Midas Touch: Consumer Implications of the Use of Smartphone Biometric Data

Jelena Ardalic

Google-ACCAN Intern

Dec - April, 2017-18

accan

“Midas Touch: Consumer Implications of the Use of Smartphone Biometric Data Capturing Capabilities”

Authored by Jelena Ardalic.

Edited by: Narelle Clark (ACCAN)

Published in 2018.

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers.

Australian Communications Consumer Action Network
Website: www.accan.org.au
Email: research@accan.org.au
Telephone: +61 2 9288 4000
If you are deaf, or have a hearing or speech impairment, contact us through the National Relay Service: www.relayservice.gov.au.

ISBN: 978-1-921974-55-7

This work can be cited as: Ardalic, J., 2018, *Midas Touch: Consumer Implications of the Use of Smartphone Biometric Data Capturing Capabilities*, Australian Communications Consumer Action Network, Sydney.

Table of Contents

Acknowledgements

This report would not have been possible without the expertise, assistance and input of the following:

- ACCAN; and
- Google Australia Pty Ltd.

Executive summary

When the first smartphone was released in the 1990s, it was nowhere near as technologically advanced as the smartphones released in the last decade. In the last decade, consumers have been presented with smartphones from brands such as Google, Apple, Samsung, Sony, Huawei and HTC.

As smartphones became more accessible, easy to use and convenient, Australian consumers began purchasing and utilising smartphones more and more. One form of technology that has enabled the accessibility and ease of use is biometric technology in smartphones for purposes ranging from identification, verification, authorisation and authentication.

A biometric is any unique, biological characteristic that can be measured to identify and verify a human being. In the popular mind, biometrics have typically been associated with Hollywood spy movies or crime scenes and criminals. Yet biometrics have mainly been used in Australia on a national level by the Australian government to screen travellers at border checkpoints and, more recently, on a national scale for identity matching capabilities. The focus of this report, however, is the more recent application of biometrics – that is, in smartphones – and the implications of this.

The use of biometrics in smartphones has been promoted as a benefit to Australian consumers, aimed to make smartphones more accessible, simple to use and secure, as opposed to the use of PINs, passcodes or passphrases, which are often difficult to remember and easily compromised.

Biometric systems are not entirely secure. General biometrics systems can be subject to security breaches, while smartphone biometrics tend to be securely located within a smartphone. Recent breaches have proven that even the new iPhone X Face ID can be compromised. An important thing to note is that once compromised, biometrics cannot be changed like a password can.

The most relevant legislation that applies to smartphone biometrics is the *Privacy Act 1988* (Cth). The Act seeks to balance out the protection of individuals' privacy versus that of the interests of entities in performing their functions and activities.[1] The Act includes biometrics under its definition of sensitive information,[2] which is important in the context of potential data breaches.

The previous point links with another privacy implication of the use of smartphone biometrics, which is the use of biometrics in identifying consumers without their knowledge, especially if consumers are unaware of how their biometric data is being stored and shared.

Through reviewing surveys, peer-viewed and non-peer-reviewed texts, government and industry papers, as well as conducting interviews with a range of industry professionals, what remains consistent is that smartphone biometrics, although convenient and simple to use, have enormous privacy implications that affect consumers if compromised.

As such, it is crucial for government and industry to ensure that consumers are adequately informed of just how severe the worst implications of smartphone biometric data capturing capabilities really are. Consumers should also be empowered to take a more proactive role in understanding more about their biometric data. This includes being made aware of what biometric data is, how it is stored on their smartphone, how secure it is, the ways in which their captured biometric data is being used and can be used, as well as the implications of this.

[1] s 2A(b).
[2] s 6(1)(d)-(e).

Introduction

In the ancient myth of King Midas, King Midas, the Phrygian ruler, had it all but he wanted one more thing, which was the power to turn everything he touched into gold. His wish was granted by god Dionysus and he was able to turn everything he touched into gold. His love for gold and new found Midas touch quickly lost its shine – King Midas' daughter turned to gold, his food turned to gold, and he was lonely and starving. It was not a blessing, but a curse. It was possible to have too much of a good thing.

When we receive or purchase our smartphones and use its biometric features, we fall in love with its beauty, ease of use, and convenience. We enable the biometric features and we feel like we have the world at our fingertips. We think we have the Midas touch and before we know it, just like King Midas, things do not end well. Or do they in this case?

About this Report

The aim of this research project was to examine the implications of the advancements in smartphone biometric data capturing capabilities for Australian consumers. This means looking at current and emerging capabilities of smartphone technology with regard to biometric data capturing and examining what the implications of this are.

To address this aim, a variety of sources have been used, including:

- Smartphone usage consumer surveys and studies;
- Peer-reviewed and non-peer-reviewed literature;
- Government and industry policy papers, reports and submissions; and
- Independently conducted phone interviews with government and industry professionals.

The project outputs include:

- An explanation of the current uses of biometrics generally in both an Australian and international perspective;
- An explanation of how smartphones are currently being used by Australian consumers, especially in relation to biometrics;

- An explanation of the current biometric data capturing capabilities in smartphones with both an Australian and international perspective;
- The implications of the use of smartphone biometrics;
- An assessment of current and incoming legislation in relation to biometrics;
- The impact on consumer connectivity that will arise from developments in smartphones and other biometric data capturing capabilities; and
- Some potential approaches that government and industry can take to help support the use of this technology, especially in relation to Australian consumers.

What are Biometrics?

Biometrics are measurements and use any physical or behaviourally unique characteristics to identify or verify an individual.[3] There are a range of biometrics including: fingerprints, hand geometry, face recognition, voice recognition, retinal scanning, iris scanning, hand signature, keystroke dynamics, brain wave sensors, and electrocardiography.[4]

The Different Types of Biometrics

Fingerprints

Fingerprints are among one of the most common biometrics used due to their ability to be used almost universally and their uniqueness.[5] Fingerprint scanning technology can analyse the unique individual patterns on an individual's fingertips.[6] There are different ways to verify fingerprints – fingerprints may be verified by matching minutiae, or by using print/pattern-matching devices, or by methods of moiré-fringe patterns and ultrasonic. The system used for identifying users by a government level is called Automated Fingerprint Identification Systems ('AFIS') and it uses fingerprint recognition systems.[7]

---

[3] K Krishnaprasad and PS Aithal, 'Fingerprint Image Segmentation: A Review of State of the Art Techniques' (2017) 2(2) *International Journal of Management, Technology, and Social Sciences (IJMTS)* 29, 29 <https://ssrn.com/abstract=3025477>.
[4] George Kofi Gagbla, 'Applying Keystroke Dynamics for Personal Authentication' (2005) 1, 5-6 <https://ssrn.com/abstract=2508480>.
[5] Krishnaprasad and Aithal, above n 3.
[6] Gagbla, above n 4, 5.
[7] Ibid.

Hand Geometry

Similarly to fingerprints, hand geometry enables users to be identified by examining their hand. Hand geometry biometrics uses unique characteristics such as length of fingers, the thickness of fingers and hands, and overall hand surface area. However, this biometric technology is typically not used in non-high security environments but is more commonly used in server rooms, day-care centres, airports, hospitals, and government agencies due to its expensive and inconvenient nature.[8]

Facial

Facial recognition involves the analysis of the unique characteristics of a person's face, such as eyes, nose, and lips. A digital camera takes a facial image of the individual for authentication by comparing it against known facial geometry. The use of facial recognition is more prominent for public applications such as ATMs and licence verification, because of this requiring minimal user training.[9]

Voice

Voice recognition systems capture voice features such as pitch, tone and frequency that are unique to an individual in order to authenticate a user. This method tends to be used for financial log-ins and for medium-security access. Voice recognition systems are susceptible to abuse as criminals may use it to facilitate crime, such as stealing and/or duplicating another individual's voice to gain unlawful access to their systems and accounts.[10]

Iris and Retinal Scanning

Iris scanning works by analysing '*the pattern of flecks on the iris, which is on the surface of the eyes*'.[11] Gagbla argues that '*it is also expensive, but is much easier to use than retinal scanning - in fact, the image can be taken using a video camera from up to three feet away, making this method appropriate for checkout counters and ATM machines*'. As for retinal scanning, systems that analyse the retina work by directing '*low-intensity infrared light through the pupil to identify the unique blood vessel pattern in the back of the eye*'.[12] Although it can be accurate, it can be impractical, due to

[8] Ibid.
[9] Ibid.
[10] Ibid.
[11] Ibid 6.
[12] Ibid 5.

requiring the user '*to look into a receptacle and focus on a given point*'. This means that it is not user-friendly for users that wear glasses or those that are not comfortable using the scanner in close proximity to their eyes. As a result, retinal scanning is not popular or widely accepted by most users.[13] Whereas iris biometrics have '*a good verification rate and resistance to imposter [and] iris data is stable with age, and identical for left and right eyes'*.[14]

Signature

Hand signature verification involves the process of analysing how an individual signs a name.[15] Relevant features are the speed, velocity, pressure, and shape of the signature. Hand signature verification is useful for verifying identities in transactions. It is an accurate form of biometric technology and is relevant to situations where a signature is used for identification.[16]

Other Emerging Biometrics

Keystroke Dynamics

Keystroke dynamics analyse how a user types on their keyboard.[17] This has the potential to identify the user as keystroke patterns are unique to every individual.[18] Keystroke dynamics can help determine the gender and age group of individuals as opposed to relying on traditional information collection based on trust. As a result of the information collected by keystroke dynamics, it can allow eCommerce retailers to target their intended client. Further, it has been argued that keystroke dynamics can benefit women and children.[19] Indeed, keystroke dynamics are able to identify the gender and age range of the user, hence making it possible to potentially protect women and children from any cyber threats.[20] This biometric technology is cost-effective and

---

[13] Ibid.
[14] Nimalan Solayappan and Shahram Latifi, 'A Survey of Unimodal Biometric Methods' (Paper presented at Proceedings of the 2006 International Conference on Security & Management, Las Vegas, Nevada, USA, 26-29 June 2006) 3 <https://pdfs.semanticscholar.org/8b0c/87e040c8718fd11e545e911996e3a149c69d.pdf>.
[15] Gagbla, above n 4, 6.
[16] Ibid.
[17] Ibid.
[18] Soumen Roy, Utpal Roy, and DD Sinha, 'Automatically Age Group and Gender Prediction by Analysing Typing Pattern on Touchscreen' (29 November 2017) 1, 2 <https://ssrn.com/abstract=3079504>.
[19] Ibid 5.
[20] Ibid.

practical, but an issue is that it is often difficult to gain more valuable biometric data on individuals due to the fact that there is no uniform keyboard that all users being recorded use.[21]

Brain Wave Sensors

It has been suggested that brain wave sensors could be an emerging popular form of biometrics.[22] Indeed, companies have begun to develop non-invasive brain-computer interfaces that use electroencephalography ('EEG') technology to record how human brains react to certain stimuli. As an example, IBM and Intel have been developing technology that enables individual reactions to be understood and to allow humans to control technology with their minds.[23] Brain wave patterns are unique to an individual, hence the potential for this biometric technique to be used to identify and authenticate individuals.[24]

Electrocardiography

Electrocardiography ('ECG') has been another popular biometric identifier, particularly in the digital wearables industry because of the real-time biometric data it provides to both consumers and companies.[25] Eberz et al explain that ECG '*records the electrical activity of the heart over time*'. They elaborate that:

> '*while ECG is typically recorded in a hospital using 10 electrodes placed on the patient's skin, it can also be measured using two electrodes, thus making it feasible to record with wearable devices. Due to its distinctiveness and universality (every living human has a heartbeat that can be measured), ECG as a biometric has attracted considerable attention in recent years*'.

[21] Gagbla, above n 4, 6.
[22] Michelle Scheinman, 'Protecting Your Brain Waves and Other Biometric Data in a Global Economy' (8 April 2013) 1, 5 <https://ssrn.com/abstract=2382951>.
[23] Ibid 6.
[24] Ibid 7.
[25] Simon Eberz, Nicola Paoletti, Marc Roeschlin, Andrea Patané, Marta Kwiatkowska, Ivan Martinovic, 'Broken Hearted: How To Attack ECG Biometrics' (2017) Network and Distributed System Security (NDSS) Symposium 1, 1 <http://qav.comlab.ox.ac.uk/papers/epr+17.pdf>.

Distinguishing Between Verification, Identification, Authentication, and Authorisation in Biometric Systems

To be able to understand how biometrics are used and what their implications are for Australian consumers, it is important to differentiate between verification, identification, authentication and authorisation. Prasanalakshmi and Kannammal distinguish that, '*verification involves a confirming or denying a person's claimed identity. In Identification, one has to establish a person's identity*'.[26] Although, they note that for verification and identification it is best to have a specific biometric system in order to minimise any complexities that each system may have, as '*identification involves comparing the acquired biometric information against templates corresponding to all users in the database, while verification involves comparison with only those templates corresponding to claimed identity*'. Clarke argues that definitions regarding identity verification are often exaggerated, as they suggest that technologies such as biometrics are '*foolproof, and can deliver verity, or truth*'.[27] Instead, Clarke suggests that a better term for common definitions of verification is identity authentication. Authentication works by comparing one thing against the other, such as an individual claiming to belong to one entity being compared against the biometric data relevant to that entity, and then if the measurements match, the person is authenticated because they are who they are claiming to be. As for authorisation, it can be described as '*the process whereby it is determined what a particular (id)entity is permitted to do*'.[28]

What is a Smartphone?

A smartphone is defined as '*a combination cellphone and handheld computer…A lot more personal than a personal computer, a smartphone is generally within reach at all times*'.[29] Another definition similarly suggests that a smartphone is essentially '*a mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded apps*'.[30]

---

[26] B Prasanalakshmi and A Kannammal, 'Analyzing Security Measures with Unimodal and Multimodal Biometrics' (2009) *International Conference on Sensors, Security, Software and Intelligent Systems* 26, 26 <https://ssrn.com/abstract=2946038>.
[27] Roger Clarke, *Biometrics and Privacy, 'Uses of Biometrics'* (15 April 2001) <http://www.rogerclarke.com/DV/Biometrics.html>.
[28] Roger Clarke, *A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation* (15 February 2010) <http://www.rogerclarke.com/ID/IdModel-1002.html>.
[29] PC Magazine, *Encyclopedia: Definition of: Smartphone* <https://www.pcmag.com/encyclopedia/term/51537/smartphone>.
[30] Oxford Dictionaries, *Smartphone* <https://en.oxforddictionaries.com/definition/smartphone>.

In the 1990s the first smartphone was introduced - the first being the IBM Simon in 1992.[31] Since then, smartphones have been developed, such as Apple's first iPhone and Google's Sooner and HTC Dream by 2007.[32]

Figure 1: Early models of smartphone.[33]

A consumer's captured biometric data is often stored on the user's smartphone device. This means that this data is centralised, or in one location. For example, on Android devices, fingerprint data is stored in what is called a 'Trusted Execution Environment' ('TEE').[34] Android Central explains that '*a TEE is a separate and isolated area in the*

[31] Steven Tweedie, 'The world's first smartphone, Simon, was created 15 years before the iPhone', *Business Insider* (online), 14 June 2015 <https://www.businessinsider.com.au/worlds-first-smartphone-simon-launched-before-iphone-2015-6?r=US&IR=T>.
[32] Andrew Martonik, *A look back at Sooner, Google's first Android phone* (21 October 2015) Android Central <https://www.androidcentral.com/look-back-google-sooner-first-android-phone>.
[33] PC Magazine, *Encyclopedia: Definition of: Smartphone* <https://www.pcmag.com/encyclopedia/term/51537/smartphone>.
[34] Jerry Hildenbrand, *How does Android save your fingerprints?* (26 September 2017) Android Central <https://www.androidcentral.com/how-does-android-save-your-fingerprints>.

phone's hardware'. Running on the TEE hardware is Google's Trusty OS. Android Central explains:

> '*When you register a fingerprint on your Android phone, the sensor grabs the data from the scan. Trusty OS analyzes this data inside the TEE, then creates two things: a set of validation data and an encrypted fingerprint template. This appears to be junk data to everything except the TEE who also has the key to decipher that junk data. This encrypted fingerprint template is stored in an encrypted container either on the TEE or on your phone's encrypted storage. Three encryption layers mean it's nearly impossible to get the data, and even if you could it's useless without a way to decipher it*'.[35]

Apple states that the chip in their users' device:

> '*includes an advanced security architecture called the Secure Enclave, which was developed to protect your passcode and fingerprint data. Touch ID doesn't store any images of your fingerprint, and instead relies only on a mathematical representation. It isn't possible for someone to reverse engineer your actual fingerprint image from this stored data. Your fingerprint data is encrypted, stored on the device, and protected with a key available only to the Secure Enclave. Your fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data. It can't be accessed by the OS on your device or by any applications running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases*'.[36]

[35] Ibid.
[36] Apple Support, *About Touch ID advanced security technology* (11 September 2017) Apple <https://support.apple.com/en-au/HT204587>.

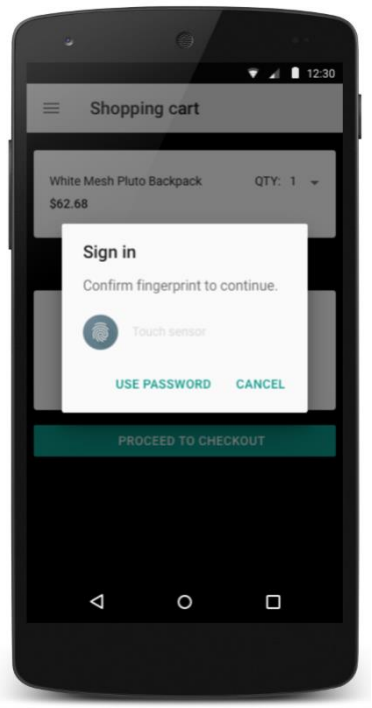


Figure 2: Android smartphone shows a pop-up on screen asking the user to confirm their fingerprint to authorise payment.[37]

[37] Android Developer, *Android 6.0 APIs* (25 April 2018) <https://developer.android.com/about/versions/marshmallow/android-6.0.html>.

Australian Consumer Smartphone and Biometric Usage

Having established the different forms of biometrics, for the purposes of this paper fingerprint, facial, iris and voice biometrics will be the primary biometrics referred to due to the predominance of them because of smartphone advancements in relation to these biometrics[38] and because of the ease and accuracy of using them.[39]

Australians and Their Smartphones: What Do The Statistics Say?

The most current and detailed survey of Australian consumers and their smartphones is the *Deloitte Mobile Consumer Survey 2017*. The survey indicates that Australians are among one of the world's highest adopters of smartphones, with an estimated 88 per cent of Australians owning one,[40] which shows a four per cent increase from 2016.[41] As well, the Australian Bureau of Statistics reported that, '*as at 30 June 2017, there were approximately 26.3 million mobile handset subscribers in Australia*'.[42] This is a slight increase since December 2016, rising only 3.4 per cent. Indeed, it is estimated that by 2022, there are set to be approximately 19.27 million Australian smartphone users.[43]

---

[38] See generally Obi Ogbanufe and Dan J Kim, 'Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment' (2018) 106 *Decision Support Systems* 1, 2 <https://doi.org/10.1016/j.dss.2017.11.003>.
[39] See generally Hayiel Hino, 'Assessing Factors Affecting Consumers' Intention to Adopt Biometric Authentication Technology in E-shopping' (2015) 14(1) *Journal of Internet Commerce* 1, 3 <https://doi.org/10.1080/15332861.2015.1006517>.
[40] *Deloitte Mobile Consumer Survey 2017,* 4 <https://www2.deloitte.com/au/mobile-consumer-survey>.
[41] Ibid 6.
[42] Australian Bureau of Statistics (ABS), *8153.0 - Internet Activity, Australia, June 2017* (29 September 2017) <http://www.abs.gov.au/ausstats/abs@.nsf/0/00FD2E732C939C06CA257E19000FB410?Opendocument>.
[43] Statista, *Number of smartphone users in Australia from 2015 to 2022 (in millions)* (July 2017) <https://www.statista.com/statistics/467753/forecast-of-smartphone-users-in-australia/>.

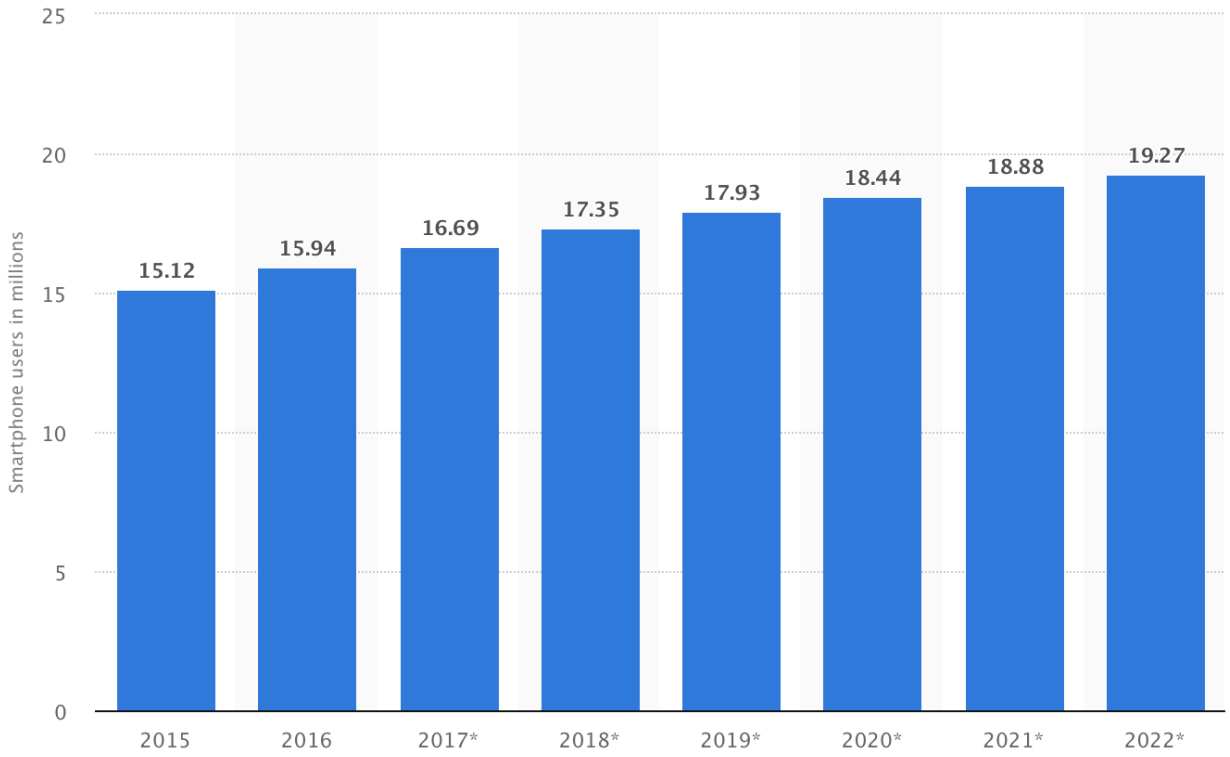


Figure 3: Graph shows that by 2020 will be an estimated 19.27 million Australian smartphone users.[44]

Australians are also using their smartphones everywhere and at any time, with over a third of Australians checking their phone within five minutes of waking up every morning and 70 per cent accessing their phones during mealtimes with others.[45] The most popular uses of smartphones among Australians are to check emails, social media and instant messaging.[46] This is particularly popular among the 18-24 age group as well as the 25-44 age group - the latter of which has seen a surge.

In Australia, Apple is the dominant brand of smartphone that Australians are using, with a reported 41 per cent of Australians owning an Apple smartphone.[47] This is followed by Samsung smartphones, with 34 per cent of Australians owning this brand and the remaining 25 per cent comprising of 'other' brands. This is useful in indicating the

[44] Ibid.
[45] *Deloitte Mobile Consumer Survey 2017*, above n 40.
[46] Ibid 15.
[47] Ibid 8.

future use of biometrics, as both these brands of smartphones have readily useable implementations of biometric technologies such as fingerprint, facial, iris and speech recognition. Indeed, according to Counterpoint Research, it is estimated that '*more than a billion smartphones will ship with facial recognition in 2020*'.[48]

Currently Trending: Australians are Increasingly Utilising Fingerprint Biometrics

The *Deloitte Mobile Consumer Survey 2017* demonstrates that Australians are increasingly utilising smartphone biometrics, particularly their fingerprints.[49] Since 2016, the use of fingerprint authentication has risen, with a reported 35 per cent increase in consumer use of this feature. Moreover, there has been an increase in the use of mobile payment technologies due to their increased availability and ease of use, with an increase of 25 per cent in purchasing done through a smartphone. Indeed, the Deloitte survey suggests that more Australians are both shopping and paying with their smartphones.[50] Particularly, fingerprints are a popular method of identifying Australian consumers' identities as well as authenticating their purchases. Since 2016, the use of fingerprint authentication on smartphones has increased 35 per cent.[51] Moreover, '*mobile payment technologies are becoming increasingly available, with in-app payment and touchless technology overcoming traditional barriers to purchase on smartphones*'. This consumer move has been attributed to smartphones' greater screen size, smartphone technology improvements, and mobile friendly webpages.

At least once a month, 24 per cent of Australians use their smartphone to shop online.[52] Since 2016, the amount of Australians that use their smartphone to browse online shopping websites has increased 14 per cent, whereas online purchases have risen by 25 per cent. Currently, it is the 18-24 age group that remain the primary users of biometric payment authentication technologies at 50 per cent, particularly among Apple users. This could be attributed to Apple being the most common smartphone used by Australians in this age group. It is interesting to note that the 18-24 age group shares the most data with companies online and according to the survey, trusts that these companies will not use their personal information nor share it with third parties. This may account for this age group's willingness to use their biometrics to authenticate

---

[48] Pavel Naiya, 'More than one billion smartphones to feature facial recognition in 2020' (Press Release, 7 February 2018) <https://www.counterpointresearch.com/one-billion-smartphones-feature-face-recognition-2020/>.
[49] *Deloitte Mobile Consumer Survey 2017*, above n 40.
[50] Ibid 41.
[51] Ibid 42.
[52] Ibid.

online payments. As a future indicator, financial technology experts have predicted that older, more traditional electronic payment methods, such as those utilising PINs and chip-based credit cards, '*will eventually be replaced with mobile and biometrics authentication based payment*'.[53]

Deloitte revealed that 94 per cent of their *Mobile Consumer Survey* respondents used their fingerprint to unlock their device, followed by 36 per cent which used their fingerprint to log into apps, 30 per cent to authorise payments/purchases, and 18 per cent to authorise money transfer to other people/organisations.[54]

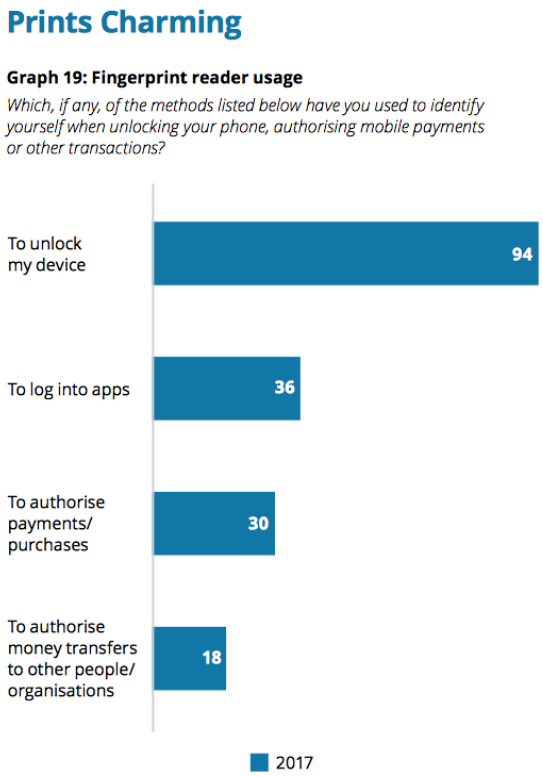


Figure 4: Graph from the *Deloitte Mobile Consumer Survey* shows fingerprint reader usage.[55]

Deloitte reported:

---

[53] Fintech Finance, *Fintech experts say mobile and biometric authentication to replace PINs within five years* <http://www.fintech.finance/01-news/fintech-experts-say-mobile-and-biometric-authentication-to-replace-pins-within-five-years/>, cited in Ogbanufe and Kim, above n 38, 1.
[54] *Deloitte Mobile Consumer Survey 2017*, above n 40, 43.
[55] Ibid.

'*As of mid-2017, 31 percent of all smartphone owners aged 16-75 used fingerprint recognition for at least one application, up 35 percent from 2016. Forty-five percent of smartphones now incorporate a fingerprint reader (up from one in three last year), and 69 percent of those who have the technology on their phones use it*'.[56]

Deloitte have estimated that the use of fingerprint authorisation is likely to rise in consumers accessing sensitive data, although PIN, passcode and passphrase identification methods still remain the most popular form of unlocking a smartphone, with 68 per cent of survey respondents using this method. However, it is likely that this will decline given the ease of unlocking a smartphone with a fingerprint and other more recent popular smartphone biometrics like facial biometrics in comparison to a six-digit PIN, passcode or passphrase.[57]

Biometrics, Security and Identity Crime

Research suggests that Australians are comfortable with the use of biometric technologies for security and verification purposes when accessing government services and in the context of airport security,[58] although Australians are not comfortable with the use of such technologies for the purposes of marketing, accessing public transport or enrolling in educational courses. As for the public sector, '*Australians appear to be quite comfortable with the idea of providing biometric information including fingerprints, voice recordings and iris scans to access government services such as those provided by Medicare (81%) and the Australian Taxation Office (75%)*'. Indeed, Australian Unisys survey results showed that respondents '*would be willing to use these biometrics to access their bank records (69%), health records (68%) and welfare payments (63%), and to submit tax returns or access their tax records (65%)*'.[59]

Australian consumers have reported that they are comfortable with the use of biometrics in order to prevent identity crime.[60] Emami et al note that as part of the National Identity Security Strategy (AGD 2012) in September 2014, an anonymous

---

[56] Ibid.
[57] Ibid.
[58] Catherine Emami, Dr Rick Brown and Dr Russell G Smith, 'Use and acceptance of biometric technologies among victims of identity crime and misuse in Australia' (2016) 511 *Trends and issues in crime and criminal justice* 1, 2 <https://aic.gov.au/publications/tandi/tandi511>.
[59] Ibid.
[60] Ibid 3.

online survey took place where a 5000-person sample of the Australian public was asked a series of questions regarding their views and experiences of identity crime. In this study, respondents revealed that they were most likely to use passwords and fingerprint recognition, and least willing to use voice recognition.[61] Particularly, 61 per cent of respondents to this study reported that they would use fingerprint recognition in the future. The results indicated that 96 per cent of the 427 survey respondents were willing to use biometric technologies in the future to protect their personal information from being compromised. Emami et al argue that the older respondents' willingness to use biometric technologies could be attributed to their potential concern over their personal information being misused, hence wanted to adopt more allegedly secure means of identification, i.e. biometrics.[62] Concerns about identity theft are serious, as identity crime costs Australians roughly $2.2 billion per year.[63] As for the younger respondents, Emami et al suggest that they may be unwilling to use biometrics due to any perceptions about biometrics being overly complex and impeding their quick access to the internet.[64] Moreover, Emami et al suggested that part of the reason why consumers may be unwilling to adopt the wider use of biometrics could be due to negative associations with using biometrics, such as fingerprints, due to criminal and policing associations.[65]

Visually Impaired Individuals and Cybersecurity

Literature suggests that vision impaired individuals are often vulnerable to cyber attacks. Azenkot et al found that vision impaired individuals tend not to be concerned or aware about cybersecurity, as they often use their smartphones without utilising the password features due to the inconvenience and accessibility issues with doing so.[66] For example, if a user were to mask their password by utilising a screen reader for example, some screen readers would then read the password characters or numbers as stars or clicks, hence making it almost impossible for users to type in their password

---

[61] Ibid 4.
[62] Ibid.
[63] Australian Government, Attorney-General's Department, *Face Matching Services, Fact Sheet – Face Matching Services* 1, 2 <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Face-matching-services-fact-sheet.pdf>.
[64] Emami et al, above n 58, 4.
[65] Ibid 2.
[66] Shiri Azenkot, Kyle Rector, Richard E Ladner, and Jacob O Wobbrock, 'PassChords: secure multi-touch authentication for blind people' (Paper presented at Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility, Boulder, Colorado, USA, 22-24 October 2012) 159, 159.

due to no text entry feedback.[67] Moreover, even if a user did not wish to mask their passwords, the screen reader may speak the password characters aloud, hence revealing a user's password to anyone around them. Further, even if a vision impaired user were to use a password manager or password recovery mechanism, it would often be quite impractical for them to use. As a result, vision impaired smartphone users may opt for storing their passwords elsewhere written in Braille, in files, or saved in applications.[68] As well, a reported study of blind individuals completed by Lobo et al showed that these individuals are more likely to use easy-to-type passwords, which are more predictable.[69]

Smartphones that enable users to access their device by using biometrics can enhance accessibility for those with blindness.[70] Despite the occasional accessibility issues with the use of fingerprint recognition (i.e. occasional failure to pinpoint how to place a fingerprint on the reader), respondents to the Lobo et al study that were iPhone users reported that Touch-ID was a convenient option. Moreover, users surveyed by Lobo et al expressed that they would not feel as comfortable with only biometrics-enabled access methods. Instead, blind users said they preferred a backup PIN option, in case their multiple fingerprint access attempts failed so that they would not need to be concerned about getting locked out of their device. Nonetheless, the use of biometrics to access smartphones makes using smartphones more accessible and secure for vision-impaired individuals.[71]

---

[67] Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia, 'Privacy concerns and behaviors of people with visual impairments' (Paper presented at Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea, 18-23 April 2015) 3523, 3527.
[68] Ibid 3529.
[69] Sylvan Lobo, Ulemba Hirom, VS Shyama, Mridul Basumatori, and Pankaj Doke, 'Coping with Accessibility Challenges for Security - A User Study with Blind Smartphone Users' (2017) 3, 10 <https://link.springer.com/chapter/10.1007/978-3-319-68059-0_1>.
[70] Ibid 12.
[71] Ibid.

The Implications of the Use of Smartphone Biometrics

From Passcodes to Biometrics

Security and Convenience

Manufacturers have promoted the idea that smartphone biometrics are more secure and convenient for the modern consumer.[72] Paul and Irvine argue that '*a key selling point of biometric authentication is that it allows users to move away from passwords, both for use in authenticating to third parties, and for unlocking their own physical device*'. Particularly, biometrics can remove the need for manually entering in passwords or PINs and they avoid issues that arise with log-ins such as forgotten or lost passwords. Juniper Research reported that one of the biggest benefits of using biometrics for authentication is increased security because of the risk of forgetting passwords or having passwords compromised, as well as reducing the risk from lost or stolen credit cards.[73] Moreover, they suggest that by 2019 '*more than 770 million biometric authentication apps will be downloaded per annum*'.

Despite the cited convenience and security benefits, such benefits are not felt by all.[74] A survey of individuals reveals that 90 per cent of respondents are concerned about data privacy with biometric authentication.[75] In an interview with the Chairman of the Australian Privacy Foundation and co-convenor of the Cyberspace Law and Policy Community, David Vaile, he said that consumers are left with '*the lifelong problem…of an irrevocable identifier, which looks like a benefit in the hands of the system operator,*

[72] Greig Paul and James Irvine, 'Fingerprint Authentication is here, but are we ready for what it brings?' (2017) 1, 1 <https://pure.strath.ac.uk/portal/files/45829838/Paul_Irvine_IEEE_CEM_2015_Fingerprint_authentication_is_here_but_are_we_ready.pdf>.
[73] Juniper Research, 'Biometric Authentication App Downloads to Reach 770 Million by 2019, finds Juniper Research' (Press Release, 20 January 2015) <https://www.juniperresearch.com/press/press-releases/biometric-authentication-app-downloads-to-reach-77>.
[74] Justin Lee, *Report shows growing public acceptance of biometric authentication* (15 July 2015) Biometric Update <http://www.biometricupdate.com/201507/report-shows-growing-public-acceptance-of-biometric-authentication>.
[75] Ibid.

but is very clearly a huge risk for the individual in part because you're stuck with it for life and in part because it's something that's very close to you'.[76]

Just like biometrics are unique to individuals, PINs, passcodes and passphrases are also considered unique to individuals and they are kept private, up until the point where authentication is needed. Yet with PINs, passcodes and passphrases, they can be subjected to compromise in a variety of ways, including brute force attacks, social engineering, key loggers, malware, as well as picked up during network transit and then recalled later on.[77] However, biometric systems can also be subject to brute force attacks, social engineering, key loggers and malware, which, although difficult, is not impossible.[78]

The NSW Attorney-General Internal Controls and Governance 2017 Report, in reviewing NSW agencies,[79] found that '*most agencies do not sufficiently monitor or restrict privileged access to their systems and some do not enforce password controls*'. As for agency monitoring of cyber security threats, it is unknown due to most agencies defining 'cyber attacks' differently.[80] However, it is reported that agencies have

---

[76] Interview with David Vaile, Chairman of the Australian Privacy Foundation and co-convenor of the Cyberspace Law and Policy Community (telephone, 7 February 2018).
[77] Bobby L Tait, 'Secure cloud-based biometric authentication utilising smart devices for electronic transactions' (2014) 6(1) *International Journal Electronic Security and Digital Forensics* 52, 54 <https://www.inderscienceonline.com/doi/abs/10.1504/IJESDF.2014.060170>.
[78] Adrian S Ungureanu and Claudia Costache, 'Palm Print as a Smartphone Biometric: Another option for digital privacy and security' (2016) 5(3) *IEEE Consumer Electronics Magazine* 71, 72 <http://ieeexplore.ieee.org/document/7539264/?reload=true>; Bkav Corporation, *Bkav's new mask beats Face ID in "twin way": Severity level raised, do not use Face ID in business transactions* (27 November 2017) <http://www.bkav.com/dt/top-news/-/view_content/content/103968/bkav﷒s-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions>; Chris Ip, *The Galaxy S8 Iris Scanner Can be Hacked With Aging Tech* (23 May 2017) Engadget <https://www.engadget.com/2017/05/23/galaxy-s8-iris-scanner-hacked/>; Roi Perez, *Starbug's in your eyes: German hacker spoofs iris recognition* (26 October 2015) SC Magazine UK <https://www.scmagazineuk.com/starbugs-in-your-eyes-german-hacker-spoofs-iris-recognition/article/535281/>; Paul Greig and James Irvine, 'IEDs on the Road to Fingerprint Authentication: Biometrics have vulnerabilities that PINs and passwords don't' (2016) 5(2) *IEEE Consumer Electronics Magazine* 79, 81 <http://ieeexplore.ieee.org/document/7450785/>; Yulong Zhang, Zhaofeng Chen, Hui Xue, and Tao Wei FireEye Labs, 'Fingerprints On Mobile Devices: Abusing and Leaking' (2015) *Blackhat Conference* 4-5, 7-9 <https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf>.
[79] For full list of agencies examined see pages 75-6 of New South Wales Auditor-General's Report, Audit Office of New South Wales, *Report on Internal Controls & Governance 2017* (20 December 2017) Audit Office of New South Wales 1, 3 <http://bit.ly/2Es7Ivk>.
[80] Ibid 4.

sufficient resources to monitor their cyber security. Of particular relevance to this paper was the cited issue of password controls within IT issues.[81] It was reported that '*forty-one per cent of agencies did not meet either their own standards or minimum standards for password controls*'. Yet, the recommendations did not point to the use of biometrics, but rather, recommended that '*agencies should review and enforce password controls to strengthen security over sensitive systems*'. More specifically, it was recommended that there be minimum lengths for PINs, passcodes and passphrases, further difficulty requirements, restrictions on the amount of failed log-in attempts, PIN, passcode and passphrase history, and that it be made mandatory to change PINs, passcodes and passphrases within certain periods of time. As such, PINs, passcodes and passphrases present difficulties both on the security and convenience level.

Phang and Pavlovksi argue that one of the biggest issues with the use of smartphone biometrics is that they can be compromised, resulting in a consumer's details being leaked against their will, or hacked.[82] Phang and Pavlovski explain that this is because:

> '*Human biometric markers are generally visible to everyone with people leaving physical residues on everything we touch, everywhere we go. Hence, many traits can be obtained in a generally straightforward manner using commodity technology available in the marketplace. Moreover, camera technology is sufficiently mature to enable high resolution photography of facial features, geometric attributes, and observable characteristics*'.

While there is apparent safety because biometrics are intrinsically and physiologically unique, it is because of this that makes any security compromise of them especially dangerous to consumers.[83] Indeed, consumers' usernames, PINs, passcodes and passphrases may be changed if compromised, hence allowing consumers some additional controls over their personal information. On the other hand, biometrics generally cannot be changed, hence the greater the danger and the less control over their personal information.[84] A security expert from Kaspersky Lab, Olga Kochetova, explained that the difference between biometrics and passwords is that once hacked,

---

[81] Ibid 18.
[82] Samantha SS Phang and Christopher J Pavlovski, 'Hazards of Biometric Authentication in Practice' (2016) 4(1) *IT in Industry* 34, 39 <http://it-in-industry.com/itii_papers/2016/4116itii05.pdf>.
[83] Greig Paul and James Irvine, 'IEDs on the Road to Fingerprint Authentication: Biometrics have vulnerabilities that PINs and passwords don't' (2016) 5(2) *IEEE Consumer Electronics Magazine* 79, 81 <http://ieeexplore.ieee.org/document/7450785/>.
[84] Ibid.

passwords can be changed, whereas biometrics cannot, thereby rendering a victim's personal information fully compromised forever.[85]

Biometrics in Payment Authentication

General trends in card fraud in Australia can point to the proliferation of crime in Australia, which is relevant to biometrics as many payment systems have begun implementing biometrics to authenticate users and transactions. Indeed, the *Deloitte Mobile Consumer Survey 2017* showed that there has been a 25 per cent increase in smartphone enabled purchases by Australian consumers,[86] particularly with Australian consumers increasingly using their fingerprints to identify themselves and authenticate purchases.[87] This can be seen as a positive outcome from the use of smartphone biometrics, especially as the Australian Payments Networks reported that Australian card fraud rose from the period from 2006 to 2016.[88] Indeed, card fraud increased 17 per cent from 2015 to 2016, with Card Not Present ('CNP') fraud increasing 15 per cent and representing 78 per cent of total card fraud. CNP fraud can be attributed to the difficulty that merchants have when attempting to differentiate between the original cardholders' details and the stolen information.[89] As a result, the use of biometrics in both authentication and identification could be useful for Australian consumers, because if cards are being stolen and PINs, passcodes and passphrases are being compromised, biometrics can provide another form of security for consumers.

Multimodal Biometrics

A multimodal biometric system is one where multiple biometric technologies are amalgamated to enhance the authentication and identification process.[90] Gagbla argues that '*this creates a more efficient and secured biometric system with a high level of credibility*'. The argument that multimodal biometrics enhances authentication and identification, security and efficiency stems from the argument that by utilising more biometrics – or in other words, multimodal biometric systems – consumers are better protected from any potential negative impacts that may come from using

---

[85] Kaspersky Lab, 'Biometric skimmers are here: Kaspersky Lab Examine Near-Future Threats to ATMs' (Press Release, 22 September 2016) <https://usa.kaspersky.com/about/press-releases/2016_biometric-skimmers-are-here>.
[86] *Deloitte Mobile Consumer Survey 2017*, above n 40.
[87] Ibid 41.
[88] Australian Payments Network, *Australian Payments Fraud 2017 Jan-Dec 2016 Data* 1, 2-3 <http://bit.ly/2DcBJ2a>.
[89] Ibid 3.
[90] Gagbla, above n 4, 6.

unimodal (or one form of) biometrics.[91] Indeed, the argument goes that just in case one form of biometric is spoofed, '*the person would still have to be authenticated using the other biometric*'. Counterpoint Research has said that in the future, they expect that '*mobile devices will combine biometric sensors for the face, iris, voice and fingerprints. Rather than competing against each other, each biometric technology will be layered on top of each other with the most convenient and least intrusive being selected on an application by application basis*'.[92]

This is particularly relevant when dealing with false rejections and false positives, as the single use of biometrics can result in skewed identification and authentication. Krishnaprasad and Aithal explain that, '*the False Rejection Rate is when the system fails to adequately identify an enrollee and is increased when the user wears glasses, adjusts their facial hair and changes their hairstyle*'.[93] This is also known as a 'false negative' and it can result in the correct individual being rejected by the biometric database.[94] Another thing that can occur is a 'false positive', which is slightly different to false negatives, in that '*the assertion will be authenticated, even though the person who presented was not the one the system thought it was*'.[95] As a result, it has been suggested that multimodal biometrics should be utilised as opposed to unimodal biometrics. Prasanalakshmi and Kannammal argue that by relying only on unimodal biometrics, it may not provide enough information about individuals.[96] An example is the use of fingerprint biometrics, as the fingerprints of minors tend to be undeveloped, tend to be faded in senior citizens, and perhaps worn out in some individuals.[97] Despite the argument that multimodal biometrics should be used in order to provide more accurate information about individuals, it has been suggested by Clarke that '*the tighter the tolerances are set (to avoid false positives), the more false negatives will arise; and the looser the tolerances are set (to avoid false negatives), the more false positives occur. The tolerance is therefore set to reflect the interests of the scheme's primary sponsor, with little attention to the concerns of other stakeholders*'.[98]

---

[91] Prasanalakshmi and Kannammal, above n 26, 29.
[92] Naiya, above n 48.
[93] K Krishnaprasad and PS Aithal, 'A Conceptual Study on User Identification and Verification Process using Face Recognition Techniques' (2017) *International Journal of Applied Engineering and Management Letters (IJAEML)* 1(1) 6, 8 <https://ssrn.com/abstract=2988405>.
[94] Clarke, *A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation*, above n 28.
[95] Ibid.
[96] Prasanalakshmi and Kannammal, above n 26, 29.
[97] Ibid.
[98] Clarke, *A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation*, above n 28.

It is argued that the use of multimodal biometric systems makes it more difficult to hack biometrics, due to the difficulty of accessing such systems.[99] Khan argues that unimodal biometrics can be faked, even with the use of a high-resolution image of a fingerprint presented to a system such as a fingerprint scanner.[100] The argument that follows is that '*by using multiple biometrics, even if one modality could be spoofed, the person would still have to be authenticated using the other biometric*'.[101] In addition, it often takes more effort to forge multiple biometrics, therefore the use of multimodal biometrics can be a deterrent to those wishing to unlawfully access biometrics. However, should a multimodal biometrics system be hacked, there will be a greater loss of personal information on consumers, rather than a compromise to just one form of biometric.

Biometrics Can Be Hacked

Australia's Current Cybersecurity Landscape

The Australian Cyber Security Centre ('ACSC') *Cyber Security Strategy 2016* outlines that Australians are using the internet increasingly, with eight in ten Australians accessing the internet every day.[102] Particularly, the *Deloitte Mobile Consumer Survey 2017* shows that there has been an increase in 4G subscribers.[103] Even with this increase, Wi-Fi is the most common form of connection for 63 per cent of Australian smartphone users, which is up from 49 per cent in 2016. Moreover, the ACSC *Cyber Security Strategy 2016* highlights that '*the Internet based economy is growing twice as fast as the rest of the global economy*', which is attributed to increasing business innovation and connectivity.[104] As a result, the Australian Government has emphasised the need to have strong cybersecurity in order to increase trust and confidence in cyberspace, hence furthering economic opportunities in the connected Australian economy. This is particularly relevant when considering that Australian '*businesses and governments are also benefiting from improved online and mobile technology... [by] using information gathered online to tailor products and services to individual needs*'. However, with these benefits, there are negatives, as '*Government, telecommunications, resources, energy, defence, banking and finance sectors are*

---

[99] Prasanalakshmi and Kannammal, above n 26, 29.
[100] Imran Khan, *Multimodal Biometrics– Is Two Better Than One?* (2006) Frost & Sullivan Insight <http://www.frost.com/prod/servlet/market-insight-print.pag?docid=80082644>.
[101] Ibid.
[102] Australian Government, *Australia's Cyber Security Strategy 2016* 1, 14 <http://bit.ly/2mjGv6T>.
[103] *Deloitte Mobile Consumer Survey 2017*, above n 40, 18.
[104] Australian Government, *Australia's Cyber Security Strategy 2016*, above n 102.

likely to remain key targets for cyber criminals and malicious state actors alike'.[105] Indeed, when connected to the internet, there is always the risk of being compromised.

The ACSC *Cyber Security Survey 2016* indicates that, '*most organisations (90%) faced some form of attempted or successful cyber security compromise during the 2015-16 financial year*'.[106] Indeed, the survey shows that malicious cyber threats against organisations occur on a daily basis. The survey results indicated that 58 per cent of organisations surveyed '*experienced at least one incident that successfully compromised data and/or systems*'. The ACSC reported that, '*government and commercial bulk data repositories provide a single point of storage for valuable information on large numbers of Australians*'.[107] In particular, one of the most valuable types of information cybercriminals seek is personally identifiable information ('PII'). The motivation behind gaining access to PII is to use the compromised PII to commit financial crimes, identity theft, and terrorism. Indeed, '*basic information, such as name, birth date and address, is often enough for criminals to impersonate victims*', as such, hacked biometrics could be of invaluable use to cybercriminals. In particular, '*the growth of online communication networks, forums and darknet marketplaces has also eased entry to the cybercrime market and introduced the notion of cybercrime as a service that can be purchased*'.[108]

The *First Annual Update for 2017* to the Australian *Cyber Security Strategy* indicates that despite the fact that Australian companies have been targeted more by malicious cyber attacks, they are becoming better equipped in how to deal with such attacks.[109] Despite this, the *First Annual Update for 2017* outlines that, '*cybercrime remains the most visible and damaging aspect of the cyber threat environment for the majority of Australian citizens and businesses*'.[110]

---

[105] Ibid 15.
[106] Australian Government, Australian Cyber Security Centre ('ACSC'), *2016 Cyber Security Survey* 1, 6 <https://www.acsc.gov.au/publications/ACSC_Cyber_Security_Survey_2016.pdf>.
[107] Australian Government, ACSC, *2017 Threat Report* 1, 38 <https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf>.
[108] Ibid 48.
[109] Australian Government*, Australia's Cyber Security Strategy: 2017 Update* 1, 8 <http://bit.ly/2mtpg3K>.
[110] Ibid 10.

How Biometrics Can Be Hacked

With new technologies such as smartphone biometrics, come concerns about the security of such technologies. Axelrod argues that '*physical privacy has been significantly affected by security and safety innovations, particularly with electronic locks based on codes, fobs and biometric technology, and from connecting security systems to the Internet of Things (IoT)*'.[111] In addition, it is extremely difficult to change biometrics, in comparison to a lost or compromised password, which can be quickly changed.[112] As a result, Paul and Irvine suggest that consumers may not have as much control as they think they do when using biometrics, due to the restricted ability to change biometrics.

The Australian Law Reform Commission has warned against the dangers of improperly accessed biometrics, by arguing that as with any personal information being stored in a centralised or local database or in an individual's possession, biometrics could be improperly accessed by nefarious individuals wishing to use them for another objective.[113] With advances to biometric data capturing capabilities, there are updates to how cybercriminals are operating.[114] Kaspersky Lab recently announced that dark web sellers have already began offering ATM biometrics skimmers, with fingerprint skimmers being most popular. Indeed, this links to the recent ACSC *Threat Report*, which highlighted the growth of darknet marketplaces that have enabled cybercrime to become a service available for purchase.[115]

Recent examples involving government employees and leading smartphone brands below demonstrate the vulnerability in the use of both biometrics generally and smartphone biometrics. One of the most well-known government data breaches was the Office of Personnel Management hack in December 2014. This hack led to the leak

---

[111] C Warren Axelrod, 'The New Age of Near-Zero Privacy' (2016) 4 *ISACA Journal* 1, 5 <https://www.isaca.org/Journal/archives/2016/volume-4/Documents/The-New-Age-of-Near-zero-Privacy_joa_Eng_0716.pdf>.
[112] Paul and Irvine, IEDs on the Road to Fingerprint Authentication: Biometrics have vulnerabilities that PINs and passwords don't, above n 83.
[113] Australian Government, Australian Law Reform Commission, *For your Information: Australian Privacy law and Practice*, Report No 108 (2008) Ch 9 Overview: Impact of Developing Technology on Privacy: Biometrics <https://www.alrc.gov.au/publications/9. Overview%3A Impact of Developing Technology on Privacy/biometric-systems>, citing Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004) 13–15.
[114] Kaspersky Lab, above n 85.
[115] Australian Government, ACSC, *2017 Threat Report*, above n 107, 48.

of approximately 5.6 million current and former government employees' personal data being compromised.[116] This personal data included employees' fingerprints.

Recently, Vietnam based security firm, Bkav, was able to demonstrate how their security experts from Vietnam managed to hack Apple's new Face ID biometric feature.[117] They were able to do so for less than $200 USD, by using a 3D mask made out of stone powder, silicone and glued on 2D photographs of the eyes. Indeed, Bkav was able to do this because stone powder is more accurate than paper tape (which they used in their previous mask to hack Face ID the first time) and because the photographs of the eyes used were printed infrared images, which is the same technology that Face ID uses to recognise faces.

Figure 5: Screenshot from a video uploaded on Bkav Corporation's YouTube account that shows that the researcher unlocked the iPhone X.[118]

Since the Bkav hack, Apple has said that the chance of a random individual breaking into another user's iPhone using Face ID was 1 in a million, in comparison to the 1 in

---

[116] Julianne Pepitone, 'OPM Hack: 5.6 Million Fingerprints (Not 1.1 Million) Were Stolen' 23 September 2015 *NBC News* (online) <https://www.nbcnews.com/tech/security/opm-5-6-million-fingerprints-not-1-1-million-were-n432281>.

[117] Bkav Corporation, *Bkav's new mask beats Face ID in "twin way": Severity level raised, do not use Face ID in business transactions* (27 November 2017) <http://www.bkav.com/dt/top-news/-/view_content/content/103968/bkav﷯s-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions>.

[118] Bkav Corporation, *Bkav's New Mask Beats Face ID in "Twin Way": Do not Use Face ID in Business Transactions* (26 November 2017) YouTube <https://youtu.be/rhiSBc061JU>.

50,000 probability with the iPhone's fingerprint scanner.[119] Moreover, Face ID allows for five attempts before prompting a user to enter their passcode. Apple has also commented that '*the odds of guessing a typical 4-digit passcode are 1 in 10,000*' and less complex passcodes such as '1234' are more easily guessed.[120]

Another hack by the German hacking group, Chaos Computer Club, saw them penetrate the Samsung Galaxy 8 iris scanner.[121] They did this by using a point-and-shoot camera, laser printer and contact lens. Their hack begins with simply taking a close range (about five metres) photograph of their target and printing the zoomed in image of the eye on a laser printer and then placing a normal contact lens on top of the print so that it would curve, just like a human eyeball. This unlocked the Samsung Galaxy 8. Similarly, at an annual Chaos Computer Club conference in Germany, a biometrics specialist, Jan Krissler, demonstrated how he could spoof iris recognition, by using extracted iris data of the German chancellor, Angela Merkel.[122] Krissler simply used an image of Merkel taken at a press conference, but noted that a high-resolution billboard and/or magazine image could also be used, and explained that iris recognition could be spoofed by using any of the former printed onto a contact lens. All that was needed was a photo editing software, such as Photoshop, which Krissler used to enhance the contrast of the image of Merkel and printed the image of Merkel's iris using a laser printer.

---

[119] Mai Nguyen, 'Vietnamese researcher shows iPhone X face ID 'hack'', *Reuters* (online), 15 November 2017 <https://www.reuters.com/article/us-apple-vietnam-hack/vietnamese-researcher-shows-iphone-x-face-id-hack-idUSKBN1DE1TH>; Apple, above n 36.
[120] Apple, above n 36.
[121] Chris Ip, 'The Galaxy S8 Iris Scanner Can be Hacked With Aging Tech', *Engadget* (online), 23 May 2017 <https://www.engadget.com/2017/05/23/galaxy-s8-iris-scanner-hacked/>.
[122] Roi Perez, 'Starbug's in your eyes: German hacker spoofs iris recognition', *SC Magazine UK* (online), 26 October 2015 <https://www.scmagazineuk.com/starbugs-in-your-eyes-german-hacker-spoofs-iris-recognition/article/535281/>.

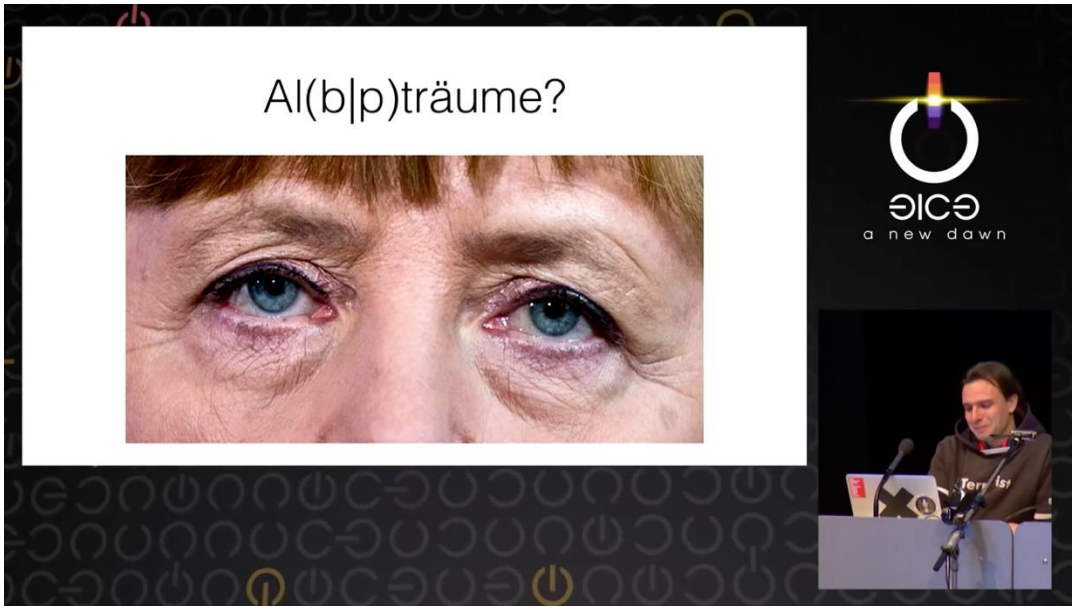


Figure 6: Screenshot from a YouTube video that shows the zoomed in image of the German Chancellor, Angela Merkel's, eyes, taken from five metres away that Krissler was able to exploit.[123]

In addition, Krissler explained that a fake fingerprint that could be used to spoof fingerprint sensors such as Apple's Touch ID sensor was possible to create by using a fingerprint from a print scanner and then making a mould of the fingerprint.[124] Fingerprints could also be spoofed using photographs of fingerprints, which was how Dr Von Der Leyen, the German defence minister's, thumbprint was extracted. Japanese researchers have also suggested that fingerprints can be copied when looking at photos taken in strong lighting and from a distance of three metres.[125] The researchers also '*created a transparent titanium oxide film which will mask prints within photographs, yet permit validation with biometric scanners now woven into many mobile devices*' by trawling images of people doing the two-fingered peace sign and then zooming in and gaining access to the victim's fingerprints. In addition, smartphone fingerprint sensors can also become compromised through the creation of a copy of the original fingerprints made out of materials that are designed to mimic human skin.[126] As well, research conducted by New York University and Michigan State University

---

[123] Media.ccc.de, *starbug: Ich sehe, also bin ich ... Du (english translation)* (29 December 2014) YouTube <https://youtu.be/VVxL9ymiyAU>.
[124] Ibid.
[125] Darren Pauli, 'Peace-sign selfie fools menaced by fingerprint-harvesting tech', *The Register* (online), 12 January 2017 <https://www.theregister.co.uk/2017/01/12/fingerprint_photographs/>.
[126] Paul and Irvine, IEDs on the Road to Fingerprint Authentication: Biometrics have vulnerabilities that PINs and passwords don't, above n 83.

researchers showed that fingerprint scanners are subject to compromise because they are able to be bypassed by 'master prints' – or fingerprints that are able to match different fingerprint patterns – and allow access to seemingly secure systems with a 65 per cent success rate.[127] However, it is worth noting that the researchers achieved this success rate by testing the master prints in a computer simulation as opposed to testing the prints on actual smartphones. Further, it was revealed that Android's Pattern Lock system was able to be compromised, but only through a method of recording the Android smartphone owner unlocking their device and then being analysed by advanced computer vision algorithm software.[128]

Paul and Irvine provide a further example of how an individual can access another user's account without having to go through the process of creating a fake physical fingerprint:

> '*a fingerprint sensor within a computer system is typically designed to convey a measurement of an individual's raw fingerprint to another component of the computer system that is responsible for either deriving a cryptographic key or unlocking an existing cryptographic key held securely on the device. Therefore, by identifying the input format expected by the key storage or computation module, it is possible to present a falsified (or previously captured) fingerprint reading "on the wire," thus bypassing the need to create a fake physical fingerprint*'.[129]

Similarly, in an interview with the CEO of the NSW Data Analytics Centre, Ian Oppermann, he said, '*if someone has your fingerprints, if someone has your behaviours, if someone knows this is what you're like at this time of the day…Someone could quite literally come in and be you as far as the system is concerned and pass every single test*'.[130]

---

[127] Brett Williams, 'Study suggests your phone's fingerprint scanner is easily fooled', *Mashable Australia* (online), 12 April 2017 <https://mashable.com/2017/04/11/smartphone-fingerprint-scanner-vulnerability/ - kPZdzR2uyiq1>; Aditi Roy, Nasir Memon, and Arun Ross, 'MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems' (2017) 12(9) *IEEE Transactions on Information Forensics and Security* 2013, 2013 <http://ieeexplore.ieee.org/document/7893784/>.

[128] Brett Williams, 'Thieves might be able to break into your Android phone — if they're very, very determined', *Mashable Australia* (online), 24 January 2017 <https://mashable.com/2017/01/23/android-pattern-lock-hack-report/ - 5ZPVIpvirmqG>.

[129] Paul and Irvine, Fingerprint Authentication is here, but are we ready for what it brings?, above n 72, 3.

[130] Interview with Ian Oppermann, CEO of the NSW Data Analytics Centre (telephone, 14 February 2018).

On a slightly more technical level, one of the vulnerabilities in the use of fingerprints to access smartphones is that they are prone to a 'Confused Authorisation Attack'.[131] Indeed, Zhang et al notes that '*authorization grants access rights to resources, while authentication verifies who you are*'. The issue is that the '*security systems often mistakenly treat authorization as authentication, or fail to provide context proof for the authorization objects*' and '*without proper context proof, the attacker can mislead the victim to authorize a malicious transaction by disguising it as an authentication or another transaction*'. An example provided by Zhang et al is the imitation of a lock screen on a smartphone that can trick the victim into thinking that they are unlocking their device with their fingerprint, when in reality, the attacker could be using their fingerprint to authorise a nefarious monetary transaction in the background.

Another vulnerability discovered was that fingerprints were not being stored securely in smartphones.[132] In a 2015 report, Zhang et al explained that at the time their report was being published, '*some vendors claimed that they store users' fingerprints encrypted in a system partition, [but] they put users' fingerprints in plaintext and in a world-readable place by mistake*', meaning it was not stored as securely as intended. An example is the HTC One Max, where users' fingerprints were saved as world-readable. This means that '*any unprivileged processes or apps can steal users' fingerprints by reading this file*'. Zhang et al reported that '*other vendors store fingerprints in TrustZone or Secure Enclave, but that there are still known vulnerabilities or attacks to leverage to peek into the secret world*'. Zhang et al further explained:

> '*to make the situation even worse, each time the fingerprint sensor is used for auth operation, the auth framework will refresh that fingerprint bitmap to reflect the latest wiped finger. So the attacker can sit in the background and collect the fingerprint image of every swipe of the victim*'.[133]

According to Zhang et al:

> '*instead of directly communicating with the fingerprint sensor, all the normal world components are supposed to invoke the TrustZone fingerprint for sensor operations. However, most vendors fail to lock down the sensor (from being accessed by the normal world programs) when the processor switched back*

---

[131] Yulong Zhang, Zhaofeng Chen, Hui Xue, and Tao Wei FireEye Labs, 'Fingerprints On Mobile Devices: Abusing and Leaking' (2015) *Blackhat Conference* 4 <https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf>.
[132] Ibid 5.
[133] Ibid.

> *from the secure world. Without the proper lock-down, the attacker from normal world can directly read the fingerprint sensor*'.[134]

Hackers are usually able to do this in the background and are able to do so without the smartphone owner's knowledge usually, meaning that the hacker can continue reading the fingerprints every time the victim touches their smartphone. Moreover, this shows '*that attackers with remote code execution exploits can remotely harvest everyone's fingerprints on a large scale, without being noticed*'. Zhang et al further explained that:

> '*the attackers can stealthily embed prefabricated fingerprints in the devices as an authorization backdoor, before providing a new device to the victim. The root cause of this vulnerability is that the UI displaying the number of registered fingerprints is a separate component (in the normal world, without TrustZone's protection) from the actual fingerprint auth framework in the secure world. Attackers can deceive the user to believe that there are only N fingerprints registered on the device but there are actually more than N. Such extra pre-embedded fingerprints can be used to bypass the auth framework like a backdoor. It is usually the Settings app that displays the registered fingerprint number to the users, so the attacker needs to modify the Settings app*'.[135]

Another example of how a biometrics system can be hacked is provided by Ungureanu and Costache who argue that to actually attempt to hack a biometrics system, a hacker would need '*to generate (or acquire) a large number of samples of the biometric (for example, fingerprints)*'.[136] Yet they noted that this is more difficult than launching a brute force attack – meaning that it is more difficult than using a trial-and-error method of attempting to enter into a system or user account by entering in PINs, passwords and passphrases generated in a large pool. In saying so, Ungureanu and Costache argue that '*it is by no means impractical*' to do so.

Biometrics Can Be Hacked…Now What?

Having established some of the ways that consumers' smartphone biometrics can be compromised, it is worth considering how to prevent such compromises, or cyber attacks. Zhang et al recommended that at the time their report was published in 2015, that '*to avoid being attacked by malware or being exploited for remote code execution,*

---

[134] Ibid 7.
[135] Ibid 8-9.
[136] Adrian S Ungureanu and Claudia Costache, 'Palm Print as a Smartphone Biometric: Another option for digital privacy and security' (2016) 5(3) *IEEE Consumer Electronics Magazine* 71, 72 <http://ieeexplore.ieee.org/document/7539264/?reload=true>.

we suggest normal users to choose mobile device vendors with timely patching/upgrading to the latest version, and always keep your device up to date'.[137] As well, it is recommended that applications should only be installed from legitimate sources. In e-mail correspondence with Stephen Clarke from Jebel Consultant Group, he advised that for consumers to ensure their smartphone biometrics remain in their control, they should not let '*a raw biometric sample leave the phone (e.g. the picture of the face). As soon as a biometric sample leaves the phone the consumer has lost control of it*'.[138]

As for enterprises and governments, Zhang et al recommended that they '*should seek professional services to get protections against advanced targeted attacks*'.[139] Whereas, mobile device vendors '*should improve the security design of the fingerprint auth framework with improved recognition algorithm against fake fingerprint attacks, and better protection of both fingerprint data and the scanning sensor*'. Further, '*vendors should figure out how to differentiate authorization with authentication and provide context proof*'. As well, '*the existing fingerprint auth standard should be further improved to provide more detailed and secured guidelines for developers to follow*'.

The ACSC in their *Cyber Security Survey 2016* argued that to effectively manage any potential attacks against systems, businesses need to be cyber resilient, as they argue that '*cyber resilience is a whole-of-business concern*'.[140] The ACSC defines cyber resilience as '*an organisation's ability to prepare for, withstand and recover from cyber threats and incidents*'. Indeed, it appears that companies are motivated to protect information, as results from the organisations that were surveyed for the ACSC *2016 Cyber Security Survey* indicated that the primary motivation for investing in cyber security was to protect company owned data (76 per cent) and to protect customer information (73 per cent).[141] However, this concern could be attributed to the legal obligations that most organisations have to protect customer PII.[142] Nevertheless, it is clear that dealing with cyber threats is a priority in Australia and this is important to note when examining the implications of the use of smartphone biometrics, because it can assist Australian consumers in better understanding the cybersecurity landscape their smartphone biometrics are operating in.

---

[137] Zhang et al, above n 131, 9.
[138] Interview with Stephen Clarke, Jebel Consultant Group (email, 22 February 2018).
[139] Zhang et al, above n 131, 9.
[140] Australian Government, ACSC, *2016 Cyber Security Survey*, above n 106.
[141] Ibid 17.
[142] Ibid.

Legal: Consumer Privacy and Consent

Privacy under Australian Law

Australia currently does not have any legislation specifically related to the use of smartphone biometrics. Under Australian legislation, it is only privacy, data breaches, biometrics generally, and unauthorised computer access that is addressed. The relevant legislation includes the *Privacy Act 1988* (Cth), *Criminal Code Act 1995* (Cth), *Migration Legislation Amendment (Identification and Authentication) Act 2004* (Cth), *Australian Passports Act 2005* (Cth), *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* (Cth), *Migration Amendment (Strengthening Biometrics Integrity) Act 2015* (Cth), Identity-matching Services Bill 2018 (Cth), and the Australian Passports Amendment (Identity-matching Services) Bill 2018 (Cth).

Privacy Act 1988 (Cth)

When Australia's *Privacy Act* was created, legislators were influenced by Australia's obligations under the *International Covenant on Civil and Political Rights*[143] and Article 17 states that:

1. '*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation*.
2. *Everyone has the right to protection of the law against such interference or attacks*'.[144]

The *Privacy Act* aims '*to promote the protection of the privacy of individuals*'.[145] Although, the Act accounts for the balancing act between protecting individual privacy and that of the interest of entities in performing their functions and activities.[146] Listed under Schedule 1 of the *Privacy Act* are the 13 Australian Privacy Principles ('APPs'), which work to govern how most Australian government agencies, private sector and non-profit agencies with an annual turnover of more than $3 million, all private health

[143] Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments And Approaches To Oversight' (2017) 40(1) *University of New South Wales Law Journal* (Advance) 1, 11 <http://unswlawjournal.unsw.edu.au/sites/default/files/04-mannsmith-advance-access-final.pdf>.
[144] United Nations Human Rights, *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, (entered into force 23 March 1976) <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.
[145] Mann and Smith, above n 143, 12; *Privacy Act 1988* (Cth) s 2A(a).
[146] Ibid; *Privacy Act* s 2A(b).

service provides, and some small businesses are to handle personal information. The *Privacy Act* applies to incorporated businesses in Australia, but it also applies to businesses operating out of Australia, provided if they are collecting personal information from, or store personal information in, Australia and conduct their business in Australia.[147]

Why the Privacy Act is Important

Given the developments being made in the biometrics space, the *Privacy Act* is important to consider, as the Act addresses the management of PII, such as biometrics. Under Schedule 1 of the Act, the 13 APPs are listed. The APPs create obligations on some government agencies, private sector and non-profit agencies with regard to how they handle personal information. Under the *Privacy Act*, there is reference to biometrics, as the Act defines sensitive information as including '*biometric information that is to be used for the purposes of automated biometric verification or biometric identification*' as well as '*biometric templates*'.[148]

Biometric technologies are by default invasive because not only do they identify individuals, but they can link them to other datasets, sometimes without their fully informed consent.[149] Sensitive information on concerned individuals must only be collected if the relevant individual has consented,[150] except if the entity collecting the information '*is an enforcement body*' and there is a reasonable belief that '*the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities*'.[151] In addition, entities are not permitted to use and share information collected for a particular purpose for a secondary purpose, unless the concerned individual has consented.[152] Although, if '*the use or disclosure of the information is reasonably necessary for one or more enforcement related activities*', then the consent of the concerned individual will not be needed.[153]

These exemptions under the *Privacy Act* are important to highlight because if any agency has any enforcement functions, they do not need the consent of the individual concerned, nor a warrant or court order to gather and store photographs in the creation

---

[147] *Privacy Act* s 5B.
[148] s 6(1)(d)-(e).
[149] Mann and Smith, above n 143.
[150] *Privacy Act* sch 1 cl 3.3(a).
[151] Ibid sch 1 cl 6.1.
[152] Ibid sch 1 cl 6.1 (APP 6).
[153] Ibid sch 1 cl 6.2(e).

of facial templates, which are shared with other agencies.[154] Mann and Smith have criticised the broad reach of these exemptions, arguing that this can then lead to the compromise of individual rights under the auspices of arguing it is for the benefit of the greater community.[155] This is a strong argument, given the lack of constitutional protection of Australians' rights to privacy. Mann and Smith have warned about the potential for '*function creep*', which they argue occurs:

> '*Where the use of information taken for a particular purpose is used for other purposes for which consent was not obtained…This concept appears relevant to the development of the NFBMC as a national 'hub' of facial templates. This may be an example of function creep because individuals consented to providing a photograph to obtain a passport, yet did not consent to their biometric information being extracted from that image and being used for law enforcement, security or intelligence purposes*'.[156]

Mann and Smith have recommended that in Australia, there be an official officer '*with statutory responsibilities in relation to the oversight of the collection, retention and use of biometric information*'.[157] As well, they recommended that there be '*a strong, independent and sufficiently funded regulatory authority…to meet challenges posed by new technologies, rapid information sharing and the ease of identification provided by biometrics*'. Indeed, it is increasingly important to intensively regulate the use of biometric information in Australia, due to the increasing use of biometric information by law enforcement and security agencies. An example of regulating the use of biometric information could be the creation of a code of conduct that governs the use of biometric information and enables self-regulation. The use of biometric information could also be governed by ensuring there is enough public education and engagement, in order to enable Australians to have a role in understanding and dealing with how their biometric information is being used.[158]

Criminal Code Act 1995 (Cth)

As for the unauthorised access to, or modification of, restricted data, the *Criminal Code Act 1995* regulates this.[159] The maximum penalty for committing such an offence is two years imprisonment. Another offence includes the unauthorised impairment of

---

[154] Mann and Smith, above n 143, 12.
[155] Ibid 13.
[156] Ibid.
[157] Mann and Smith, above n 143, 24.
[158] Ibid.
[159] s 478.1(1).

electronic communication, which falls under s 477.3(1) of the *Criminal Code* and carries a maximum penalty of 10 years imprisonment.

Migration Legislation Amendment (Identification and Authentication) Act 2004 (Cth)

The *Migration Legislation Amendment (Identification and Authentication) Act 2004* permits the collection of personal identifiers (including biometrics) from non-citizens during the visa application process and while entering the country during clearance.[160]

Australian Passports Act 2005 (Cth)

The *Australian Passports Act 2005* introduced the use of biometric passports. The Act enables the Minister for Foreign Affairs to:

> '*specify methods (including technologies) that are to be used:*
>
> a) *for the purposes of confirming the validity of evidence of the identity of an applicant for an Australian travel document or a person to whom an Australian travel document has been issued; or*
>
> b) *for performing other functions in connection with this Act*'.[161]

Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014 (Cth)

A few years later, the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* was introduced. The amendment '*extended the collection of personal identifiers to Australian citizens entering or leaving the country*'.[162] As a result, one of the personal identifiers able to be collected under the Act included biometric information collected by a SmartGate.

Migration Amendment (Strengthening Biometrics Integrity) Act 2015 (Cth)

The *Migration Amendment (Strengthening Biometrics Integrity) Act 2015* '*consolidated seven previous provisions into a broad, discretionary power to collect one or more*

---

[160] Mann and Smith, above n 143, 10.
[161] s 47(1)(a).
[162] Mann and Smith, above n 143, 10.

personal identifiers from both non-citizens and citizens'.[163] Personal identifiers include biometrics.

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)

Since 22 February 2018, the *Privacy Amendment (Notifiable Data Breaches) Act 2017* has been in effect. This Amendment requires that all organisations and government agencies that are securing personal information as per the *Privacy Act* must notify individuals if the unauthorised access to, unauthorised disclosure of, or loss of their personal information, or data, is likely to cause serious harm and if they have '*reasonable grounds to believe that an eligible data breach has happened*' or if they are directed to do so by the Commissioner.[164]

Identity-matching Services Bill 2018 (Cth)

The Identity-matching Services Bill 2018 was recently introduced in early February 2018 in Parliament by the Department of Home Affairs Minister, Peter Dutton, and it is a Bill that seeks to legally encompass the Council of Australian Governments ('COAG') signed last October 2017. The Bill seeks to make the existing process of identifying an unknown person much simpler for law enforcement agencies by enabling real time identity-matching services. As per the Bill, there will be five national facial recognition/identity-matching services available for use by the Department of Home Affairs. The two systems are the:

- National Driver Licence Facial Recognition Solution (NDLRD), which will contain two systems within it:
    - A system which holds identifying information; and
    - A system that enables biometric facial recognition comparisons.
- The interoperability hub, which will not store any personal information, but will transfer queries to the appropriate database that will make the identification, or matching, possible.

[163] Ibid.
[164] *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) s 26WA.

Australian Passport Amendment (Identity-matching Services) Bill 2018 (Cth)

Another Bill recently introduced is the Australian Passports Amendment (Identity-matching Services) Bill 2018. This Bill seeks to ensure that all the relevant travel documents and data is available for the Minister for the purpose of identity-matching services as signed at the COAG in October 2017.

European Union General Data Protection Regulation (GDPR)

The *GDPR* '*contains new data protection requirements that will apply from 25 May 2018*'.[165] These requirements will '*harmonise data protection laws across the EU and replace existing national data protection rules*'. The *GDPR* will apply '*to the data processing activities of businesses…that are data processors or controllers with an establishment in the EU*'. The *GDPR* will also apply '*to the data processing activities of processors and controllers outside the EU…where the processing activities are related to*:

- *offering goods or services to individuals in the EU (irrespective of whether a payment is required); and*
- *monitoring the behaviour of individuals in the EU, where that behaviour takes place in the EU (Article 3)*'.[166]

This is relevant to Australians, as it means that '*some Australian businesses covered by the Privacy Act, may need to comply with the GDPR if they*:

- *have an establishment in the EU (regardless of whether they process personal data in the EU); or*
- *do not have an establishment in the EU, but offer goods and services or monitor the behaviour of individuals in the EU*'.[167]

This signals a privacy-centric approach and it ensures that data breach notification procedures are complied with under the *GDPR* and *Privacy Act*.[168]

---

[165] Australian Government, Office of the Australian Information Commissioner (OAIC), *Australian businesses and the EU General Data Protection Regulation* (January 2018) Privacy Business Resource 21, 1, 2 <https://www.oaic.gov.au/resources/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation.pdf>.
[166] Ibid 3.
[167] Ibid 2.

The OAIC states that, '*Australian businesses with customers in the EU, or that operate in the EU, should confirm whether they are covered by the GDPR, and if so, take steps to ensure compliance by May 2018*'.[169]

The *GDPR* is similar to the *Privacy Act* in that it applies to personal data in *GDPR* terms, or personal information in *Privacy Act* terms. Similarly, there are special protections in both the *GDPR* and *Privacy Act* regarding the processing of personal data in relation to an individuals' race, ethnicity, political opinions, religious views, membership in trade unions, genetic data, biometric data for identification purposes, health care data, and sex life or sexual orientation.[170] Similarly to the *Privacy Act*, specifically APP 1.2, the *GDPR* seeks to ensure accountability and governance, by ensuring that privacy is the default for controllers, meaning that impact assessments should be made and data protection officers should be appointed.[171]

Consent is another topic that is relevant to the *GDPR* as well as the *Privacy Act*, as the *GDPR* highlights that consent must be freely given, specific and informed, and unambiguously indicated by the individual concerned.[172] This is similar to the *Privacy Act*, as the individual concerned must also be adequately informed and have the capacity to consent prior to consenting as well as be able to give their consent voluntarily and specifically. What is interesting to note with the *GDPR* is that the individual has more rights than they do under the *Privacy Act* – under the *GDPR*, individuals have rights such as a right to have the personal information erased (Art 17), right to data portability (Art 20) and a right to object (Art 21). Whereas under the *Privacy Act*, the only protection that individuals have is that businesses are to take reasonable actions to erase or de-identify personal information that is no longer needed (APP 11.2). The *GDPR* places rules on the transfer of personal data outside the EU, noting that personal data may be transferred outside the EU in certain circumstances such as to countries that have an adequate level of data protection, to countries that have standard data protection clauses or binding corporate rules, and if there are approved codes of conduct or certification in place.[173] As for the *Privacy Act*, if a business is looking to share personal information outside of Australia, the business

---

[168] Ibid.
[169] Ibid 3.
[170] European Parliament & Council, General Data Protection Regulation ('GDPR') (to be entered into force 25 May 2018) art 9; *Privacy Act* s 6(1); APP 3.3, 6.2(a), and 7.4.
[171] GDPR arts 5, 24, 25, 35, and 37.
[172] Ibid art 4(11).
[173] Ibid ch V.

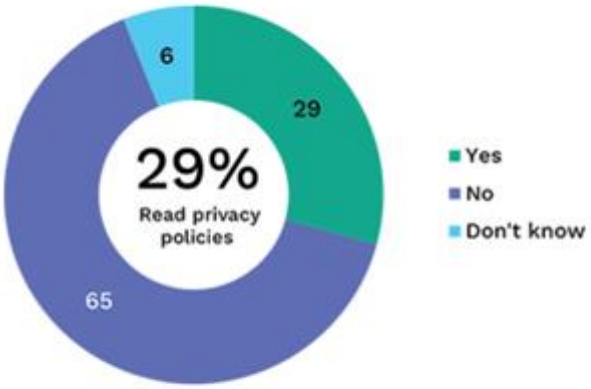
must take reasonable steps to ensure that the recipient of the personal information does not breach the APPs regarding the personal information (APP 8).

Storing and Sharing of Biometric Data

The Australian Law Reform Commission has suggested that with the wider use of biometric systems, it could lead to extensive surveillance of innocent individuals.[174] This concern is even greater when biometrics are used in a multitude of contexts to identify individuals, especially if consumers are unaware of the widespread use of their biometrics and have not consented to their biometrics being accessed and used widely.[175]

Australians have reported having high levels of concern over their online privacy (69 per cent), yet the percentage of Australians reading privacy policies on the websites they visit has declined, dropping from 44 per cent in 2013 to 29 per cent in 2017.[176]

Figure 34. Reading privacy policies



Q30: Do you normally read the privacy policy attached to any internet site?
Base: All respondents in streams 2 and 3 (n=1213)

[174] Australian Government, Australian Law Reform Commission, *For your Information: Australian Privacy law and Practice*, Report No 108 (2008) Ch 9 Overview: Impact of Developing Technology on Privacy: Biometrics <https://www.alrc.gov.au/publications/9. Overview%3A Impact of Developing Technology on Privacy/biometric-systems>.
[175] Ibid.
[176] Australian Government, OAIC, *Australian Community Attitudes to Privacy Survey (ACAPS) 2017* <https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017>.

Figure 7: Infographic taken from OAIC website that shows how many respondents read privacy policies on internet sites.[177]

Out of this group that said they read privacy policies, 45 per cent reported fearing becoming a victim of identity fraud and 39 per cent stated that they had been a victim of identity fraud or had known someone that had been a victim of identity fraud.[178] As well, 68 per cent of Australians reported being uncomfortable with search engines and social media sites storing their online behaviour on their databases and storing information about them. Moreover, respondents reported that these five areas were the biggest privacy risks for Australians:

- Online services and social media sites (32%)
- Identity theft and fraud (19%)
- Security of their data/data breaches (17%)
- Financial details/information/fraud (12%)
- Personal information being easily available and not secure (7%).

One of the implications of the use of biometric data in smartphones is that the collection of biometric data can often begin with the initial ideas of improving costs, efficiency and security, but result in uncertainty regarding what governments, organisations and companies are doing with consumer biometric data.[179] In an interview with Frank Zeichner, the CEO of the Internet of Things Alliance Australia, he said that '*it's less about the devices, more about the data and how that data is shared and stored*'.[180] Recently, there was a court case regarding facial recognition software, with users suing Facebook '*for violating their privacy by identifying and tagging them in photos without their consent*'.[181] What follows is that individuals' biometric data may be clandestinely collected without their knowledge and used without their consent.[182] Indeed, facial recognition technology is able to be utilised in public spaces without consumers even knowing, since the human face is able to be captured relatively seamlessly and secretly. As a result, the widespread use of tools such as facial recognition technology in public spaces would make it impossible for consumers to go

[177] Ibid.
[178] Ibid.
[179] Phang and Pavlovski, above n 82, 38; Christopher Zara, 'Facebook Keeps Getting Sued Over Face-Recognition Software, And Privacy Groups Say We Should Be Paying More Attention', *International Business Times* (online), 3 September 2015 <http://www.ibtimes.com/facebook-keeps-getting-sued-over-face-recognition-software-privacy-groups-say-we-2082166>.
[180] Interview with Frank Zeichner, CEO of Internet of Things Alliance Australia (IoTAA) (telephone, 15 February 2018).
[181] Phang and Pavlovski, above n 82, 38.
[182] Ibid.

about their day privately.[183] Furthermore, it is not just in the physical public domain that biometric data is able to be captured, but also the cyber domain.[184] Indeed, social media makes it easy to download images, videos and audio from a person's social media webpage. This can result in '*unintentional censorship, control and inhibition of our actions and the emotional harm of constant monitoring*'.[185] Clarke argues that '*biometrics undermines the privacy of personal behaviour, to the point that freedom of speech and thought are threatened - and the chilling effect on behaviour arises whether or not the system works, and whether or not the behaviour is of a kind that the system designer is intending to chill*'.[186]

Along with unwarranted monitoring, biometrics can reveal other sensitive, personal information about consumers.[187] Nakar and Greenbaum suggest that such information can include '*easily discriminable characteristics such as age, race or gender, social status, religion and even immigration status*'.[188] Indeed, an issue to consider is whether the biometric capturing device or reader can be trusted to not store or share any of the biometrics on and with any other unauthorised parties.[189]

There are companies dedicated to collecting user personal data and some of these companies are not always totally secure, as reports of security breaches demonstrate this.[190] An example of this is the data analytics company, Alteryx, when a security flaw they said was discovered by an analyst from a security company called Upguard exposed the personal information of 123 million US households in December 2017.[191] In addition, Upguard announced another hack reported in September 2017 by the company Equifax.[192] The US company Equifax announced that the personal information of approximately 143 million customers had been compromised through a

---

[183] Sharon Nakar and Dov Greenbaum, 'Now You See Me, Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy' (2017) 23(1) *Boston University Journal of Science & Technology Law* 88, 92 <https://www.bu.edu/jostl/files/2017/04/Greenbaum-Online.pdf>.
[184] Phang and Pavlovski, above n 82.
[185] Nakar and Greenbaum, above n 183, 92-3.
[186] Roger Clarke, 'Biometrics as 'RegTech'?' (Working Version, 23 August 2017) <http://www.rogerclarke.com/ID/BiomRegI.html>.
[187] Ibid.
[188] Nakar and Greenbaum, above n 183, 120.
[189] Paul and Irvine, Fingerprint Authentication is here, but are we ready for what it brings?, above n 72, 6.
[190] Hayley Tsukayama, 'Companies you've never heard of are exposing your personal data', *The Washington Post* (online), 22 December 2017 <http://dpo.st/2zjJm46>.
[191] Ibid.
[192] Ibid.

cyber attack.[193] The ACSC reported that '*information accessed included name, social security numbers, birth dates, addresses and in some instances, drivers licence details – more than enough to facilitate identity theft activities*'. Additionally, Upguard also discovered that in early 2017, the data firm, Deep Root, which was hired by US Republican candidates, suffered a security flaw that resulted in 198 million individuals information exposed.[194] Moreover, a larger company, Axciom, reported a breach of 1.6 billion customer records in 2005. The breaches have been attributed to the increase in data collection, which is occurring at such a rapid pace, while security lags behind.[195] This should be a cautionary example of the dangers of collecting and storing biometric data, particularly if it is stored in a centralised location.

Another technological advancement may potentially see consumer biometric data used to track users on their smartphones when accessing the internet, similar to the tracking capabilities of cookies. This is something that should be considered before the use of smartphone biometrics becomes more widespread.[196] Moreover, by using biometric data to track internet users, it would aid in preventing attempts to limit tracking, such as clearing cookies, and as such be of value not just to advertisers but cybercriminals.[197] In an interview conducted with Dr Katina Michael, she said '*it's almost like we've been sold the message that resistance is futile, but the thing is it's not futile…consumers somehow have lost their ability to voice and lobby their concerns and I think what happened is because they've become productised*'.[198]

[193] Australian Government, ACSC*, 2017 Threat Report*, above n 107.
[194] Tsukayama, above n 190.
[195] Ibid.
[196] Paul and Irvine, Fingerprint Authentication is here, but are we ready for what it brings?, above n 72, 4.
[197] Ibid.
[198] Interview with Dr Katina Michael, board member of the Australian Privacy Foundation (telephone, 9 February 2018).

Current Uses of Biometrics in Australia

Australia's ePassport and SmartGates

Since 2007, ePassports have been able to be used with Australia's SmartGates, which are available at eight of Australia's international airports.[199] These passports contain an embedded microchip, which contains data such as a digitised photo of the passport holder's face.[200] The way ePassports work is that '*a special code is used to write data to the microchip, the chip is protected by a secure electronic "key", and an additional access code guards against electronic eavesdropping or "skimming" of information on the microchip*'.[201]

Figure 8: Australian ePassport.[202]

Those holding ePassports and aged 16 years or over[203] can use Australia's SmartGates on arrival. Australia's SmartGates essentially work to speed up the usual

[199] Australian Government, Department of Home Affairs, *Arrivals SmartGate* <https://www.homeaffairs.gov.au/trav/ente/goin/arrival/smartgateor-epassport>.
[200] Australian Government, Department of Foreign Affairs and Trade, 'Australia Launches ePassports' (Media Release, 25 October 2005) archived material <https://foreignminister.gov.au/releases/2005/fa132_05.html>.
[201] Ibid.
[202] Australian Government, Department of Home Affairs, *Arrivals SmartGate* <https://www.homeaffairs.gov.au/trav/ente/goin/arrival/smartgateor-epassport>.

customs and immigration processes, while using facial recognition to identify those visiting or returning to Australia.

Figure 9: SmartGate.[204]

The personal information and facial photograph which is collected upon arrival to Australia when using the SmartGate is regularly disclosed, as per the *Australian Border Force Act 2015* (Cth).[205] This means this information is shared with the:

- Australian Federal Police
- Attorney-General's Department
- Australian Crime Commission
- Department of Agriculture
- Department of the Environment
- Australian Transactions Reports and Analysis Centre
- Department of Foreign Affairs and Trade
- Director of Public Prosecutions
- State and Territory Police forces

---

[203] Or an Australian child aged 10 to 15 years of age (inclusive) if accompanied by at least two adults, Australian Government, Department of Home Affairs, *Arrivals SmartGate* <https://www.homeaffairs.gov.au/trav/ente/goin/arrival/smartgateor-epassport>.
[204] Ibid.
[205] Ibid.

- Overseas customs and immigration authorities.

The Australian Department of Home Affairs website outlines that the '*records of a passenger's personal information are retained until they are disposed of according to the latest Disposal Authority approved by the National Archives of Australia under the Archives Act 1983*'.[206] In addition, the Department of Home Affairs, which includes the Australian Border Force, has a legal obligation to be compliant with Part 6 of the *Australian Border Force Act 2015* when revealing any personal information that has been collected through the arrivals SmartGate. As per the provisions under Part 6, entrusted persons are obliged to ensure that any personal information that is disclosed be for legitimate purposes where disclosure is allowable. Nonetheless, the Department of Home Affairs must comply with the APPs regarding collecting, using and disclosing personal information.[207]

At the time of writing this report, it was reported that in May 2018, Sydney Airport will be trialling a new system where a traveller's face will be their passport and boarding pass.[208]

National Facial Biometric Matching Capability

At a special meeting of the COAG on counter-terrorism in October 2017, leaders arranged to launch a National Facial Biometric Matching Capability ('NFBMC') and signed an Intergovernmental Agreement on Identity Matching Services.[209] The aim behind this move was '*to protect Australians by making it easier for security and law enforcement agencies to identify people who are suspects or victims of terrorist or other criminal activity, and prevent the use of fake or stolen identities — which is a key enabler of terrorism and other serious crime*'. As a result of the Intergovernmental Agreement, '*agencies in all jurisdictions will be able to use new face matching services to access passport, visa, citizenship and driver licence images – while maintaining robust privacy safeguards*'.[210] More recently, it was announced that Australian drivers'

---

[206] Ibid.
[207] Ibid.
[208] Matt O'Sullivan, 'Sydney Airport biometric trial for Qantas flights: No passport required', *The Traveller* (online), 22 February 2018 <http://www.traveller.com.au/sydney-airport-biometric-trial-for-qantas-flights-no-passport-required-h0wgzn>.
[209] Council of Australian Governments (COAG), Special Meeting of the Council of Australian Governments on Counter-Terrorism Communiqué (Canberra, Australia, 5 October 2017) 1 <http://bit.ly/2DeacOt>.
[210] Ibid.

licences will be a new addition to the Commonwealth Government's biometric database.[211] The ABC reported, '*a system known as "the Interoperability Hub" is already in place in Australia, allowing agencies to take an image from CCTV and other media and run it against a national database of passport pictures of Australian citizens — a system known as "The Capability"*'.[212] Australian drivers' licences will now be added to this system, which means that government and private bodies will be able to access an Australian driver's licence photo, age and address. With this addition, there are concerns over individuals having their biometric identity used for commercial purposes and by organised crime groups seeking to capture as much biometric data on individuals as possible. As well, it could be used to wrongly link innocent individuals to criminal investigations.

The Australian Government Attorney-General's Department Fact Sheet on Face Matching Services distinguishes between the Face Verification Service ('FVS') and the Face Identification Service ('FIS').[213] The FVS is a '*is a one-to-one image based verification service that can match a person's photo against an image on one of their government records, such as a passport photo, to help verify their identity. Often these transactions will occur with the individual's consent*'. Whereas the FIS '*is a one-to-many image based identification service that can match a photo of an unknown person against multiple government records to help establish their identity. Access to the FIS will be restricted to agencies with law enforcement or national security related functions*'.

The Australian Government has argued that its investing in this system will assist in combatting identity crime, which they note is '*one of the most common crimes in Australia and costs around $2.2 billion per year*', with approximately 1 in 20 Australians falling victim to identity crime that leads to financial loss per year.[214] Moreover, it is not just identity crime that is the issue, but the fact the stolen identities are then used to facilitate other crimes such as terrorism, drug trafficking, human trafficking, child exploitation and money laundering.[215]

---

[211] Rebecca Trigger, 'Experts sound alarm as biometric data from drivers' licences added to government database', *ABC news* (online), 16 January 2018 <http://www.abc.net.au/news/2018-01-15/alarm-raised-as-drivers-licences-added-to-government-database/9015484>.
[212] Ibid.
[213] Australian Government, Attorney-General's Department, *Face Matching Services, Fact Sheet – Face Matching Services*, above n 63, 1.
[214] Ibid 2.
[215] Ibid.

The sharing of facial images for law enforcement purposes is already covered by legislation, but the collection, use and sharing of Australian driver licence information through the driver licence database remains to be legislated.[216] The Australian Government Attorney-General's Department has said that '*this legislation will not increase the powers of police agencies to collect this information, or to use information in ways that they are not already authorised to do. It will provide a more transparent basis for the Commonwealth to operate the driver licence database, with additional privacy safeguards*'.[217] However, in an official statement sent by the Australian Federal Police, they said that '*the use of biometrics on smartphones has not benefited or adversely impacted law enforcement practices and is just another form of lock for a phone. The same legislative measures apply to smartphone biometrics as they do to pin codes and passwords in relation to electronic devices*'.[218]

The Digital Rights Watch and Australian Privacy Foundation, among other Australian organisations dedicated to protecting citizens' digital and privacy rights, have criticised the creation of a national biometrics database, arguing that it contravenes Australians' privacy rights and establishes unwarranted mass surveillance.[219] The national database will commence operation from mid-2018 onwards.[220]

Biometric Identification Services

The Australian Criminal Intelligence Commission ('ACIC') website outlines that '*the Biometric Identification Services ('BIS') project will deliver capability to replace the existing National Automated Fingerprint Identification System ('NAFIS') and enhance law enforcement's biometric capabilities with the delivery of a national facial recognition solution*'.[221] It will have identifying capabilities regarding fingerprints, palm prints, footprints and facial recognition, as well as matching services.

---

[216] Ibid 3.
[217] Ibid.
[218] Email from Australian Federal Police to the author of this report, 23 February 2018.
[219] Digital Rights Watch, *Comprehensive National Face Database Incompatible With A Free Society* (6 October 2017) <http://digitalrightswatch.org.au/2017/10/06/comprehensive-national-face-database-incompatible-with-a-free-society/>.
[220] Australian Government, Attorney-General's Department, *Face Matching Services* <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Face-verification-service.aspx>.
[221] Australian Criminal Intelligence Commission ('ACIC'), *Biometric Identification Services* (16 June 2017) <https://www.acic.gov.au/our-services/biometric-matching/biometric-identification-services>.

National Criminal Investigation DNA Database ('NCIDD')

Another Australian biometric database is the National Criminal Investigation DNA Database ('NCIDD'), which was formerly operated by CrimTrac and is now operated by the ACIC.[222] In contrast, the NCIDD only includes DNA information of individuals only if the individual has been convicted of a criminal offence or has been a suspect for a set amount of time.[223] Whereas the NFBMC includes biometric information of all Australians along with their passport. In addition, '*the Digital Transformation Agency is currently considering plans for the integration of biometrics, and possibly, the NFBMC forming the foundation of the new Trusted Digital Identity Framework*'.[224]

Australian Taxation Office ('ATO') Voice Biometrics

The ATO has made use of voice biometric technology since first introducing it in September 2014.[225] The ATO's use of voice biometrics has replaced '*an authentication process which required citizens to provide personal details or have the correct documentation details in front of them when they called*'.[226] The use of voice biometrics has reduced the length of the process for ATO contact centre agents as well as customers. Pal notes that since 2016, '*over 1.7m Australians have enrolled voiceprints with the ATO, so that when they call the contact centre, they must simply repeat, "In Australia my voice identifies me"*'.[227] Although, customers are still given the option to speak with a live contact agent and they can enrol and verify themselves through normal conversation with an agent. The ATO has also introduced voice biometrics on their mobile app, which allows customers to secure their transactions on the mobile app, '*by allowing users to log in into the app via the "In Australia my voice identifies me" passphrase*'. Pal reports that users of the ATO's voice biometrics option have reported positive feedback.[228]

---

[222] Mann and Smith, above n 143, 7.
[223] Ibid 8.
[224] Ibid.
[225] Gregory Pal, 'Voice of the people: the case for biometrics in government' (2016) 5 *Biometric Technology Today* 5, 6 <https://www.sciencedirect.com/science/article/pii/S096947651630087X>.
[226] Ibid.
[227] Ibid.
[228] Ibid.

While transitioning to the use of voice biometrics, the ATO consulted '*with privacy and civil liberties groups from the start to ensure the system was mutually agreeable to both policy makers and the general public*'.[229] As such, Pal argues that,

> '*by embracing voice biometrics as part of their wider digital strategy, governments will be better equipped to provide public services that meet the needs of a digital-first population, at the same time as strengthening security and reducing costs. Yet, as with all change management, the process of implementation must be carefully controlled, with open dialogue and widespread education about the technology and the ethical implications that come with it*'.[230]

Some Australian banks have implemented biometric capabilities allowing their customers to log into their mobile banking services with their fingerprints or voices, as opposed to traditional methods such as passwords.[231] This suggests that banks are noticing trends in consumer smartphone biometrics use.

[229] Ibid.
[230] Ibid 7.
[231] Alison Banney, *The rise of voice biometrics in banking* (7 February 2018) Finder <https://www.finder.com.au/the-rise-of-voice-biometrics-in-banking>.

Country Case Studies

India

Aadhaar Project

In India, the Aadhaar Project was introduced under the Unique Identification Authority of India ('UIDAI') by the United Progressive Alliance ('UPA') government in 2009.[232] The Aadhaar Project introduced the Aadhaar card, which '*contains the demographic features such as name of the citizen, father/mother's name, date of birth, sex, address of the citizen, and biometric features such as photograph, fingerprints and iris (eye) details*'.[233] In addition to these features, citizens are provided with a unique 12-digit identity number, printed on their card. This information is located on a single, centralised database and is regarded as the world's largest biometrics database. Indian citizens are able to update most of their personal information stored on their Aadhaar Card online on the official UIDAI website, provided they provide relevant information or documents. However, citizens are not able to change their biometric data, due to its uniqueness.[234]

The Aadhaar card is more than a means for proof of identity – it allows citizens to link their card to other government schemes.[235] The Aadhaar Project is addressed in the 2016 Aadhaar Bill (Targeted Delivery of Financial and Other Subsidies, Benefits and Services), and '*in this bill, [the] Aadhaar card was made mandatory for authentication purposes like salary payment, pension schemes, school enrolment, train booking, for getting [a] driving license, to get a mobile SIM, to use a cyber café etc*'.[236] Moreover the Aadhaar card has eased the Know Your Customer processes, with citizens being able to verify their identity through the use of biometric validation located within the Aadhaar card.[237]

---

[232] Raja Siddharth Raju, Sukhdev Singh, and Kiran Khatter, 'Aadhaar Card: Challenges and Impact on Digital Transformation' (2017) 1, 1 <https://arxiv.org/ftp/arxiv/papers/1708/1708.05117.pdf>.
[233] Ibid 2.
[234] Ibid.
[235] Ibid 2-3.
[236] Ibid.
[237] Ibid 5.

The Aadhaar card has also enabled Indian citizens to engage in cashless transactions.[238] Moreover, the IDFC Bank Ltd, became the first bank to allow customers to pay using biometrics using their fingerprint. This option was created for Indian citizens who do not own a smartphone or those who own a phone without banking features. This payment option was made possible by the process that the '*IDFC bank distributes a biometric enabled device to the merchants to connect it to smartphones for transaction purposes*'. Other Indian banks followed IDFC Bank by enabling Aadhaar pay.

Breaches to Aadhaar

Since Aadhaar's inception, there have been security breaches. Indeed, a recently reported security breach reported by The Tribune was that one of their reporters was able to gain access to services offered by anonymous sellers on WhatsApp.[239] The sellers offered to share leaked Aadhaar data of over 1 billion Aadhaar numbers. For $500 RS (less than $10 AUD) and a 10 minute wait, the service included an "agent" creating a gateway for the reporter and then the reporter was able to gain access to any Aadhaar data. The Tribune reported that, '*you could enter any Aadhaar number in the portal, and instantly get all particulars that an individual may have submitted to the UIDAI (Unique Identification Authority of India), including name, address, postal code, PIN, photo, phone number and email*'. For an extra 300 RS (less than $6 AUD), the agent was able to provide software that can print off Aadhaar cards that correspond to the Aadhaar number the user (in this case, the reporter) was searching for. After hearing about the breach, UIDAI officials in Chandigarh were quick to notify the UIDAI technical consultants in Bangaluru.[240] While no fingerprint or retina data were released in the hack, this signals a cautionary tale of the implications of a wide scale, national security breach of a biometrics database.[241]

---

[238] Ibid 8.
[239] Rachna Khaira, 'Rs 500, 10 minutes, and you have access to billion Aadhaar details', *The Tribune* (online), 4 January 2018 <http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html>.
[240] Ibid.
[241] Michael Safi, 'Personal data of a billion Indians sold online for £6, report claims', *The Guardian* (online), 4 January 2018 <https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar>.

Under the *Aadhaar Act*, publicly displaying Aadhaar numbers is illegal.[242] However, a twitter user @iam_anandv tweeted in October 2017 that he found out that by simply searching his tagline, the search results revealed Aadhaar details.[243]

Figure 10: Tweet by Twitter user @iam_anandv who found out that by simply searching his tagline in a search engine, the search results revealed Aadhaar details.[244]

After being legally required to release information, the UIDAI admitted that in November 2017 there were over 200 websites that contained private Aadhaar details.[245] Recent reports stated that, '*Airtel was accused of opening up bank accounts for customers without their consent when gathering Aadhaar biometrics to*

[242] Rohith Jyothish, 'The World's Biggest Biometric Database Keeps Leaking People's Data', *Fast Company* (online), 12 January 2018 <https://www.fastcompany.com/40516447/the-worlds-biggest-biometric-database-keeps-leaking-peoples-data>.
[243] Ibid.
[244] Ibid.
[245] Ibid.

authenticate their mobile phone accounts'.[246] Along with the security breaches of Aadhaar, other access issues have been documented by Human Rights Watch, such as, '*poor internet connectivity, machine malfunction, and worn out fingerprints such as those of older people or manual laborers*'.[247] Nonetheless, the security flaws of the Aadhaar Project should be seen as a warning sign for any wide scale implementation of a centralised biometrics database.

United Kingdom (UK)

The *Deloitte Mobile Consumer Survey 2017* results for the UK revealed that 79 per cent of smartphone users in the UK are using their device's fingerprint scanner and that smartphone biometrics use has increased from previous years. Further, Deloitte UK reported that the UK is the highest adopter of smartphone fingerprint biometrics of all developed countries surveyed.[248] The UK's adoption of smartphone biometrics is also prevalent in policing, as in February 2018, it was reported that new mobile fingerprinting technology will enable frontline offices within the UK to use an app on their smartphones to identify people in under a minute by connecting them to two real-time databases.[249] Nonetheless, the *Deloitte Mobile Consumer Survey* for the UK revealed that the use of smartphone fingerprint sensors increased by a third since the previous year amongst the 16-75 age group in the UK.[250] As well, over a third of mobile devices in the UK enable the use of biometrics. Amongst the group who are using smartphone biometrics, 96 per cent of respondents use it to unlock their smartphone. Moreover, the use of smartphones as well as smartphone fingerprint sensors for authenticating money transfers has also increased. Deloitte UK has highlighted that 3D facial recognition is set to become the preferred type of biometrics in smartphones by the end of 2018.[251]

---

[246] Ashish Malhotra, 'The World's Largest Biometric ID System Keeps Getting Hacked', *Vice* (online), 9 January 2018 <https://motherboard.vice.com/en_us/article/43q4jp/aadhaar-hack-insecure-biometric-id-system>.
[247] Human Rights Watch, *India: Identification Project Threatens Rights* (13 January 2018) <https://www.hrw.org/news/2018/01/13/india-identification-project-threatens-rights>.
[248] Deloitte (UK), 'Surge in UK adoption of fingerprint recognition points way to mainstream biometric authentication at the expense of the password' (Press Release, 8 December 2017) <https://www2.deloitte.com/uk/en/pages/press-releases/articles/surge-in-uk-adoption-of-fingerprint-recognition.html>.
[249] UK Government Digital Service, Gov.UK, 'Police trial new Home Office mobile fingerprint technology' (Press Release, 10 February 2018) <https://www.gov.uk/government/news/police-trial-new-home-office-mobile-fingerprint-technology>.
[250] Deloitte (UK), above n 248.
[251] Ibid.

The UK is not engaging with any national-level use of smartphone biometrics, although they have been and continue to invest heavily in the use of biometric technology, particularly to enhance government identity systems.[252] Examples include biometric visas, biometric passports and the cancelled biometric National Identity Scheme ('NIS'). Bright argues that, '*whilst the government has been keen to position them as tools for combating identity fraud, illegal migration and (perhaps most of all) terrorism, opponents regard them as evidence of increasing government surveillance, where the life of the everyday citizen becomes subject to ever increasing intrusion and control*'.[253] This argument is particularly relevant when considering that it was reported that over 50 per cent of people on Britain's counter-terrorism biometric databases are innocent.[254] Nonetheless, there has also been a proposal for the use of biometrics within schools in the UK.[255] Although, there are harms with implementing such a system as the UK Information Commissioner's Office[256] argues that collecting biometrics such as fingerprints from children may make children '*feel like criminals*'.[257] However, the problem with the legitimacy of biometric systems is that there is a lack of knowledge about new technologies, such as biometrics, because gaining knowledge on such technologies can be difficult.[258]

In contrast to Australia's lack of a specific Commissioner for the use of biometrics, under the UK's *Protection of Freedoms Act 2012* (UK) c 9, a Commissioner for the Retention and Use of Biometric Material ('Biometrics Commissioner') has been established.[259] Indeed, the Commissioner acts to govern the responsible storing and use of biometric information in the UK and to ensure that surveillance and counter-terrorism laws are not an excuse for overzealous use of biometrics. Their Commissioner also has statutory powers '*that specifically relate to biometrics, including oversight of the retention of biometric information via deciding on applications made by police to retain biometric information, as well as reporting to the Secretary of State about these functions or other matters considered appropriate by the Biometrics*

---

[252] Jonathan Bright, 'Building Biometrics: Knowledge Construction in the Democratic Control of Surveillance Technology' (2011) 9(1/2) *Surveillance & Society* 233 <https://ssrn.com/abstract=2641175>.
[253] Ibid.
[254] Alexander J Martin, 'More than half of people on UK counter-terror biometrics databases are innocent' (26 May 2016) *The Register* <http://bit.ly/2CREpGs>; Alastair R MacGregor QC, *Further Report By The Biometrics Commissioner on Issues Raised In His 2015 Annual Report* (April 2016) <https://regmedia.co.uk/2016/05/26/police_biometrics.pdf>.
[255] Bright, above n 252, 237.
[256] For purposes such as but not limited to: monitoring attendance and student use of libraries, and managing school payment systems; Ibid.
[257] Ibid.
[258] Ibid 233.
[259] Mann and Smith, above n 143, 20.

Commissioner'.[260] Although, the Commissioner's powers are limited to DNA and fingerprint biometrics, and do not apply to other forms, such as advanced facial recognition technology.[261]

Despite the UK recently deciding to leave Europe, the *GDPR* will apply to the UK from 25 May 2018, meaning that there will be stringent measures implemented to regulate and protect the flow of consumer data.[262] As well, the Data Protection Bill was published in the UK on 14 September 2017, meaning that data protection law will be modernised in the UK. The UK's Information Commissioner's Office, has stated that the Bill and the *GDPR* are to be read side by side.[263]

Canada

In Canada, fingerprints have been collected from refugee claimants, detainees and persons ordered for deportation from Canada since 1993 by the Canada Border Services Agency ('CBSA').[264] Since 2006, the Canadian Air Transport Security Authority has also been utilising biometrics, such as fingerprints and iris scans for staff working in secure areas at airports. According to the Government of Canada, '*the CBSA also offers voluntary trusted traveller programs (such as NEXUS and CANPASS) that use iris capture technology to confirm the identity of low-risk air travellers who are members of these programs*'.

More recently, the Canadian government announced that it will begin trialling the 'Known Traveller Digital Identity' system, which was launched at the World Economic Forum meeting in Davos, Switzerland.[265] The system will utilise technologies such as biometrics, blockchain technology and artificial intelligence. The Canadian government is one of the governments involved in this project and the project is said to improve border security, minimise the threat of cyber-terrorism and allow travellers to have

---

[260] Ibid.
[261] Ibid.
[262] Gemalto, *Biometric data and the General Data Protection Regulation* (18 February 2018) <https://www.gemalto.com/govt/biometrics/biometric-data>.
[263] Ibid.
[264] Government of Canada, *Use of biometrics in Canada* (29 June 2015) <https://www.canada.ca/en/immigration-refugees-citizenship/corporate/mandate/corporate-initiatives/biometrics/use-canada.html>.
[265] Rahul Kalvapalle, *Canada testing 'digital ID' system that uses blockchain, biometrics to screen travellers* (27 January 2018) Global News <https://globalnews.ca/news/3991496/known-traveller-digital-identity-pilot-canada/>.

more control over how and when their information is being shared with authorities.[266] The aim of the Known Traveller Digital Identity system is to allow airport authorities to devote more time and resources on scrutinising high-risk travellers.[267] Also, the system '*would allow travellers to use an app to store and share information with authorities in advance, allowing more time for pre-screening*'. The data would be stored on the publicly accessible and decentralised blockchain in an encrypted form, hence promising advanced privacy.[268]

At the time of writing, there have been no Canadian consumer smartphone biometrics usage figures available.

[266] Ibid; Max Greenwood, *Canada Will Use Blockchain and Biometrics to Establish Digital Borders* (25 January 2018) Tech Vibes <https://techvibes.com/2018/01/25/canada-will-use-blockchain-and-biometrics-to-establish-digital-borders>.
[267] Kalvapalle, above n 265.
[268] Ibid.

Conclusion and Recommendations

The purpose behind this research report was to examine the implications of the advancement in smartphone biometric data capturing capabilities and use for Australian consumers. Having analysed consumer surveys and studies, peer-reviewed and non-peer-reviewed literature, government and industry policy papers and findings, and independently conducted interviews with leading government and professional sources, the findings indicate that there are both positive and negative implications in the use of smartphone biometrics.

Positive implications include better accessibility, ease of use, convenience and security (to an extent). Whereas negative implications include an easier point of access to sensitive data (i.e. if stored on the smartphone or a centralised network, copying someone's biometric data) and greater security implications if compromised (i.e. once stolen, biometrics cannot be changed and can be used to facilitate crime). Negative implications also include inaccessibility to some consumers (i.e. the use of biometrics can exclude handicapped individuals, minors, and the elderly from screening, due to non-existent or underdeveloped biometrics, as well as 'false positives'), lack of consumer consent or control over how their smartphone biometric data is stored and shared, and privacy concerns.

Recommendations for Consumers

Given the high smartphone adoption rates and smartphone biometric usage rates, it is recommended that Australian consumers be more empowered in order to *decide* whether to opt-in or opt-out of using their biometric data to access their smartphones.

This means that Australian consumers should have more access to information regarding:

- What biometrics are;
- How their biometric data is stored on their smartphones;
- What the current and future implications of the use of their smartphone biometric data are;

- Whether accessibility and convenience outweighs the potential for a highly compromising security breach if their biometric data is stolen or corrupted; and
- What can be done to ensure consumers are more in control of their biometric data.

Recommendations for Government

The report shows examples that establishes that government is primarily concerned with the capture of biometric data generally and not in the context of smartphones (for the time-being). Nonetheless, it may well be that government efforts to establish wide scale biometric data collection systems are influencing industry to enhance their biometric data capturing capabilities, particularly regarding smartphone brands.

As such, government should:

- Aim to be a positive example of how biometric data can be captured without compromising the integrity of consumers through their increasing surveillance of citizens' data under the guise of improving national security;
- Comply with privacy and data breach notification legislation;
- Use their platform to better empower consumers to be made more aware of what their biometric data is, how it is being used, and what consumers can do to be more in control of their data;
- Use their platform to inform and guide industry into helping consumers do the aforementioned; and
- Be a good example of best practice.

Recommendations for Industry

As creators and distributors of smartphones and their biometric data capturing capabilities and as analysts of that data, industry have an obligation to their consumers to adopt best practice.

It is recommended that industry:

- Ensure that their smartphones that enable biometric data capture are secure;
- Ensure that consumers are made more aware of how their biometric data is being captured and utilised for industry or government gains;
- Comply with privacy and data breach notification legislation; and
- Not share data outside of explicitly permitted and necessary use of biometric data.

Authors

Jelena Ardalic

Jelena Ardalic is a law graduate from the University of New South Wales, who also holds a Bachelor in Media (Journalism). Jelena has experience working in cyber law and policy, telecommunications policy and within law firms. Jelena has an interest in biometrics, blockchain technology, cyber law, cybercrime, national security, telecommunications, and advances in technology.

References

Articles and Reports

Ahmed, Tousif, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia, 'Privacy concerns and behaviors of people with visual impairments' (Paper presented at Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea, 18-23 April 2015) 3523

Australian Government, Australian Cyber Security Centre ('ACSC'), *2016 Cyber Security Survey* 1 <https://www.acsc.gov.au/publications/ACSC_Cyber_Security_Survey_2016.pdf>

Australian Government, ACSC, *2017 Threat Report* 1 <https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf>

Australian Government, *Australia's Cyber Security Strategy 2016* 1 <http://bit.ly/2mjGv6T>

Australian Government*, Australia's Cyber Security Strategy: 2017 Update* 1 <http://bit.ly/2mtpg3K>

Australian Government, Australian Law Reform Commission, *For your Information: Australian Privacy law and Practice*, Report No 108 (2008) Ch 9 Overview: Impact of Developing Technology on Privacy: Biometrics <https://www.alrc.gov.au/publications/9. Overview%3A Impact of Developing Technology on Privacy/biometric-systems>

Australian Government, Office of the Australian Information Commissioner ('OAIC'), *Australian Businesses and the EU General Data Protection Regulation* (January 2018) Privacy Business Resource 21 <https://www.oaic.gov.au/resources/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation.pdf>

Australian Government, OAIC, *Australian Community Attitudes to Privacy Survey (ACAPS) 2017* <https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017>

Australian Payments Network, *Australian Payments Fraud 2017 Jan-Dec 2016 Data* 1 <http://bit.ly/2DcBJ2a>

Axelrod, Warren C, 'The New Age of Near-Zero Privacy' (2016) 4 *ISACA Journal* 1 <https://www.isaca.org/Journal/archives/2016/volume-4/Documents/The-New-Age-of-Near-zero-Privacy_joa_Eng_0716.pdf>

Azenkot, Shiri, Kyle Rector, Richard E Ladner, and Jacob O Wobbrock, 'PassChords: secure multi-touch authentication for blind people' (Paper presented at Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility, Boulder, Colorado, USA, 22-24 October 2012) 159

Bright, Jonathan, 'Building Biometrics: Knowledge Construction in the Democratic Control of Surveillance Technology' (2011) 9(1/2) *Surveillance & Society* 233 <https://ssrn.com/abstract=2641175>

Clarke, Roger, *A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation* (15 February 2010) <http://www.rogerclarke.com/ID/IdModel-1002.html>

Clarke, Roger, *Biometrics and Privacy, 'Uses of Biometrics'* (15 April 2001) <http://www.rogerclarke.com/DV/Biometrics.html>

Clarke, Roger, 'Biometrics as 'RegTech'?' (Working Version, 23 August 2017) <http://www.rogerclarke.com/ID/BiomRegI.html>

Deloitte Mobile Consumer Survey 2017 <https://www2.deloitte.com/au/mobile-consumer-survey>

Eberz, Simon, Nicola Paoletti, Marc Roeschlin, Andrea Patané, Marta Kwiatkowska, Ivan Martinovic, 'Broken Hearted: How To Attack ECG Biometrics' (2017) Network and

Distributed System Security (NDSS) Symposium 1 <http://qav.comlab.ox.ac.uk/papers/epr+17.pdf>

Emami, Catherine, Dr Rick Brown and Dr Russell G Smith, 'Use and acceptance of biometric technologies among victims of identity crime and misuse in Australia' (2016) 511 *Trends and issues in crime and criminal justice* 1 <https://aic.gov.au/publications/tandi/tandi511>

Gagbla, George Kofi, 'Applying Keystroke Dynamics for Personal Authentication' (2005) 1 <https://ssrn.com/abstract=2508480>

Hino, Hayiel, 'Assessing Factors Affecting Consumers' Intention to Adopt Biometric Authentication Technology in E-shopping' (2015) 14(1) *Journal of Internet Commerce* 1 <https://doi.org/10.1080/15332861.2015.1006517>

Khan, Imran, *Multimodal Biometrics– Is Two Better Than One?* (2006) Frost & Sullivan Insight <http://www.frost.com/prod/servlet/market-insight-print.pag?docid=80082644>

Krishnaprasad, K and PS Aithal, 'A Conceptual Study on User Identification and Verification Process using Face Recognition Techniques' (2017) *International Journal of Applied Engineering and Management Letters (IJAEML)* 1(1) 6 <https://ssrn.com/abstract=2988405>

Krishnaprasad, K and PS Aithal, 'Fingerprint Image Segmentation: A Review of State of the Art Techniques' (2017) 2(2) *International Journal of Management, Technology, and Social Sciences (IJMTS)* 29 <https://ssrn.com/abstract=3025477>

Lobo, Sylvan, Ulemba Hirom, VS Shyama, Mridul Basumatori, and Pankaj Doke, 'Coping with Accessibility Challenges for Security - A User Study with Blind Smartphone Users' (2017) 3 <https://link.springer.com/chapter/10.1007/978-3-319-68059-0_1>

Mann, Monique and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments And Approaches To Oversight' (2017) 40(1) *University of New South*

Wales Law Journal (Advance) 1 <http://unswlawjournal.unsw.edu.au/sites/default/files/04-mannsmith-advance-access-final.pdf>

Nakar, Sharon and Dov Greenbaum, 'Now You See Me, Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy' (2017) 23(1) *Boston University Journal of Science & Technology Law* 88 <https://www.bu.edu/jostl/files/2017/04/Greenbaum-Online.pdf>

New South Wales Auditor-General's Report, Audit Office of New South Wales, *Report on Internal Controls & Governance 2017* (20 December 2017) Audit Office of New South Wales 1 <http://bit.ly/2Es7Ivk>

Ogbanufe, Obi and Dan J Kim, 'Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment' (2018) 106 *Decision Support Systems* 1 <https://doi.org/10.1016/j.dss.2017.11.003>

Pal, Gregory, 'Voice of the people: the case for biometrics in government' (2016) 5 *Biometric Technology Today* 5 <https://www.sciencedirect.com/science/article/pii/S096947651630087X>

Paul, Greig and James Irvine, 'Fingerprint Authentication is here, but are we ready for what it brings?' (2017) 1 <https://pure.strath.ac.uk/portal/files/45829838/Paul_Irvine_IEEE_CEM_2015_Fingerprint_authentication_is_here_but_are_we_ready.pdf>

Paul, Greig and James Irvine, 'IEDs on the Road to Fingerprint Authentication: Biometrics have vulnerabilities that PINs and passwords don't' (2016) 5(2) *IEEE Consumer Electronics Magazine* 79 <http://ieeexplore.ieee.org/document/7450785/>

Phang, Samantha SS and Christopher J Pavlovski, 'Hazards of Biometric Authentication in Practice' (2016) 4(1) *IT in Industry* 34 <http://it-in-industry.com/itii_papers/2016/4116itii05.pdf>

Prasanalakshmi, B and A Kannammal, ‘Analyzing Security Measures with Unimodal and Multimodal Biometrics’ (2009) *International Conference on Sensors, Security, Software and Intelligent Systems* 26 <https://ssrn.com/abstract=2946038>

Roy, Aditi, Nasir Memon, and Arun Ross, ‘MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems’ (2017) 12(9) *IEEE Transactions on Information Forensics and Security* 2013 <http://ieeexplore.ieee.org/document/7893784/>

Roy, Soumen, Utpal Roy, and DD Sinha, ‘Automatically Age Group and Gender Prediction by Analysing Typing Pattern on Touchscreen’ (29 November 2017) 1 <https://ssrn.com/abstract=3079504>

Scheinman, Michelle, ‘Protecting Your Brain Waves and Other Biometric Data in a Global Economy’ (8 April 2013) 1 <https://ssrn.com/abstract=2382951>

Siddharth Raju, Raja, Sukhdev Singh, and Kiran Khatter, ‘Aadhaar Card: Challenges and Impact on Digital Transformation’ (2017) 1 <https://arxiv.org/ftp/arxiv/papers/1708/1708.05117.pdf>

Solayappan, Nimalan and Shahram Latifi, ‘A Survey of Unimodal Biometric Methods’ (Paper presented at Proceedings of the 2006 International Conference on Security & Management, Las Vegas, Nevada, USA, 26-29 June 2006) 3 <https://pdfs.semanticscholar.org/8b0c/87e040c8718fd11e545e911996e3a149c69d.pdf>

Tait, Bobby L, ‘Secure cloud-based biometric authentication utilising smart devices for electronic transactions’ (2014) 6(1) *International Journal Electronic Security and Digital Forensics* 52 <https://www.inderscienceonline.com/doi/abs/10.1504/IJESDF.2014.060170>

Tsukayama, Hayley, ‘Companies you’ve never heard of are exposing your personal data’, *The Washington Post* (online), 22 December 2017 <http://dpo.st/2zjJm46>

Ungureanu, Adrian S and Claudia Costache, ‘Palm Print as a Smartphone Biometric: Another option for digital privacy and security’ (2016) 5(3) *IEEE Consumer Electronics Magazine* 71 <http://ieeexplore.ieee.org/document/7539264/?reload=true>

Zhang, Yulong, Zhaofeng Chen, Hui Xue, and Tao Wei FireEye Labs, ‘Fingerprints On Mobile Devices: Abusing and Leaking’ (2015) *Blackhat Conference* 1 <https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf>

Legislation

Australian Passports Act 2005 (Cth)

Australian Passports Amendment (Identity-matching Services) Bill 2018 (Cth)

Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014 (Cth)

Criminal Code Act 1995 (Cth)

European Parliament & Council, General Data Protection Regulation (entered into force 25 May 2018)

Identity-matching Services Bill 2018 (Cth)

Migration Amendment (Strengthening Biometrics Integrity) Act 2015 (Cth)

Migration Legislation Amendment (Identification and Authentication) Act 2004 (Cth)

Privacy Act 1988 (Cth)

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)

United Nations Human Rights, International Covenant on Civil and Political Rights, opened for signature 16 December 1966, (entered into force 23 March 1976)

Author's own communication

Email from Australian Federal Police to the author of this report, 23 February 2018

Interview with David Vaile, Chairman of the Australian Privacy Foundation and co-convenor of the Cyberspace Law and Policy Community (telephone, 7 February 2018)

Interview with Frank Zeichner, CEO of Internet of Things Alliance Australia (IoTAA) (telephone, 15 February 2018)

Interview with Ian Oppermann, CEO of the NSW Data Analytics Centre (telephone, 14 February 2018)

Interview with Dr Katina Michael, board member of the Australian Privacy Foundation (telephone, 9 February 2018)

Interview with Stephen Clarke, Jebel Consultant Group (email, 22 February 2018)

Other

Android Developer, *Android 6.0 APIs* (25 April 2018) <https://developer.android.com/about/versions/marshmallow/android-6.0.html>

Apple Support, *About Touch ID advanced security technology* (11 September 2017) Apple <https://support.apple.com/en-au/HT204587>

Australian Bureau of Statistics (ABS), *8153.0 - Internet Activity, Australia, June 2017* (29 September 2017) <http://www.abs.gov.au/ausstats/abs@.nsf/0/00FD2E732C939C06CA257E19000FB410?Opendocument>

Australian Criminal Intelligence Commission ('ACIC'), *Biometric Identification Services* (16 June 2017) <https://www.acic.gov.au/our-services/biometric-matching/biometric-identification-services>

Australian Government, Attorney-General's Department, *Face Matching Services, Fact Sheet – Face Matching Services* 1 <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Face-matching-services-fact-sheet.pdf>

Australian Government, Attorney-General's Department, *Face Matching Services* <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Face-verification-service.aspx>

Australian Government, Department of Foreign Affairs and Trade, 'Australia Launches ePassports' (Media Release, 25 October 2005) archived material <https://foreignminister.gov.au/releases/2005/fa132_05.html>

Australian Government, Department of Home Affairs, *Arrivals SmartGate* <https://www.homeaffairs.gov.au/trav/ente/goin/arrival/smartgateor-epassport>

Banney, Alison, *The rise of voice biometrics in banking* (7 February 2018) Finder <https://www.finder.com.au/the-rise-of-voice-biometrics-in-banking>

Bkav Corporation, *Bkav's new mask beats Face ID in "twin way": Severity level raised, do not use Face ID in business transactions* (27 November 2017) <http://www.bkav.com/dt/top-news/-/view_content/content/103968/bkav﷒s-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions>

Bkav Corporation, *Bkav's New Mask Beats Face ID in "Twin Way": Do not Use Face ID in Business Transactions* (26 November 2017) YouTube <https://youtu.be/rhiSBc061JU>

Council of Australian Governments (COAG), Special Meeting of the Council of Australian Governments on Counter-Terrorism Communiqué (Canberra, Australia, 5 October 2017) 1 <http://bit.ly/2DeacOt>

Deloitte (UK), 'Surge in UK adoption of fingerprint recognition points way to mainstream biometric authentication at the expense of the password' (Press Release, 8 December 2017) <https://www2.deloitte.com/uk/en/pages/press-releases/articles/surge-in-uk-adoption-of-fingerprint-recognition.html>

Digital Rights Watch, *Comprehensive National Face Database Incompatible With A Free Society* (6 October 2017) <http://digitalrightswatch.org.au/2017/10/06/comprehensive-national-face-database-incompatible-with-a-free-society/>

Fintech Finance, *Fintech experts say mobile and biometric authentication to replace PINs within five years* <http://www.fintech.finance/01-news/fintech-experts-say-mobile-and-biometric-authentication-to-replace-pins-within-five-years/>

Gemalto, *Biometric data and the General Data Protection Regulation* (18 February 2018) <https://www.gemalto.com/govt/biometrics/biometric-data>

Government of Canada, *Use of biometrics in Canada* (29 June 2015) <https://www.canada.ca/en/immigration-refugees-citizenship/corporate/mandate/corporate-initiatives/biometrics/use-canada.html>

Greenwood, Max, *Canada Will Use Blockchain and Biometrics to Establish Digital Borders* (25 January 2018) Tech Vibes <https://techvibes.com/2018/01/25/canada-will-use-blockchain-and-biometrics-to-establish-digital-borders>

Hildenbrand, Jerry, *How does Android save your fingerprints?* (26 September 2017) Android Central <https://www.androidcentral.com/how-does-android-save-your-fingerprints>

Human Rights Watch, *India: Identification Project Threatens Rights* (13 January 2018) <https://www.hrw.org/news/2018/01/13/india-identification-project-threatens-rights>.

Ip, Chris, *The Galaxy S8 Iris Scanner Can be Hacked With Aging Tech* (23 May 2017) Engadget <https://www.engadget.com/2017/05/23/galaxy-s8-iris-scanner-hacked/>

Juniper Research, 'Biometric Authentication App Downloads to Reach 770 Million by 2019, finds Juniper Research' (Press Release, 20 January 2015) <https://www.juniperresearch.com/press/press-releases/biometric-authentication-app-downloads-to-reach-77>

Jyothish, Rohith, 'The World's Biggest Biometric Database Keeps Leaking People's Data', *Fast Company* (online), 12 January 2018 <https://www.fastcompany.com/40516447/the-worlds-biggest-biometric-database-keeps-leaking-peoples-data>

Kalvapalle, Rahul, *Canada testing 'digital ID' system that uses blockchain, biometrics to screen travellers* (27 January 2018) Global News <https://globalnews.ca/news/3991496/known-traveller-digital-identity-pilot-canada/>

Kaspersky Lab, 'Biometric skimmers are here: Kaspersky Lab Examine Near-Future Threats to ATMs' (Press Release, 22 September 2016) <https://usa.kaspersky.com/about/press-releases/2016_biometric-skimmers-are-here>

Khaira, Rachna, 'Rs 500, 10 minutes, and you have access to billion Aadhaar details', *The Tribune* (online), 4 January 2018 <http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html>

Lee, Justin, *Report shows growing public acceptance of biometric authentication* (15 July 2015) Biometric Update <http://www.biometricupdate.com/201507/report-shows-growing-public-acceptance-of-biometric-authentication>

MacGregor, Alastair R QC, *Further Report By The Biometrics Commissioner on Issues Raised In His 2015 Annual Report* (April 2016) <https://regmedia.co.uk/2016/05/26/police_biometrics.pdf>

Malhotra, Ashish, 'The World's Largest Biometric ID System Keeps Getting Hacked', *Vice* (online), 9 January 2018 <https://motherboard.vice.com/en_us/article/43q4jp/aadhaar-hack-insecure-biometric-id-system>

Martin, Alexander J, 'More than half of people on UK counter-terror biometrics databases are innocent' (26 May 2016) *The Register* <http://bit.ly/2CREpGs>

Martonik, Andrew, *A look back at Sooner, Google's first Android phone* (21 October 2015) Android Central <http://www.androidcentral.com/look-back-google-sooner-first-android-phone>

Media.ccc.de, *starbug: Ich sehe, also bin ich ... Du (english translation)* (29 December 2014) YouTube <https://youtu.be/VVxL9ymiyAU>

Naiya, Pavel, 'More than one billion smartphones to feature facial recognition in 2020' (Press Release, 7 February 2018) <https://www.counterpointresearch.com/one-billion-smartphones-feature-face-recognition-2020/>

Nguyen, Mai, 'Vietnamese researcher shows iPhone X face ID 'hack'', *Reuters* (online), 15 November 2017 <https://www.reuters.com/article/us-apple-vietnam-hack/vietnamese-researcher-shows-iphone-x-face-id-hack-idUSKBN1DE1TH>

O'Sullivan, Matt, 'Sydney Airport biometric trial for Qantas flights: No passport required', *The Traveller* (online), 22 February 2018 <http://www.traveller.com.au/sydney-airport-biometric-trial-for-qantas-flights-no-passport-required-h0wgzn>

Oxford Dictionaries, *Smartphone* <https://en.oxforddictionaries.com/definition/smartphone>

Pauli, Darren, ‘Peace-sign selfie fools menaced by fingerprint-harvesting tech’, *The Register* (online), 12 January 2017 <https://www.theregister.co.uk/2017/01/12/fingerprint_photographs/>

Pepitone, Julianne, ‘OPM Hack: 5.6 Million Fingerprints (Not 1.1 Million) Were Stolen’ 23 September 2015 *NBC News* (online) <https://www.nbcnews.com/tech/security/opm-5-6-million-fingerprints-not-1-1-million-were-n432281>

Perez, Roi, *Starbug's in your eyes: German hacker spoofs iris recognition* (26 October 2015) SC Magazine UK <https://www.scmagazineuk.com/starbugs-in-your-eyes-german-hacker-spoofs-iris-recognition/article/535281/>

PC Magazine, *Encyclopedia: Definition of: Smartphone* <https://www.pcmag.com/encyclopedia/term/51537/smartphone>

Safi, Michael, ‘Personal data of a billion Indians sold online for £6, report claims’, *The Guardian* (online), 4 January 2018 <https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar>

Statista, *Number of smartphone users in Australia from 2015 to 2022 (in millions)* (July 2017) <https://www.statista.com/statistics/467753/forecast-of-smartphone-users-in-australia/>

Trigger, Rebecca, ‘Experts sound alarm as biometric data from drivers' licences added to government database’, *ABC news* (online), 16 January 2018 <http://www.abc.net.au/news/2018-01-15/alarm-raised-as-drivers-licences-added-to-government-database/9015484>

Tweedie, Steven, ‘The world's first smartphone, Simon, was created 15 years before the iPhone’, *Business Insider* (online), 14 June 2015 <https://www.businessinsider.com.au/worlds-first-smartphone-simon-launched-before-iphone-2015-6?r=US&IR=T>

UK Government Digital Service, Gov.UK, ‘Police trial new Home Office mobile fingerprint technology’ (Press Release, 10 February 2018) <https://www.gov.uk/government/news/police-trial-new-home-office-mobile-fingerprint-technology>

Williams, Brett, ‘Study suggests your phone's fingerprint scanner is easily fooled’, *Mashable Australia* (online), 12 April 2017 <https://mashable.com/2017/04/11/smartphone-fingerprint-scanner-vulnerability/ - kPZdzR2uyiq1>

Williams, Brett, ‘Thieves might be able to break into your Android phone — if they're very, very determined’, *Mashable Australia* (online), 24 January 2017 <https://mashable.com/2017/01/23/android-pattern-lock-hack-report/ - 5ZPVIpvirmqG>

Zara, Christopher, ‘Facebook Keeps Getting Sued Over Face-Recognition Software, And Privacy Groups Say We Should Be Paying More Attention’, *International Business Times* (online), 3 September 2015 <http://www.ibtimes.com/facebook-keeps-getting-sued-over-face-recognition-software-privacy-groups-say-we-2082166>

(Inside back cover:

Leave blank and delete this text)