. The Dutch digital passport prototype works from a distributed ledger technology mobile app that is only accessible to Dutch citizens after presenting themselves for a face-to-face identity verification. The Dutch solution is the world's first permissionless decentralised digitised passport and a true peer-to-peer identity exchange with potential for global adoption. It offers Dutch citizens the opportunity to become the owners of their own identities and not have these solely in the hands of a single (federated) authority (Stokkink & Pouwelse 2018).

Conclusion

In a rapidly changing, digitised world, the impact of identity crime and misuse continues to grow, with industry's response being to improve and develop more secure methods of authentication of identity. Previously deployed systems of simple username and password are becoming obsolete as criminals have become more skilled in compromising such systems. Biometric technologies are becoming the preferred authentication system, especially by those individuals who have experienced identity crime in the past.

This report has outlined the findings of qualitative research conducted by the AIC using a sample of respondents to the AIC identity crime and misuse survey of 2018. The responses of the AIC interviewees were compared with findings of the latest AIC identity crime survey for 2019 and surveys conducted by the Ada Lovelace Institute (2019) in the United Kingdom, and the Biometrics Institute (2019). The objective of the present report was to examine the extent of previous use of, and future willingness to use, various biometric technologies to protect personal information, and the associated market restrictions within the biometrics industry. Individual perceptions of risk associated with the use of biometric technologies, privacy concerns and ethically obtained user consent are critically important for effective policy development and were also examined.

Based on the findings of the AIC interviews and surveys, and the Ada Lovelace Institute research, it is apparent that there is a reasonably good understanding of biometric systems among the general public. People understand the use of biometrics as a means of personal identification using characteristics unique to each individual. Survey participants understood that biometrics enable individuals to access devices, accounts or locations with the aim of preventing personal identity theft, or allowing law enforcement to track people of interest with the objective of strengthening the safety and security of communities. Despite an overall awareness of biometrics, the most common security measure used by AIC respondents remains the non-biometric option of passwords (97%), with the most commonly used biometric technologies being signatures (76%) and fingerprints (63%; see Table 1). All other biometric options also registered positive previous use rates, with the minimum previous use rate of 22 percent for iris recognition.

Although passwords/PINs are still quite popular, many of those surveyed expressed their preference to use biometric technologies and, for some, a willingness to try human microchip implantation. The support for chip implants was surprisingly strong as long as health and security concerns were addressed. Recent victims of identity crimes expressed a greater overall willingness to use biometric technologies as well as chip implantation to protect their personal information. Smith, Gannoni and Goldsmid (2019) have stated that as the biometrics market continues to develop, further research is needed to understand individual motivations to use biometric technologies, particularly in the rapidly developing areas of facial recognition and multi-modal systems that combine various biometrics. The Ada Lovelace Institute (2019) has identified an additional gap in the research to address concerns by minority groups who report lower levels of comfort with the use of facial recognition technology due to bias.

The findings of the AIC interviews and surveys revealed acceptance of biometrics use in government settings to be much higher than for use in the private sector, although respondents were asked to assess acceptability in general, rather than in terms of specific biometric methodologies—such as how data are stored and accessed. However, the support for government use was not found to be unconditional by those surveyed, demonstrating a general opposition to covert surveillance and watch-list matching (except for serious crime and terrorism). There was a general lack of confidence among the various survey cohorts in the use of biometric technologies by the private sector, with the view expressed that commercial benefit will ultimately override ethics.

There were concerns expressed about potential problems with biometrics such as system error, human error, false enrolment and inaccurate matching due to physical changes or ethnic bias. Public education on biometric systems, how they work and what they are used for is generally lacking. Government and industry need to provide more information on biometric technologies to the public and explain security and privacy aspects more fully. A greater level of user information is required to explain vulnerabilities and how to use systems securely. These questions could be addressed in future surveys by asking precisely about how data are obtained from users, stored and made use of in various contexts.

A recurring sentiment of the various survey participants regarding the use of biometric systems was having freedom of choice, with many suggesting that an opt in/opt out policy should be the accepted norm. There was, however, flexibility among the majority of those surveyed when national security and community safety were used as justification for enforced use of biometrics and crowd surveillance. Use of biometrics data without informed consent remains an issue and obstacle for industry growth and development. Stricter regulations and policy upgrades may or may not limit innovation and more review is needed.

Privacy and data protection concerns continue to be the leading market restraint for the biometrics industry as reported by the Biometrics Institute (2019) and by the AIC interviewees and survey respondents. The survey by the Ada Lovelace Institute also supported these views. The Australian Government's National Identity Security Strategy (Department of Home Affairs 2020b) aims to address this by adhering to privacy obligations under Australian Privacy Principles and developing a government best practice for sharing biometric data.

The largest area of predicted biometrics industry growth is facial recognition technology and the associated AI that assists that technology. Multi-modal systems are also likely to take on importance in the years ahead. Despite this growth, AI Now (2019) has called on industry, government and business to halt all use of facial recognition technology until adequate regulations are in place to address associated risks. The Ada Lovelace Institute (2019) has also found public support in the United Kingdom for biometrics companies pausing sales of facial recognition technology, arguing a need for more government regulation. Half of the Ada Lovelace Institute (2019) cohort were also in agreement that the private sector should not be allowed to supply the technology to the police.

The expenses associated with incorporating biometric systems within an organisation are being addressed through the rapidly developing area of BaaS. Microsoft has also announced the development of FRaaS as a future addition to its Azure cloud app ecosystem. These developments will rapidly expand public and private access to biometric technology and the perceived privacy and ethics issues associated with the technology. International legislation and policy reform must be addressed to alleviate concerns and ensure that privacy rights are maintained.

The biometrics industry is rapidly developing and is arguably outpacing current privacy laws and ethics policies. Further dialogue is needed to understand the driving force behind areas of user mistrust. This input will enable public and private sector organisations to be more efficient and thorough in their legislation and planning. Public trust plays a central role, with continued and ongoing research needed to understand user willingness or unwillingness to use these stronger security methods. More information is required on systems' vulnerabilities to bias, fraud and misuse along with greater investigation into the adaptive behaviour of criminals as a result of these enhanced user authentication processes. Understanding the attitudes of members of the public towards the impact on privacy of surveillance technologies used for public security is also an essential, but complex, consideration for policymakers.

References

URLs correct as at February 2021

Ada Lovelace Institute 2019. *Beyond face value: Public attitudes to facial recognition technology*. London: Nuffield Foundation. https://www.adalovelaceinstitute.org/beyond-face-value-public-attitudes-to-facial-recognition-technology/

AI Now Institute (AI Now) 2020. *AI 2019 report*. New York: New York University. https://ainowinstitute.org/AI_Now_2019_Report.pdf

Anderson R 2020. *Security engineering: A guide to building dependable distributed systems*, 3rd ed. Oxford: Wiley

Attorney-General's Department (AGD) 2013. *National Identity Security Strategy 2012*. Canberra: AGD. Now available from the Department of Home Affairs: https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-security

Australian Bureau of Statistics 2019. *Australian demographic statistics, Jun 2019*. ABS cat. no. 3101.0. Canberra: Australian Bureau of Statistics. https://www.abs.gov.au/ausstats/abs@.nsf/mf/3101.0

Australia Post 2020. *Digital iD*. https://www.digitalid.com/

Aware 2020. Biometrics-as-a-service (BaaS). https://www.aware.com/biometrics-as-a-service/

Bajkowski J 2019. CBA's new app will soon drill government biometric holdings. *iTnews* https://www.itnews.com.au/news/cbas-new-app-will-soon-drill-government-biometric-holdings-528918?eid=1&edate=20190801&utm_source=20190801_AM&utm_medium=newsletter&utm_campaign=daily_newsletter

Biometrics and Forensics Ethics Group 2019. *Ethical issues arising from the police use of live facial recognition technology*. Croydon: Biometrics and Forensics Ethics Group. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf

Biometrics Institute 2020. *Biometrics Institute industry survey 2020*. London: Biometrics Institute

Biometrics Institute 2019. *Biometrics Institute industry survey 2019*. London: Biometrics Institute

Burt C 2019a. Australia Digital Transformation Agency to integrate biometrics with myGov this year. *Biometric Update*. https://www.biometricupdate.com/201908/australia-digital-transformation-agency-to-integrate-biometrics-with-mygov-this-year

Burt C 2019b. Australia Post accredited as trusted provider for government digital identity service. *Biometric Update*. https://www.biometricupdate.com/201907/australia-post-accredited-as-trusted-provider-for-government-digital-identity-service

Bushell-Embling D 2018. DTA launches first myGovID pilot. *GovTech Review*. https://www.govtechreview.com.au/content/public-sector-network/article/dta-launches-first-mygovid-pilot-51640953

Chip My Life 2020. Implant chips. *Chip My Life*. https://chipmylife.io/collections/implants

Crampton J 2019. Platform biometrics. *Surveillance & Society* 17(1/2). https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/13111

Department of Home Affairs 2020a. *Australia's 2020 cyber security strategy: A call for views*. Canberra: Department of Home Affairs. https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-strategy-2020-discussion-paper.pdf

Department of Home Affairs 2020b. *National identity security strategy: A national biometric interoperability framework for Government in Australia*. Canberra: Department of Home Affairs. https://www.homeaffairs.gov.au/criminal-justice/files/national-biometric-interoperability-framework-for-government-in-australia.pdf

Digital Transformation Agency (DTA) 2020. Creating a GovPass digital identity. https://www.dta.gov.au/blogs/creating-govpass-digital-identity

Faulkner C 2017. What is NFC? Everything you need to know. *TechRadar*. https://www.techradar.com/news/what-is-nfc

Franks C & Smith RG 2020. *Identity crime and misuse in Australia: Results of the 2019 online survey*. Statistical Report no. 27. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/sr/sr27

Goldsmid S, Gannoni A & Smith RG 2018. *Identity crime and misuse in Australia 2017: Results of the 2017 online survey.* Statistical Report no. 11. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/sr/sr27

Greene J 2020. What is biometrics as a service? *Imageware.* https://blog.iwsinc.com/what-is-biometrics-as-a-service

Hall R 2017. *Surveillance and public space*. Oxford: Oxford Research Encyclopedias. https://oxfordre.com/communication/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-145

Hendry J 2020. Govpass: The DTA's answer to Austalia's digital ID problem. *iTnews*. https://www.itnews.com.au/news/govpass-the-dtas-answer-to-australias-digital-id-problem-538856

Hoffman C 2016. What is RFID, and is it really a security concern? *How-To-Geek*. https://www.howtogeek.com/189936/htg-explains-what-is-rfid/

International Data Group (IDG) 2018. *Executive summary: 2018 cloud computing survey*. Framingham: International Data Group. https://cdn2.hubspot.net/hubfs/1624046/2018%20Cloud%20Computing%20Executive%20Summary.pdf

Jorna P, Smith R & Norman K 2020. *Identity crime and misuse in Australia: Results of the 2018 online survey*. Statistical Report no. 19. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/sr/sr19

Kollewe J 2018. Alarm over talks to implant UK employees with microchips. *Guardian*. https://www.theguardian.com/technology/2018/nov/11/alarm-over-talks-to-implant-uk-employees-with-microchips

Lupton D & Michael M 2017. Depends on who's got the data: Public understandings of personal digital dataveillance. *Surveillance & Society* 15(2). https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/whos_data

Ma A 2018. Thousands of people in Sweden are embedding microchips under their skin to replace ID cards. *Business Insider Australia*. https://www.businessinsider.com.au/swedish-people-embed-microchips-under-skin-to-replace-id-cards-2018-5?r=us&ir=t

Martin S 2019. Committee led by coalition rejects facial recognition database in surprise move. *Guardian*. https://www.theguardian.com/australia-news/2019/oct/24/committee-led-by-coalition-rejects-facial-recognition-database-in-surprise-move

Parliamentary Joint Committee on Intelligence and Security 2019. *Advisory report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019*. Canberra: Parliament of Australia. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Identity-Matching2019/Report

Pascu L 2020. AIH Technology joins Microsoft Partners Network, ventureLAB's Tech undivided initiative. *Biometric Update.* https://www.biometricupdate.com/202003/aih-technology-joins-microsoft-partners-network-venturelabs-tech-undivided-initiative

Reserve Bank of Australia 2020. Inflation calculator. *Reserve Bank of Australia.* https://www.rba.gov.au/calculator/financialYearDecimal.html

Rhue L 2018. *Racial influence on automated perceptions of emotions*. College Park: University of Maryland:. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765

Riley C, Buckner K, Johnson G & Benyon D 2009. Culture and biometrics: Regional differences in the perception of biometric authentication technologies. *AI & Society*. 24: 295–306. https://doi.org/10.1007/s00146-009-0218-1

Semnani-Azad Z, Chien S, Forster Y, Schuckers S, & Gan H 2019. *Development of trust measure in biometric technology*. Proceedings of the 52nd Hawaii International Conference of System Sciences. Honolulu: University of Hawaii at Manoa. https://par.nsf.gov/servlets/purl/10136377

Singh S 2018. Understanding Aadhaar: The unique identification authority of India and its challenges. *Human Rights Defender* 27(3): 21–24.

Rowe E, Akman T, Smith RG & Tomison AM 2013. Organised crime and public sector corruption: A crime scripts analysis of tactical displacement risks. *Trends & issues in crime and criminal justice* no. 444. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi444

Smith RG, Brown R & 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. https://aic.gov.au/publications/rpp/rpp130

Smith RG & Franks C 2020. *Counting the costs of identity crime and misuse in Australia, 2018–19*. Statistical Bulletin no. 28. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/sr/sr28

Smith RG, Gannoni A & Goldsmid S 2019. *Use and acceptance of biometric technologies in 2017*. *Trends & issues in crime and criminal justice* no. 569. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi569

Smith RG & Hutchings A 2014. *Identity crime and misuse in Australia: Results of the 2013 online survey.* Research and public policy series no. 128. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/rpp/rpp128

Smith RG & Jorna P 2018. *Identity crime and misuse in Australia: Results of the 2016 online survey.* Statistical Report no. 6. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/sr/sr19

Stokkink Q & Pouwelse J 2018. *Deployment of a blockchain-based self-sovereign identity.* Cornell University. https://arxiv.org/abs/1806.01926

Sydney Morning Herald 2003. The print that never fades. https://www.smh.com.au/national/the-print-that-never-fades-20031127-gdhv4w.html

United States Government Accountability Office 2002. *Technology assessment: Using biometrics for border security.* GAO-03-174. Washington, DC: Government Accountability Office. https://www.gao.gov/products/GAO-03-174

Yoti 2020. Multi-factor biometric authentication. https://www.yoti.com/business/authentication/

AIC reports

Research Report

Christie Franks is a Research Analyst at the Australian Institute of Criminology.

Dr Russell G Smith is Professor in the College of Business, Government and Law at Flinders University and a former Principal Criminologist at the Australian Institute of Criminology.

Australia's national research and
knowledge centre on crime and justice

aic.gov.au