AUTOMATED FACIAL RECOGNITION TECHNOLOGY: RECENT DEVELOPMENTS AND APPROACHES TO OVERSIGHT

MONIQUE MANN* AND MARCUS SMITH**

I INTRODUCTION

There has been a rapid expansion in the type and volume of information collected for security purposes following the terrorist attacks on the United States of America ('US') on 11 September 2001. This event has been described as precipitating a program of 'globalized surveillance'.[1] New technology, biometric identification and other developments such as metadata retention can provide governments with an increasingly comprehensive picture of citizens' lives. This has resulted in a rapidly expanding use of human biometric information in law enforcement investigations and other applications.[2] The first part of this article describes Automated Facial Recognition Technology ('AFRT') and its law enforcement and border security applications, as well as integration with image sources such as closed circuit television ('CCTV'), social media and big data. Recent developments including biometric identification documents (licences and passports) and information sharing arrangements that promote searching between state, territory and national government databases to facilitate a national facial recognition system will be discussed. These developments are reviewed against the backdrop of tension between individual privacy rights and collective security objectives. The second part of the article examines existing privacy protections, law enforcement exemptions, and regulatory options based on an international review of current oversight models. As is often the case in relation to technological advancements, government regulation and the legal system have

* Lecturer, School of Justice, Crime and Justice Research Centre, Faculty of Law, Queensland University of Technology and Board of Directors of the Australian Privacy Foundation.

** Adjunct Professor of Law, Faculty of Business, Government and Law, University of Canberra.

The authors would like to thank Professor Reece Walters, Dr Ian Warren, and the three anonymous reviewers for their helpful comments on earlier versions of this article. The authors would also like to thank Michael Wilson and the editors of the UNSW Law Journal for excellent research and editorial assistance.

1 David Lyon, *Surveillance after September 11* (Polity, 2003) 109–10.

2 David Lyon, 'Biometrics, Identification and Surveillance' (2008) 22 *Bioethics* 499, 500. For a discussion of how the increasing use of biometric identifiers has been justified within law enforcement see Hendrik Hegemann and Martin Kahl, 'Constructions of Effectiveness and the Rationalization of Counterterrorism Policy: The Case of Biometric Passports' (2015) 38 *Studies in Conflict & Terrorism* 199.

lagged behind, and potential regulatory approaches have not been adequately discussed in either public debate or the academic literature. In the absence of a constitutional bill of rights or a cause of action for serious invasion of privacy in Australia, there are limited protections in relation to biometric information, and those that do exist, such as protections provided by the *Privacy Act 1988* (Cth), are subject to exemptions. This has led to a significant governance gap. In order to align with international regulatory practices, the functions and funding of the Office of the Australian Information Commissioner ('OAIC') should be strengthened or, alternatively, a Biometrics Commissioner should be introduced.

II AUTOMATED FACIAL RECOGNITION TECHNOLOGY

A Development and Application

The use of photographs for suspect identification is a well-established component of police investigation. AFRT is an extension of facial 'profiling' or 'mapping' that has been used in criminal justice systems around the world since the 19th century, and continues to be used today.[3] Traditional forensic facial mapping involves comparing measurements between facial features (a quantitative method known as photo-anthropometry or photogrammetry) or the similarities and differences in facial features (a qualitative method known as morphological analysis).[4] In comparison with these techniques, AFRT involves the automated extraction, digitisation and comparison of the spatial and geometric distribution of facial features. Using an algorithm similar to the ones used in fingerprint recognition, AFRT compares an image of a face with one stored in a database.[5] At the enrolment stage, a digital photograph of a subject's face is taken and a contour map of the position of facial features is converted into a digital template using an algorithm. AFRT systems digitise, store and compare facial templates that measure the relative position of facial features.[6] The processes associated with extraction, digitisation and database storage are significant because they extend privacy considerations beyond the mere capture

3 For a review of Australian case law in relation to facial mapping expert evidence see, eg, Gary Edmond et al, 'Law's Looking Glass: Expert Identification Evidence Derived from Photographic and Video Images' (2009) 20 *Current Issues in Criminal Justice* 337; Gary Edmond and Mehera San Roque, '*Honeysett v The Queen*: Forensic Science, "Specialised Knowledge" and the Uniform Evidence Law' (2014) 36 *Sydney Law Review* 323. The most significant case in Australian case law is *R v Tang* (2006) 65 NSWLR 681 which established the admissibility of facial mapping expert evidence, provided that the expert does not make positive identifications. Subsequent cases follow this precedent: see, eg, *Murdoch v The Queen* [2007] NTCCA 1, [288]–[289] (The Court). There is no precedent for use of AFRT to make positive identifications in criminal cases in Australia. See also Jake Goldenfein, 'Police Photography and Privacy: Identity, Stigma and Reasonable Expectation' (2013) 36 *University of New South Wales Law Journal* 256.

4 Edmond et al, above n 3, 339.

5 Andy Adler and Michael E Schuckers, 'Comparing Human and Automatic Face Recognition Performance' (2007) 37 *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics* 1248, 1248.

6 Karl Ricanek Jr and Chris Boehnen, 'Facial Analytics: From Big Data to Law Enforcement' (2012) 45(9) *Computer* 95, 95.

of photographs. In particular, this involves the emergence of a 'surveillant assemblage' to create a 'data double' enabling automated sorting, database storage, information sharing and integration.[7] This means human bodies are abstracted into data flows, enabling identification and connection with other datasets including 'big data'. Big data is defined as the collection, aggregation and interrogation of very large datasets.[8] These datasets can be analysed through inferential techniques revealing trends and associations. Big data is difficult to regulate under 'traditional concepts of privacy' as individuals are separated from data.[9] However, biometrics can both identify individuals and provide a gateway to the large and expanding datasets held by government, law enforcement and security agencies.[10]

AFRT can be used to conduct one-to-one matching, or the verification of the identity of an individual, or one-to-many searching using databases.[11] One-to-one matching is routinely used at international borders through the comparison of faces with digital templates stored in biometric passports.[12] Additionally, AFRT can be used to search databases for a suspect in a similar way to other biometrics, such as searching a DNA database for a profile obtained from a crime scene.[13] However, in comparison to other forms of biometrics such as DNA and fingerprinting, AFRT is less invasive, can be conducted from a distance and can be integrated with existing surveillance systems. In particular, open source images can be collected from social media and integrated into AFRT systems without an individual's knowledge or consent.[14]

The integration of AFRT with CCTV (known as 'Smart CCTV') has been implemented in the United Kingdom ('UK') and the US, and, more recently, in some Australian jurisdictions.[15] Smart CCTV was reportedly first used in the UK,

---

7 Kevin D Haggerty and Richard V Ericson, 'The Surveillant Assemblage' (2000) 51 *British Journal of Sociology* 605, 606.

8 Melissa de Zwart, Sal Humphreys and Beatrix van Dissel, 'Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK' (2014) 37 *University of New South Wales Law Journal* 713, 713.

9 Ibid 721–2. See also Graham Greenleaf, 'Foreword: Abandon All Hope?' (2014) 37 *University of New South Wales Law Journal* 636; David Lyon, 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique' [2014] (July–December) *Big Data & Society* 1, 2.

10 Paul De Hert, 'Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions' in Patrizio Campisi (ed), *Security and Privacy in Biometrics* (Springer, 2013) 369, 387.

11 Philip Brey, 'Ethical Aspects of Facial Recognition Systems in Public Places' (2004) 2 *Journal of Information, Communication and Ethics in Society* 97, 98.

12 Dean Wilson, 'Australian Biometrics and Global Surveillance' (2007) 17 *International Criminal Justice Review* 207; Steven R Clark, 'Balancing Privacy and Security in the Australian Passport System' (2011) 16 *Deakin Law Review* 325.

13 See generally Marcus Smith and Monique Mann, 'Recent Developments in DNA Evidence' (Trends & Issues in Crime and Criminal Justice No 506, Australian Institute of Criminology, November 2015).

14 See generally Zak Stone, Todd Zickler and Trevor Darrell, 'Toward Large-Scale Face Recognition Using Social Network Context' (2010) 98 *Proceedings of the IEEE* 1408.

15 Brey, above n 11, 100; Kelly A Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York University Press, 2011) ch 2; NEC Australia, 'NEC Facial Recognition Helps NT Police Solve Cold Cases and Increase Public Safety in Australia' (Press Release, 1 September 2015) <http://au.nec.com/en_AU/press/201509/nec-facial-recognition-increases-public-safety-in-australia.html>.

where the London Metropolitan Police Service has operated it since 1998.[16] In 2001 police in Florida in the US trialled Smart CCTV, although this was suspended in August 2003 after no identifications were produced.[17] It is worth noting that the efficacy of AFRT remains contentious, as research has suggested accurate identification of non-stationary human faces poses challenges.[18] More recently, it has been reported that businesses in the UK are using a system known as 'Facewatch' to share CCTV images with police, with notification when a person on a 'watch list', including suspected shoplifters, enters their store.[19] This demonstrates how AFRT can be used pre-emptively to identify and manage 'risky' people who may engage in future crime.[20]

A further application of AFRT is the analysis of images taken from the internet to obtain facial templates for law enforcement databases. The widespread use of social media websites such as Facebook has contributed to a rapid expansion in the number of images uploaded to the internet. In 2011 it was estimated that Facebook held approximately 100 billion photos in its database.[21] Additionally, it is estimated that the number of facial photographs held by Facebook increases at a rate of 6 billion photos per month.[22] Facebook has an AFRT system that automatically tags photographs with the identity of the people in them, linking their images to personal details they provide on their own page, including age, gender, location, contacts and political views.[23] Facebook users can also name (or 'tag') people who are included in the photographs they upload, regardless of whether that person has a Facebook account, and therefore, regardless of whether they have provided consent for Facebook to create and store a digital facial template.[24] These developments in AFRT have also been used in other social media applications. For example, in early 2016 an application known as 'FindFace' was launched in Russia. It enables users to take

16 Brey, above n 11, 100.

17 Ibid 108.

18 See Jeremiah R Barr et al, 'Face Recognition from Video: A Review' (2012) 26(5) *International Journal of Pattern Recognition and Artificial Intelligence* 1266002-1. For an earlier review of facial recognition technology see Zhao et al, 'Face Recognition: A Literature Survey' (2003) 35 *ACM Computing Surveys* 399, 453.

19 'Facewatch "Thief Recognition" CCTV on Trial in UK Stores', *BBC News* (online), 16 December 2015 <http://www.bbc.com/news/technology-35111363>.

20 For an overview of the concept of pre-crime, see Lucia Zedner, 'Fixing the Future? The Pre-Emptive Turn in Criminal Justice' in Bernadette McSherry, Alan Norrie and Simon Bronitt (eds), *Regulating Deviance: The Redirection of Criminalisation and the Futures of Criminal Law* (Hart Publishing, 2009) 35; Jude McCulloch and Bree Carlton, 'Preempting Justice: Suppression of Financing of Terrorism and the "War on Terror"' (2006) 17 *Current Issues in Criminal Justice* 397; Jude McCulloch and Sharon Pickering, 'Pre-Crime and Counter-Terrorism: Imagining Future Crime in the "War on Terror"' (2009) 49 *British Journal of Criminology* 628; Jude McCulloch and Sharon Pickering, 'Future Threat: Pre-Crime, State Terror, and Dystopia in the 21st Century' (2010) 81 *Criminal Justice Matters* 32.

21 Yana Welinder, 'Face Recognition Privacy in Social Networks under German Law' (2012) 31(1) *Communications Law Bulletin* 5, 6.

22 Ibid.

23 Anna Bunn, 'Facebook and Face Recognition: Kinda Cool, Kinda Creepy' (2013) 25(1) *Bond Law Review* 35, 39-45.

24 Ibid, 40, 61-5. See also Norberto Nuno Gomes de Andrade, Aaron Martin and Shara Monteleone, '"All the Better to See You With, My Dear": Facial Recognition and Privacy in Online Social Networks' (2013) 11(3) *IEEE Security & Privacy* 21.

photographs of people in public and search social media sites to identify them. The application has access to a database of over 1 billion photos, and claims 70 per cent reliability in identification.[25]

This is significant as photographs on social media sites can be easily integrated into other big data used for law enforcement and security purposes. For example, in Australia, the National Open Source Intelligence Centre collects and analyses open source information, subsequently providing access to intelligence and police agencies.[26] Further, in June 2016 the Minister for Justice and Minister Assisting the Prime Minister for Counter Terrorism announced $1.6 million in additional funding for the Australian Federal Police ('AFP') to develop a new big data capability to mine information from social media sites and other 'data-rich environments' to supplement existing intelligence sources.[27] The availability of high-quality photographs, integration with existing surveillance technologies enabling tracking, collection of information from open sources, and pre-emptive applications, provides the potential for AFRT to be more intrusive than other forms of biometric identification.

B Information Sharing Arrangements

Australian jurisdictions have been preparing for an expansion in the use of AFRT for several years. The implementation of AFRT at state and territory level commenced with the introduction of biometric licences, which differ across Australian jurisdictions. For example, in 2009 AFRT was introduced in New South Wales ('NSW') through an amendment to the regulations governing drivers' licences.[28] AFRT is used to verify the identity of individuals who apply for a relevant permit (including a driver licence or certificate of registration). Some jurisdictions have implemented AFRT without reliance on Roads Traffic Authority photographic databases or biometric licences. For example, the Northern Territory government is currently trialling the NeoFace system, which captures facial templates through CCTV, police body-worn cameras ('BWCs') and surveillance drones. In September 2015 it was reported that 100 000 images had been transitioned into the AFRT database.[29]

Australian jurisdictions have begun amending legislation to enable driver licence photograph databases to be shared with federal agencies. In late 2015 the *Road Transport Legislation Amendment (Release of Stored Photographs) Regulation 2015* (NSW) was introduced to amend clause 107 of the *Road*

---

25 Shaun Walker, 'Face Recognition App Taking Russia by Storm May Bring End to Public Anonymity', *The Guardian* (online), 17 May 2016 <https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte>.

26 National Open Source Intelligence Centre, *Home* (9 December 2016) <http://www.nosic.com.au/>.

27 Michael Keenan, 'Investing in Innovation for Our Law Enforcement Elite' (Media Release, 15 June 2016) <http://www.keenan.net.au/PortfolioMedia/FeaturedPortfolioNews/tabid/141/ID/942/INVESTING-IN-INNOVATION-FOR-OUR-LAW-ENFORCEMENT-ELITE.aspx>.

28 The regulations were made pursuant to the *Road Transport (Driver Licensing) Act 1998* (NSW), which was later repealed by sch 1 of the *Road Transport Legislation (Repeal and Amendment) Act 2013* (NSW). Specifically, s 19 provided the general regulation-making power and s 40(1)(g) empowered the making of regulations prescribing a purpose for which photographs may be kept and used.

29 NEC Australia, above n 15.

Transport (Driver Licensing) Regulation 2008 (NSW). This permits the release of NSW Roads and Maritime Services ('RMS')[30] photographs collected for the purpose of issuing driver licences[31] to the NSW Crime Commission, the Australian Security Intelligence Organisation ('ASIO'), and the Identity Security Strike Team (Sydney), an inter-agency taskforce of the AFP and NSW Police. Under the amended clause 107, photographs may be released for the purposes of investigation of 'relevant criminal activity',[32] a 'terrorist act' and 'threat of a terrorist act',[33] or a 'terrorism offence'.[34] It appears that images in the NSW RMS database can now be released without warrant or the knowledge or consent of individuals concerned. While this broadens an existing power to access information for law enforcement purposes, concerns have been raised about the use of information provided for a specific purpose subsequently becoming available for secondary purposes for which consent was neither sought nor obtained.[35]

Within Australia, the most significant development occurred in late 2015, when the Commonwealth government announced that a National Facial Biometric Matching Capability ('NFBMC') would become operational in mid-2016,[36] enabling agencies to share facial templates for the purpose of AFRT.[37]

---

30 'The Authority' to which permission is given is defined in legislation as the RMS: *Road Transport Act 2013* (NSW) s 4 (definition of 'the Authority').

31 Section 55 of the *Road Transport Act 2013* (NSW) states that the Act applies to photographs created for the purpose of issuing driver licences for cars and boats, as well as 'proof of age' cards, firearms licence or permit, security industry licences, weapons permits, licences to work as a private investigator or debt collector, licences to operate a tattoo parlour, and marine safety licences. Section 57(1) of the Act outlines the circumstances in which these photographs can be released, including to the NSW Police Force. Section 57(1)(k) of the Act states that photos can be released 'in accordance with the statutory rules', which are defined in s 4 as 'regulations and rules made by the Governor under this Act', referring in this context to the *Road Transport (Driver Licensing) Regulation 2008* (NSW).

32 Defined under the *Crime Commission Act 2012* (NSW) s (4)(1) as 'any circumstances implying, or any allegations, that a relevant offence may have been, or may be being, or may in the future be, committed', which under sch 4 cl 4(1) extends to 'circumstances or allegations relating to relevant offences that were or may have been committed before the commencement of this clause'.

33 A 'terrorist act' is defined under the *Terrorism (Police Powers) Act 2002* (NSW) s 3(1) as when an 'action is done with the intention of advancing a political, religious or ideological cause' and with the intention of 'coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country' or 'intimidating the public or a section of the public'.

34 Defined under the *Australian Security Intelligence Organisation Act 1979* (Cth) s 4 as 'an offence against Subdivision A of Division 72 of the *Criminal Code*' or 'an offence against Part 5.3 of the *Criminal Code*'.

35 Sean Nicholls, 'ASIO, Crime Commission Granted Access to Photographs of NSW Citizens to Aid Terrorism Fight', *The Sydney Morning Herald* (online), 19 October 2015 <http://www.smh.com.au/nsw/asio-crime-commission-granted-access-to-photographs-of-nsw-citizens-to-aid-terrorism-fight-20151018-gkbxa6.html>.

36 Michael Keenan, 'New $18.5 Million Biometrics Tool to Put a Face on Crime' (Media Release, 9 September 2015) <https://www.ministerjustice.gov.au/Mediareleases/Pages/2015/ThirdQuarter/9-September-2015-New-$18-5-million-biometrics-tool-to-put-a-face-to-crime.aspx>. The first phase of a face verification service was announced as operational in November 2016. Negotiations with states and territories to provide access to driver licence images are ongoing. A face identification service (to identify unknown persons through one-to-many searching) is expected to become operational in 2017: see Michael Keenan, 'New Face Verification Service to Tackle Identity Crime' (Media Release, 16 November 2016) <https://www.ministerjustice.gov.au/Mediareleases/Pages/2016/FourthQuarter/New-face-verification-service-to-tackle-identity-crime.aspx>.

The NFBMC will allow for the verification of identity through one-to-one matching of identity documents, and one-to-many searching of databases to identify unknown persons. At the Commonwealth level, participating agencies include the Department of Foreign Affairs and Trade ('DFAT') (passport images), the Department of Immigration and Border Protection ('DIBP') (visa images), and the AFP; the service will expand to provide access to various other government agencies in the future.[38] Potentially concerning aspects of the NFBMC relate to integration with CCTV and other surveillance systems (municipal, state and federal government), the number of images that will be captured, and how this data will be used.

Importantly, the NFBMC is being established in a manner that does not require expanded police powers or the introduction of specific Commonwealth legislation. Amendments to state legislation and regulations, along with interagency agreements, will facilitate information sharing. As such, the NFBMC is described as linking 'the facial recognition systems of participating agencies via a network in which images may be shared, on a query and response basis, via a central exchange or interoperability hub'.[39] This means that the NFBMC is being introduced through administrative processes and is occurring outside of a legislative framework, and the increased scrutiny that entails.

An example of a similar national biometric database is the National Criminal Investigation DNA Database ('NCIDD'), initially operated by CrimTrac, now managed by the Australian Criminal Intelligence Commission ('ACIC').[40] However, in contrast to the NFBMC, the NCIDD was established through a 2001 amendment to part 1D of the *Crimes Act 1914* (Cth).[41] There are a number of other attributes of the NCIDD that differ from the approach being taken to the NFBMC. A DNA profile is only included in the NCIDD if the person has been convicted of a criminal offence, or in the case of suspects, for a 'defined period of time'.[42] This differs from the NFBMC, where the biometric information of every Australian citizen with a passport will be included. The NCIDD currently contains DNA profiles of approximately 860 000 individuals. By comparison, it

---

37 Above n 36; Information Integrity Solutions Pty Ltd, 'National Facial Biometric Matching Capability – Interoperability Hub' (Privacy Impact Assessment, Attorney-General's Department, August 2015) 15 <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Privacy-Impact-Assessment-National-Facial-Biometric-Matching-Capability.PDF>; Attorney-General's Department (Cth), *Face Verification Service* (2016) <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Biometrics.aspx>.

38 Attorney-General's Department (Cth), *Face Verification Service*, above n 37.

39 Attorney-General's Department (Cth), 'Preliminary Privacy Impact Statement of the National Facial Biometric Matching Capability – Interoperability Hub' (Department Response, December 2015) 1 <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/AGD-response-privacy-impact-assessment.pdf>.

40 CrimTrac and the Australian Crime Commission were merged to form the ACIC in July 2016 with enactment of the *Australian Crime Commission Amendment (National Policing Information) Act 2016* (Cth). The merger is described as 'bring[ing] together Australia's national criminal intelligence and information capabilities': Explanatory Memorandum, Australian Crime Commission Amendment (National Policing Information) Bill 2015 (Cth) 2.

41 Amended by the *Crimes Amendment (Forensic Procedures) Act 2001* (Cth) sch 1.

42 Marcus Smith, *DNA Evidence in the Australian Legal System* (LexisNexis Butterworths, 2016) 82–7 [3.16]–[3.28].

is estimated approximately half of the Australian population hold biometric passports. On this basis, the NFBMC will initially include the facial templates of approximately 12 million Australians.[43]

Under the National Identity Security Strategy,[44] policy documents state that integration of existing photographs into biometric systems is preferred because this reduces costs and decreases the regulatory burden. State agencies are working together to 'eliminate barriers to sharing':

> Agencies using biometrics are therefore encouraged to reuse biometric assets that may already exist across Government, rather than invest in new technologies or to enhance existing assets where possible. The Framework also encourages agencies to work together to eliminate barriers to sharing biometric and related data, where sharing is necessary in the national interest or appropriate in the public interest.[45]

This also reduces the potential for external scrutiny, although agencies must theoretically have a lawful basis to collect and use facial images. For example, the AFP is legally permitted to collect facial images only where it is 'reasonably necessary to fulfil its policing functions' and share them when it is 'reasonably necessary for law enforcement purposes'.[46] According to the Attorney-General's Department, this exception, along with the amendments to state sharing procedures outlined above, means that '[t]here is no requirement for new Commonwealth legislation, and the Australian Government has no plans to expand the powers of law enforcement agencies to collect facial images'.[47] However, the NFBMC also applies technology to convert images into digital facial templates for the purpose of multi-source comparison and identification.

It is also important to note that the implementation of the NFBMC is occurring in conjunction with broader integration of national police information systems in Australia. The ACIC has been working towards integration of all police information systems including biometric databases, metadata repositories, criminal history and general police intelligence files.[48] In 2016 NEC was engaged to implement a multimodal integrated biometric database of 12 million facial images and 6.7 million sets of fingerprints currently held in Australian police databases (state, territory and federal), which will be known as the Biometric

---

43 Approximately 48 per cent of Australians hold biometric passports, which *together with* Australians who hold biometric drivers' licences illustrates that a significant amount of citizens are subject to potential biometric surveillance: Department of Foreign Affairs and Trade (Cth), 'Program 2.2: Passport Services' in *Annual Report 2010–2011* (2011) <http://dfat.gov.au/about-us/publications/corporate/annual-reports/annual-report-2010-2011/performance/2/2.2.html>.

44 Attorney-General's Department (Cth), 'National Identity Security Strategy: Statement of Biometric Interoperability Capability Requirements' <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/statement-of-biometric-interoperability-capability-requirements.pdf>.

45 Ibid 2.

46 Attorney-General's Department (Cth), 'Face Matching Services' (Fact Sheet) 3 <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Fact-Sheet-National-Facial-Biometric-Matching-Capability.pdf>. See *Australian Federal Police Act 1979* (Cth) s 60A(2) for the legal basis of federal police recording and retaining personal information.

47 Attorney-General's Department (Cth), above n 46.

48 CrimTrac, 'ICT Blueprint for National Police Information Sharing 2014–2018' (Strategic Document, 25 June 2015) <https://crimtrac.govcms.gov.au/sites/g/files/net526/f/ICT%20blueprint%202014-18.pdf?v=1435216387>.

Identification Services ('BIS').[49] Within the merged ACIC, it can be expected that this database will form part of the NFBMC. Further, the Digital Transformation Agency ('DTA') is currently considering plans for the integration of biometrics, and possibly, the NFBMC forming the foundation of the new Trusted Digital Identity Framework ('TDIF').[50] This raises additional concerns in relation to scope creep and use for secondary (and tertiary) purposes for which consent was neither sought nor obtained. The developments discussed in this section are not only relevant to domestic law enforcement, but also have applications to Australian border security.

C Biometrics at the Border

The use of AFRT in travel documents expanded following the US terrorist attacks in 2001 due to a requirement that anyone entering that country have machine-readable biometric passports.[51] The International Civil Aviation Organisation ('ICAO') then selected AFRT as the global standard for interoperable biometric passports.[52] Aligned with these developments, and over the previous decade, the Australian Department of Immigration and Border Protection ('DIBP') has been expanding a program of collecting biometric information for border security, first from non-citizens, and now from every individual who enters or departs Australia.

The *Migration Legislation Amendment (Identification and Authentication) Act 2004* (Cth) authorised the collection of 'personal identifiers'[53] from *non-citizens* in the visa application process and in the course of immigration clearance. This legislation was followed by the *Australian Passports Act 2005* (Cth) which introduced biometric passports. According to section 47(1)(a) of the *Australian Passports Act 2005* (Cth), the Minister for Foreign Affairs 'may specify methods (including technologies) that are to be used 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'. AFRT was selected as the most appropriate biometric identifier

---

49 NEC Australia, 'CrimTrac Selects NEC to Provide National Facial Recognition and Fingerprint Matching Capability' (Press Release, 2 May 2016) <http://au.nec.com/en_AU/press/201605/crimtrac-nec-facial-recognition-fingerprint-matching-capability.html>. See generally CrimTrac, above n 48. The BIS is expected to be operational from 2017. It has not been reported whether the BIS will include information external to CrimTrac's existing information assets that are drawn from state and territory police information.

50 Digital Transformation Agency, *Digital Identity* <https://www.dta.gov.au/what-we-do/platforms/identity/>. The DTA has also clarified that the 'digital identity' will include the use of biometrics: Beverley Head, 'DTO Eyes Biometric Identity System', *InnovationAus.com* (online), 10 August 2016 <http://www.innovationaus.com/2016/08/DTO-eyes-biometic-identity-system>.

51 Clark, above n 12, 343.

52 Ibid 346. Criteria used to assess biometric technologies include, amongst others, compatibility with machine-readable travel documents, global public perception, storage, and performance: at 345–6.

53 Personal identifiers are defined in s 5A(1) of the *Migration Act 1958* (Cth) as 'fingerprints or handprints of a person' (ink or digital scanning), 'measurement of a person's height and weight', 'a photograph or other image of a person's face and shoulders', 'an audio or a video recording of a person', 'an iris scan', 'a person's signature', and 'any other identifier prescribed by the regulations, other than an identifier the obtaining of which would involve the carrying out of an intimate forensic procedure'.

in accordance with international standards established by the ICAO.[54] The scope of biometric data collection has continued to grow. For example, in 2006 the DIBP began collecting biometric information, including facial images and fingerprints from individuals caught fishing illegally in Australian waters.[55] Later in 2010 biometric information from offshore visa applicants was collected, and in 2012 from non-citizens refused entry to Australia.[56]

In 2014, as part of a tranche of national security legislation, the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* (Cth) extended the collection of personal identifiers to Australian citizens entering or leaving the country.[57] This includes the collection of biometric information by an automated border clearance system, known as a 'SmartGate'.[58] Then, the *Migration Amendment (Strengthening Biometrics Integrity) Act 2015* (Cth) consolidated seven previous provisions into a broad, discretionary power to collect one or more personal identifiers from both non-citizens and citizens. This was criticised by stakeholders and parliamentary committees when the Bill was debated, due to the breadth and scope of the discretionary power to collect biometric information, including from children without parental consent.[59] In sum, there are a number of concerns about the implementation of AFRT in Australia, particularly in light of the significant expansion in the collection and storage of personal data and growth in databases in general, coupled with diminishing opportunities for individuals to opt out, and, as will be discussed in the following sections of the article, little, if any, regulatory limits and protections.

III PRIVACY

A Privacy Rights and Enforcement Exemptions

The main privacy concerns associated with AFRT relate to the circumstances in which biometric information is obtained, retained, stored, shared between agencies, and the overall purposes for which it is used by governments, law enforcement and security agencies.[60] Biometric technology is 'privacy invasive' as it identifies individuals and can be used to link and connect information across

54 Clark, above n 12, 345–6.

55 Explanatory Memorandum, Migration Amendment (Strengthening Biometrics Integrity) Bill 2015 (Cth) 1.

56 Ibid.

57 *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* (Cth) sch 6.

58 See *Migration Act 1958* (Cth) s 166.

59 Mary Anne Neilsen, *Bill Digests*, No 111 of 2014–15, 4 June 2015, 12–14. See also Law Council of Australia, Submission No 10 to Senate Legal and Constitutional Affairs Committee*, Inquiry into the Migration Amendment (Strengthening Biometrics Integrity) Bill 2015 [Provisions]*, 10 April 2015, 18–19. The Senate Standing Committee for the Scrutiny of Bills and the Parliamentary Joint Committee on Human Rights raised concerns because the regulations that govern the collection of biometric information allow for Ministerial discretion: Neilson, above n 59, 5–6, 9.

60 de Andrade, Martin and Monteleone, above n 24.

datasets.[61] There is a range of privacy interests at stake in biometric information. These vary according to a number of factors, for example, whether they are used for verification (one-to-one confirmation) or identification (one-to-many database search), whether identifiable data or templates are stored and shared, and whether information is stored in a centralised database or localised device.[62] While these types of considerations and potential privacy impacts are relevant to all forms of biometric information, they are especially important in the context of AFRT, because faces are difficult to hide and alter, and are linked to an individual's physical existence.[63] AFRT presents additional privacy risks as it can be used to locate and track individuals through widely implemented CCTV surveillance systems, as discussed above.

The legal and philosophical concept of privacy is the assertion that some aspects of an individual's life are personal and should be free from intrusion.[64] In Australia, personal information is protected by the *Privacy Act 1988* (Cth) ('*Privacy Act*'). The *Privacy Act* was developed in response to Australia's obligations under the *International Covenant on Civil and Political Rights* ('*ICCPR*') and seeks 'to promote the protection of the privacy of individuals'.[65] However, the *Privacy Act* also states that 'the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities'.[66] The *Privacy Act* therefore takes a 'balancing' approach between individual rights to privacy and other interests, which is apparent when considering law enforcement exemptions.

Schedule 1 of the *Privacy Act* includes 13 Australian Privacy Principles ('APPs'). The APPs establish how government agencies (with exceptions), as well as private sector and not-for-profit agencies must manage personal information. While each of the APPs is relevant to developments in AFRT, the principles that relate to the notification of the collection of personal

---

61 De Hert, above n 10, 390.

62 For complete treatment of privacy issues presented by biometrics see Patrizio Campisi, 'Security and Privacy in Biometrics: Towards a Holistic Approach' in Patrizio Campisi (ed), *Security and Privacy in Biometrics* (Springer, 2013). These issues could be addressed in the design of biometric systems, policies and procedures and robust oversight of use, discussed further in the final Part of this article.

63 de Andrade, Martin and Monteleone, above n 24, 22. Another technology that raises similar concerns and that was recently implemented in Australia is Automated Licence Plate Recognition (ALPR). Licence plate information is linked to the registered vehicle owner, including their identification, enabling tracking (through CCTV or electronic toll collection). There are similarities between AFRT and ALPR, including the use of technology for surveillance through the digitisation of routinely collected information, image recognition and database technology. See also Warren et al, 'When the Profile Becomes the Population: Examining Privacy Governance and Road Traffic Surveillance in Canada and Australia' (2013) 25 *Current Issues in Criminal Justice* 565, where the authors argue that in relation to the introduction of ALPR in Australia, new technologies have resulted in a diminished requirement for reasonable suspicion and a lack of safeguards in relation to the collection and use of personal information.

64 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193. For a recent overview of the literature concerning privacy see also Colin J Bennett, 'In Defence of Privacy: The Concept and the Regime' (2011) 8 *Surveillance & Society* 485; Adam Moore, 'Defining Privacy' (2008) 39 *Journal of Social Philosophy* 411.

65 *Privacy Act* s 2A(a); *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

66 *Privacy Act* s 2A(b).

information and the use or disclosure of personal information are most important.[67] Under the *Privacy Act*, sensitive information is defined to include 'biometric information that is to be used for the purposes of automated biometric verification or biometric identification' as well as 'biometric templates'.[68] Sensitive information must only be collected with the consent of the individual concerned,[69] unless the entity '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'.[70] Entities cannot use or disclose information collected for a particular purpose for a secondary purpose, without the consent of the individual,[71] unless 'the use or disclosure of the information is reasonably necessary for one or more enforcement related activities'.[72] These exemptions are significant because agencies with an enforcement function do not need consent, a warrant, or a court order to collect and retain photographs, to process this information to create facial templates and disclose or share this information with other agencies.

In Australia, exemptions to the *Privacy Act* have been criticised as being too broad.[73] The Australian Law Reform Commission ('ALRC') conducted an inquiry into the *Privacy Act*, recommending that exemptions should only be permitted with compelling justification.[74] The exemptions made to the *Privacy Act* for the purposes of 'enforcement related activities' have been made on the basis of balancing individual interests against those of collective security. Scholars have argued that the consequence of this balancing approach is that 'individual rights are invariably "traded off" against the community interests in preventing, detecting and prosecuting crime'.[75] These exemptions, coupled with

---

67 Schedule 1 of the *Privacy Act* establishes the APPs. The APPs relate to the open and transparent management of personal information (APP 1), anonymity and pseudonymity (APP 2), collection of solicited personal information (APP 3), dealing with unsolicited personal information (APP 4), notification of the collection of personal information (APP 5), use or disclosure of personal information (APP 6), direct marketing (APP 7), cross-border disclosure of personal information (APP 8), adoption, use or disclosure of government related identifiers (APP 9), quality, security, access to, and correction of, personal information (APPs 10-13).

68 *Privacy Act* s 6(1) (definition of 'sensitive information' paras (d)–(e)).

69 *Privacy Act* sch 1 cl 3.3(a).

70 *Privacy Act* sch 1 cl 6.1. Section 6 defines 'enforcement body' as agencies that have an enforcement function, including the Australian Federal Police, the Integrity Commissioner, the Australian Criminal Intelligence Commission, the Immigration Department, and a police force or service of a State or a Territory.

71 *Privacy Act* sch 1 cl 6.1 (APP 6).

72 *Privacy Act* sch 1 cl 6.2(e). Section 6 relevantly defines 'enforcement related activity' as activities including the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction, or the conduct of surveillance activities, intelligence gathering activities or monitoring activities.

73 See, eg, Roger Clarke, *The Australian Privacy Act 1988 as an Implementation of the OECD Data Protection Guidelines* (15 February 1997) <http://www.rogerclarke.com/DV/PActOECD.html>. See also Graham Greenleaf, '"Tabula Rasa": Ten Reasons Why Australian Privacy Law Does Not Exist' (2001) 24 *University of New South Wales Law Journal* 262, 264.

74 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) vol 1, 113.

75 Simon Bronitt and James Stellios, 'Telecommunications Interception in Australia: Recent Trends and Regulatory Prospects' (2005) 29 *Telecommunications Policy* 875, 887.

the absence of a constitutional bill of rights, an enforceable cause of action or privacy tort, and an apparent lack of legislative will to protect privacy, demonstrates there are limited privacy protections in Australia relative to other comparable Western democracies. It is for these reasons that it has been argued that in Australia 'privacy seems a woefully inadequate tool to regulate the use of big data'.[76]

One prominent concern about the inadequacy of privacy protections is the potential for 'function creep', where the use of information taken for a particular purpose is used for other purposes for which consent was not obtained.[77] 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. While photographs have been a resource available for use in police investigations for some time,[78] the scale, digitisation, automation and integration of information provided by AFRT is a distinct shift in the way that the photographs are used and, at the least, warrants more detailed consideration. In the case of AFRT, it seems appropriate that safeguards are introduced.

As discussed earlier, the NFBMC has been implemented via inter-agency information sharing agreements rather than through the introduction of new Commonwealth legislation. It will operate as a 'hub' rather than a centralised database, facilitating matching between state, territory and Commonwealth databases. While there may be cost savings and other benefits as a result of this approach, it avoids scrutiny that might otherwise have occurred if new legislation was introduced. The Attorney-General's Department commissioned a Privacy Impact Assessment ('PIA') of the NFBMC, which made 16 recommendations, collectively adopted in whole or in part.[79] The PIA highlighted a number of issues and risks, emphasising the importance of compliance with the APPs regardless of whether the NFBMC 'hub' holds information in a centralised database. It was recommended that the NFBMC should be informed by a broad view of privacy, noting the potential for the information to be used in new ways as new technology becomes available, and the volume and sensitive nature of the information. The Australian Capital Territory ('ACT') Government was the only state or territory government to raise concerns about the NFBMC on the public record.[80] Despite this, and the existence of human rights legislation in the ACT, this will not undermine the implementation of a national 'hub'.[81] In the absence

76 de Zwart, Humphreys and van Dissel, above n 8, 741.

77 Brey, above n 11, 104–5.

78 Edmond et al, above n 3; Goldenfein, above n 3.

79 Information Integrity Solutions Pty Ltd, above n 37.

80 Law, Crime and Community Safety Council, 'Draft Communiqué: Law, Crime and Community Safety Council' (5 November 2015) <https://www.ag.gov.au/About/CommitteesandCouncils/Law-Crime-and-Community-Safety-Council/Documents/5-November-2015-LCCSC-Communique.pdf>.

81 The *Human Rights Act 2004* (ACT) ('*Human Rights Act*') was the first charter of human rights in Australia, modelled on the *ICCPR* (ratified by Australia in 1980). Section 12(a) states that '[e]veryone has the right not … to have his or her privacy, family, home or correspondence interfered with unlawfully

of statutory privacy protections, common law protections may provide a mechanism for limiting overreach or compelling action.

B Common Law Protection

The following section reviews relevant international cases that involve the retention of biometric information and photographs of individuals who have neither been charged nor convicted of an offence. Privacy rights in relation to biometric information have been upheld in the European Union under article 8(1) of the *European Convention on Human Rights* ('*ECHR*'),[82] which states that '[e]veryone has the right to respect for his private and family life, his home and his correspondence'. In the most prominent of these cases, *S v United Kingdom* ('*Marper*'),[83] the European Court of Human Rights considered the indefinite retention of biometric information by UK police (specifically DNA profiles and fingerprints).[84] In *Marper*, the applicants argued that article 8 of the *ECHR* was contravened by legislation enacted in the UK allowing the indefinite retention of biometric information after criminal proceedings had concluded and no conviction had been recorded. The Court found in favour of the applicants, stating:

> that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.[85]

In another UK case concerning the retention of photographs, *R (on the application of Wood) v Metropolitan Police Commissioner*,[86] Wood, a media coordinator employed for the Campaign Against Arms Trade, challenged the

---

or arbitrarily'. However, this is qualified by s 28(1), which states that '[h]uman rights may be subject only to reasonable limits set by laws that can be demonstrably justified in a free and democratic society'. If the ACT Supreme Court finds that legislation is inconsistent with the *Human Rights Act*, it cannot invalidate the provision or rule that any government Acts made under the provision are unlawful. It is only able to make a declaration of incompatibility (s 32). Amendments that came into effect in January 2009 impose a duty on public authorities to comply with the *Human Rights Act* (s 40B) and provide a right to remedy if a public authority has contravened a human right (s 40C). Victoria is the only other Australian jurisdiction to have human rights legalisation. The *Charter of Human Rights and Responsibilities 2006* (Vic) is similar to the ACT legislation and contains a provision providing a privacy right (s 13(a)), and a section that states reasonable limitations can be placed on a human right where the limitation 'can be demonstrably justified in a free and democratic society based on human dignity, equality and freedom, and taking into account all relevant factors' (s 7(2)).

82 *Convention for the Protection of Human Rights and Fundamental Freedoms,* opened for signature 4 November 1950, 213 UNTS 221213 UNTS 221 (entered into force 3 September 1953).

83 (European Court of Human Rights, Grand Chamber, Application Nos 30562/04 and 30566/04, 4 December 2008).

84 Including cellular samples, fingerprints and DNA profiles. Note that photographs or facial templates were not considered in this case.

85 (European Court of Human Rights, Grand Chamber, Application Nos 30562/04 and 30566/04, 4 December 2008) [125] (The Court).

86 [2009] 4 All ER 951.

retention of photographs taken by police at an annual arms industry trade fair. Although Wood had no criminal convictions and had never been arrested, police took photographs for intelligence purposes that could later be converted to 'spotter cards' intended for storage on a searchable database (although this did not happen to Wood's images). The Court of Appeal considered the facts of the case in light of article 8 of the *ECHR*, and found that as Wood had not committed a criminal offence, there was no basis to justify retention. A key factor in the Court's decision in this case was the proportionality of the actions of the police, especially given that Wood had not committed a criminal offence.

Further, in *R (on the Application of RMC) v Commissioner of Police of the Metropolis*,[87] RMC and FJ were arrested and photographed but not subsequently convicted of any offences. RMC and FJ unsuccessfully sought to have their photographs deleted from the Police National Computer ('PNC'). The applicants successfully challenged the decision with the Court finding that the 'existing policy concerning the retention of custody photographs … is unlawful'.[88] This case further affirmed that the retention of either biometric information or photographs of individuals who had been charged but not convicted of a criminal offence violated privacy rights established under article 8 of the *ECHR*. The judge in this case emphasised that photographs can uniquely identify individuals, in a way similar to other biometrics including DNA and fingerprints, and there was no basis for distinguishing them from other forms of biometric information.

The case law in Australia on this subject is not as developed as the UK, and there is no comparable precedent and no privacy tort.[89] Therefore, the only relevant case is *Caripis v Victoria Police (Health and Privacy)*,[90] which was heard by the Victorian Civil and Administrative Tribunal ('VCAT'). This considered similar facts as the UK cases, but arrived at a significantly different outcome. Ms Caripis brought an action against Victoria Police seeking to destroy images that were taken of her at an environmental protest. The VCAT considered whether by failing to destroy the footage, the Police contravened the *Information Privacy Act 2000* (Vic) which provided that '[a]n organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose'.[91] Victoria Police argued that the images were required for 'intelligence, planning and briefing for further protests, [and] evidence in case a complaint is made'.[92] The VCAT ultimately found that the retention of the protest footage was not an interference with Ms Caripis' privacy and police were able to retain the images for future use.[93] The *Caripis* case resulted in a different outcome to the UK cases, as in Australia there is no court of human rights, and no precedent equivalent to the *Marper* case. This must also

87 [2012] 4 All ER 510 ('*RMC*').
88 Ibid 537 [58] (Richards LJ).
89 Des Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339.
90 [2012] VCAT 1472 ('*Caripis*').
91 *Informational Privacy Act 2000* (Vic) sch 1 para 4.2. This Act has since been repealed and replaced with the *Privacy and Data Protection Act 2014* (Vic).
92 *Caripis* [2012] VCAT 1472 [26].
93 Ibid [101].

be considered with regard to the limited statutory privacy protection in Australia, described previously.

The absence of Australian precedent in this area is concerning, particularly as technology has resulted in an expansion of the application and use of biometric information. In addition to the retention of photographs, AFRT involves digitising facial templates, providing potential for information sharing and integration with big data, thus enabling use for secondary or unanticipated purposes.[94] As discussed above, in Australia, enforcement agencies or agencies with an enforcement function are exempt from the *Privacy Act* and individual privacy rights are balanced against collective security interests. Scholars have argued for more principled and pragmatic decision-making in similar cases.[95]

There is also an absence of legislation specifically governing the retention of biometric information (with the exception of DNA, where a conviction is required and retention is time limited), similar to the pre-*Marper* environment in the UK. This, coupled with a significant expansion in the collection and use of data by law enforcement, and exemptions in the *Privacy Act,* means that the current privacy framework is at risk of becoming obsolete. Lachmayer and Witzleb have argued:

> Australians lack a constitutional right to privacy and the data protection provisions of the *Privacy Act 1988* (Cth) contain significant holes. The activities of the intelligence agencies are not subject to the Act and exemptions to the APPs give law enforcement agencies relatively free reign in designing their information handling practices as well as easier access to information held by other agencies.[96]

In light of the above, a re-evaluation of privacy protections in response to new technology, and additional oversight mechanisms, are necessary. The expansion of data collection and information sharing by law enforcement and security agencies has not been matched with an expansion in oversight and accountability.

IV REGULATORY PROSPECTS

An important consideration when examining regulatory prospects for biometric technology is the responsibility for oversight, including the role of developing and reviewing policies, and responding to complaints, which may also include non-state actors with a governance function.[97] Effective oversight of

---

94 Daniel Neyland, 'Who's Who?: The Biometric Future and the Politics of Identity' (2009) 6 *European Journal of Criminology* 135*,* 152.

95 Bronitt and Stellios, above n 75. See also Simon Bronitt and James Stellios, 'Regulating Telecommunications Interception and Access in the Twenty-First Century: Technological Evolution or Legal Revolution?' (2006) 24 *Prometheus* 413; Olivier De Schutter and Françoise Tulkens, 'Rights in Conflict: The European Court of Human Rights as a Pragmatic Institution' in Eva Brems (ed), *Conflicts Between Fundamental Rights* (Intersentia, 2008) 169.

96 Konrad Lachmayer and Normann Witzleb, 'The Challenge to Privacy from Ever Increasing State Surveillance: A Comparative Perspective' (2014) 37 *University of New South Wales Law Journal* 748, 772.

97 Clifford Shearing and Jennifer Wood, 'Nodal Governance, Democracy, and the New "Denizens"' (2003) 30 *Journal of Law and Society* 400.

biometrics requires technical knowledge, resources, and the power to advocate for individual rights against strong claims to protect the community from crime and terrorism. For this reason it is argued than an independent statutory agency with adequate powers and resourcing would be the most suitable option for strengthening biometrics oversight in Australia. Further, it is important to consider international developments to ensure international best practice is adopted within Australia.

Regulation requires consideration of the competing demands between actors, including tensions between individual privacy and collective security objectives. Ayres and Braithwaite[98] and Braithwaite[99] propose 'pyramids of supports and of sanctions'[100] seeking to incorporate regulatory and oversight strategies at multiple levels. At the bottom level of the regulatory pyramid, support is provided for self-regulation, moving toward civil and criminal sanctions at higher levels, enforced by independent regulators. Within law enforcement contexts it has been argued that self-regulation alone is unworkable, as there are no incentives for police to self-regulate the collection and use of personal information for criminal investigations.[101] In the absence of a strong and independent regulator there is insufficient protection of individual rights. Therefore, regulation should occur at multiple levels, ultimately reinforced by independent oversight at the top levels of the responsive regulatory pyramid.

As the NBFMC will be established through information sharing agreements between agencies, rather than through the introduction of new or amended Commonwealth legislation, existing oversight and scrutiny measures will not be initiated. Parliamentary mechanisms exist to oversee new powers where they are introduced through legislation, including various committees and the Senate estimates process.[102] However, in this instance, normal parliamentary review processes will not occur, unless the issue is referred to a specific committee, as there is no Commonwealth legislation to review. Increased information sharing and interoperability of information systems is justified as a technological, and as such politically neutral, development. At the same time, this technocratic rationale overshadows implications for individual rights, and the need for greater regulation and oversight.[103] While considerable developments in the use and scale

98 Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992).

99 John Braithwaite, 'Fasken Lecture: The Essence of Responsive Regulation' (2011) 44 *University of British Columbia Law Review* 475, 475.

100 Ibid.

101 Sabrina A Lochner, 'Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans' (2013) 55 *Arizona Law Review* 201, 229–30.

102 Committees with a mandate relevant to the issues described in this paper include the Senate Standing Committee for the Scrutiny of Bills, the Senate Standing Committees on Legal and Constitutional Affairs, the Parliamentary Joint Committee on Intelligence and Security, the Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity, and the Parliamentary Joint Committee on Human Rights. These committees have the power to inquire into issues referred to a committee and make recommendations, including whether a specific bill should be passed. See also Australian Law Reform Commission, above n 74, ch 33.

103 See generally Paul De Hert and Serge Gutwirth, 'Interoperability of Police Databases within the EU: An Accountable Political Choice?' (2006) 20 *International Review of Law, Computers & Technology* 21.

of AFRT have already occurred, urgent policy consideration is required to address the regulatory shortcomings. We address this by examining current oversight mechanisms in Australia, and internationally, to gain insights into regulatory shortfalls and means to address these.

A Oversight Mechanisms in Australia

The OAIC is a statutory agency within the Commonwealth Attorney-General's portfolio responsible for providing advice, reviewing complaints, conducting investigations and monitoring compliance in relation to the federal *Privacy Act*.[104] At present, the OAIC has three functions including privacy, freedom of information ('FOI') and government information policy.[105]

There is a long history concerning the development of the OAIC and amalgamation of the former Privacy Commissioner. Initially, in 1989, the Privacy Commissioner, located within the Australian Human Rights and Equal Opportunity Commission (now Australian Human Rights Commission ('AHRC')), was responsible for administering the *Privacy Act*.[106] The Privacy Commissioner was separated from the AHRC in 2000,[107] and amalgamated with the OAIC in 2010. This office consists of the Australian Information Commissioner, with two other statutory offices comprising of the Freedom of Information Commissioner and Privacy Commissioner.[108] There have been recent attempts by the Australian Government to abolish the OAIC and funding to the OAIC has been reduced in recent years.[109] There are also questions in relation to independence as this office is located within the portfolio of the Attorney-General's Department, the same department responsible for policy development

104 Office of the Australian Information Commissioner, *About Us* <https://www.oaic.gov.au/about-us/>.

105 Established under the *Privacy Act 1988* (Cth) pt IV div 2, *Freedom of Information Act 1982* (Cth) s 8F, and the *Australian Information Commissioner Act 2010* (Cth) pt 2 div 3.

106 Office of the Australian Information Commissioner, *History of the Privacy Act* <https://www.oaic.gov.au/about-us/who-we-are/history-of-the-privacy-act>; Roger Clarke, *A History of Privacy in Australia* (8 January 2002) <http://www.rogerclarke.com/DV/OzHistory.html>.

107 *Privacy Amendment (Office of the Privacy Commissioner) Act 2000 (Cth)*.

108 *Australian Information Commissioner Act 2010* (Cth) s 6. Timothy Pilgrim is currently both the Australian Information Commissioner and the Australian Privacy Commissioner. One person currently administers the statutory functions of the Australian Information Commissioner and the Privacy Commissioner. Timothy Pilgrim has been appointed on a series of short term contracts to fulfill these roles: George Brandis, 'Reappointment of Timothy Pilgrim as Australian Privacy Commissioner' (Media Release, 21 August 2015) <https://www.attorneygeneral.gov.au/Mediareleases/Pages/2015/ThirdQuarter/21-August-2015-Reappointment-of-Timothy-Pilgrim-as-Australian-Privacy-Commissioner.aspx>; Leanne O'Donnell, 'Government Haste Lays Waste to Consultation' (2015) 25(23) *Eureka Street* 63, 65.

109 Office of the Australian Information Commissioner, 'Australian Government's Budget Decision to Disband the OAIC' (Statement, 15 May 2015) <https://www.oaic.gov.au/media-and-speeches/statements/australian-government-s-budget-decision-to-disband-oaic>; Paris Cowan, 'Revived OAIC to be "Leaner"', *iTnews* (online), 4 May 2016 <http://www.itnews.com.au/news/revived-oaic-to-be-leaner-419051>; John Hilvert, 'Information Commissioner Out as Privacy/FOI Office Shut Down', *iTnews* (online), 14 May 2014 <http://www.itnews.com.au/news/information-commissioner-out-as-privacyfoi-office-shut-down-385355>; Markus Mannheim, 'Freedom of Information Law Overseen by One Man Working From Home', *The Canberra Times* (online), 11 December 2014 <http://www.canberratimes.com.au/national/public-service/freedom-of-information-law-overseen-by-one-man-working-from-home-20141210-124rc6.html>.

regarding the NFBMC.[110] The hostility of the Australian Government to the OAIC and Privacy Commissioner has compounded the regulatory gaps in matters of privacy in Australia.[111]

Australian states and territories also have relevant legislation, and in most cases, Information and Privacy Commissioners.[112] The OAIC and its state and territory equivalents have broad authority in the area of biometrics. However, the complex nature of biometric information, coupled with the way it is used by law enforcement and security agencies, and continuing developments within this area, indicate the OAIC may need additional resources, specialisation and responsibilities in biometrics in order to effectively govern new developments.[113] It is important to note that the OAIC does not have a specific function or officer to oversee or regulate the collection, retention and use of biometric information. This means that at present in Australia no biometric-specific oversight mechanisms exist.[114]

B Oversight Mechanisms in the United Kingdom

Internationally, independent statutory commissioners have demonstrated an ability to limit the scope of AFRT and respond to concerns related to consent, retention and use of biometric information. For example, the UK has created a

---

110 Richard Mulgan, 'The Slow Death of the Office of the Australian Information Commissioner', *The Canberra Times* (online), 1 September 2015 <http://www.canberratimes.com.au/national/public-service/the-slow-death-of-the-office-of-the-australian-information-commissioner-20150826-gj81dl.html>. Funding was initially reduced within the 2014–15 Budget to coincide with the proposed abolition of the OAIC, although this decision was reversed in the 2015–16 and 2016–17 Budgets: Mary Anne Neilsen, 'Office of the Australian Information Commissioner: Reinstatement of Ongoing Funding' (Budget Review 2016–17, Parliamentary Library, Parliament of Australia, 2016).

111 It is also worth noting that the position of the Independent National Security Legislation Monitor, a similar oversight position in regulating security legislation, was left vacant for an extended period of time with threat of abolition during key debates around the 2014 tranche of national security legislation as described above: Roger Gyles, 'INSLM Annual Report 2014 – 2015' (Annual Report, Independent National Security Legislation Monitor, 7 December 2015) 1 <https://www.inslm.gov.au/sites/default/files/publications/inslm-annual-report-2015.pdf>; Jessie Blackbourn and Nicola McGarrity, 'The Independent Security Monitor's Unfinished Work', *Inside Story* (online), 3 April 2014 <http://insidestory.org.au/the-independent-security-monitors-unfinished-work>.

112 For example, in New South Wales there is the NSW Information and Privacy Commission, and in Queensland there is the Queensland Office of the Information Commissioner: Office of the Australian Information Commissioner, *Other Privacy Jurisdictions* <https://www.oaic.gov.au/privacy-law/other-privacy-jurisdictions>. State and territory privacy protection includes, for example: *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2009* (Qld); *Personal Information Protection Act 2004* (Tas); *Privacy and Data Protection Act 2014* (Vic).

113 During the 2016 Australian Federal Election campaign the Australian Greens called for a similar expansion of regulatory oversight via a Digital Rights Commissioner, proposed within the framework of the Australian Human Rights Commission: Australian Greens, *A Digital Rights Commissioner* <http://greens.org.au/digital-rights-commissioner>.

114 See Victorian Law Reform Commission, *Surveillance in Public Places*, Final Report No 18 (2010) ch 3. The Victorian Law Reform Commission conducted an inquiry into surveillance in public places recommending that an independent regulator be established to provide oversight of public surveillance, and that the Victorian Parliament enact new laws promoting the responsible use of surveillance devices in public places. The report did not consider the surveillance practices of police and security agencies, instead recommending that they be considered separately, which has not occurred. This is related to the use of AFRT integrated with CCTV in public places.

Commissioner for the Retention and Use of Biometric Material ('Biometrics Commissioner').[115] The Biometrics Commissioner was established under the *Protection of Freedoms Act 2012* (UK) c 9, introduced following the precedent *Marper* case, to ensure there was an office responsible for governing the retention and use of biometric information in the UK. The mandate of the Biometrics Commissioner is to regulate the use of biometric information, provide protection from disproportionate enforcement action, and limit the application of surveillance and counter-terrorism powers.[116] The UK Biometrics Commissioner's primary responsibilities involve reviewing the collection, use and retention of DNA evidence and fingerprints for law enforcement and national security purposes.[117]

The UK Biometrics Commissioner 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 Commissioner.[118] However, the Biometrics Commissioner's powers do not presently extend to other forms of biometric information other than DNA or fingerprints (and therefore the current powers do not include developments associated with AFRT).[119] However, a recent report on current and future uses of biometrics in the UK recommended that the statutory responsibilities of the Biometrics Commissioner 'be extended to cover, at a minimum, the police use and retention of facial images'.[120] Regardless, the UK Biometrics Commissioner has criticised the increasing collection of facial templates and use of AFRT in the UK PNC, without regard to the *RMC* ruling concerning the retention of photographs of those who have not been convicted of an offence, as described above.[121] The Biometrics Commissioner has expressed concern about insufficient oversight of AFRT before it became operational:

> I am concerned at the absence of any substantial progress in relation to these matters [AFRT and retention of photographs]. Among other things … I am concerned that the considerable benefits that could be derived from the searching of custody images on the PND [PNC] may be counterbalanced by a lack of public confidence in the way in which the process is operated, by challenges to its lawfulness and by fears of 'function creep'. … similar – but even more difficult – issues seem almost certain to arise in the near future in connection with the wider sharing of biometric information among organs of the state and the automated

115 *Protection of Freedoms Act 2012* (UK) c 9, s 20.

116 *Protection of Freedoms Act 2012* (UK) c 9, s 20.

117 *Protection of Freedoms Act 2012* (UK) c 9, s 20.

118 *Protection of Freedoms Act 2012* (UK) c 9, ss 20–1. See also Office of the Biometrics Commissioner, *About Us* <https://www.gov.uk/government/organisations/biometrics-commissioner/about>.

119 This highlights challenges associated with delineating clear roles, and questions about whether the mandate of a biometrics commissioner should be modality neutral and concerned with personal identifiers in general, extending the role to data protection. However, this expanded remit would potentially encroach into the operational boundary of the Information Commissioner's Office (the Australian equivalent is discussed below).

120 House of Commons Science and Technology Committee, Parliament of the United Kingdom, *Current and Future Uses of Biometric Data and Technologies* (2015) 34.

121 Alastair R MacGregor, 'Annual Report 2015: Commissioner for the Retention and Use of Biometric Material' (Annual Report, Office of the Biometrics Commissioner, December 2015) 101–3.

> searching of other Government-run databases. My hope is that those issues will be addressed with a rather greater degree of urgency.[122]

C Oversight Mechanisms in Germany

Germany provides further examples of oversight mechanisms that have demonstrated success in reviewing and limiting the use of AFRT by private companies. The Hamburg Commissioner for Data Protection and Freedom of Information ('Hamburg Commissioner') asserted that Facebook's automated photo tagging feature violated the European Union Data Protection Directive and the *Bundesdatenschutzgesetz* [Federal Data Protection Act] (Germany) 20 December 2009, BGBI I, 1990, 2954.[123] The Hamburg Commissioner requested Facebook deactivate the facial recognition feature and delete all stored biometric information collected without prior active consent (rather than retrospective opt-out). Following the Hamburg Commissioner's lead, the Irish Office of the Data Protection Commissioner ('Irish Commissioner') subsequently audited Facebook making a number of recommendations in relation to AFRT.[124] Most significantly, the Irish Commissioner stated that Facebook 'should have handled the implementation of this feature in a more appropriate manner' and recommended that measures be implemented to ensure it obtains user consent.[125] In response, Facebook deleted the facial recognition templates that had been collected and suspended creating new templates for European Union ('EU') citizens, effectively disabling AFRT in the EU.

D Oversight Mechanisms in the United States

Another oversight mechanism involves independent government accountability or audit offices responsible for conducting inquiries into police use of new technologies including biometric identification technologies. For example, the US Government Accountability Office ('GAO') recently conducted an inquiry into the Federal Bureau of Investigation's ('FBI') use of AFRT, reporting on key issues and making six recommendations. In May 2016 the GAO submitted a report to the Subcommittee on Privacy, Technology and the Law, and the Committee on the Judiciary in the US Senate.[126] This report was released at the same time the FBI applied to have the Next Generation Identification –

---

122 Ibid 103 [344] (citations omitted).

123 See Welinder, above n 21 for a review of this Act and the European Union Data Protection Directive and Facebook's use of AFRT. The Federal Data Protection Act (Germany) requires consent to collect, process and use personal information, particularly sensitive and biometric information. See also Bunn, above n 23.

124 The Irish Office of the Data Protection Commissioner conducted this audit, as this is where Facebook's European Headquarters are located.

125 Data Protection Commissioner, 'Facebook Ireland Ltd: Report of Re-Audit' (Audit Report, Office of the Data Protection Commissioner, 21 September 2012) 8–9.

126 United States Government Accountability Office, 'Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy' (Report to the Ranking Member, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, May 2016).

Interstate Photo System ('NGI-IPS')[127] exempt from the *Privacy Act of 1974*, 5 USC § 552a (2010).[128] This exemption would mean individuals are unable to confirm whether their biometric information is stored in the NGI-IPS or shared between agencies. The GAO investigated the FBI's compliance with US privacy protections, and the FBI's assessment of accuracy of AFRT. The GAO found that the FBI did not update nor release PIAs when the NGI-IPS was significantly upgraded; did not publish a Systems of Records Notice ('SORN') as required by US law until after the GAO review was completed; and failed to complete audits to oversee the use of the NGI-IPS.[129] A further finding related to the FBI's limited testing of the system's identification accuracy, risking the inclusion of innocent people in FBI investigations. The GAO made a number of recommendations to ensure the NGI-IPS is used in a way that is compliant with privacy protections and existing policy. Specifically, the GAO recommended that the Attorney-General review the PIA process to ensure PIAs are conducted and published prior to changing the NGI-IPS, assessing the SORN process to determine why this was not completed, to conduct regular audits to confirm the NGI-IPS is being used in a way that is compliant with policy and privacy protections, and to assess the accuracy of identification.[130]

The oversight and accountability models adopted in the UK, US, Germany and Ireland provide guidance about how independent oversight bodies can operate to govern new police technology, including AFRT. In contrast with the UK Biometrics Commissioner and the US GAO, the latter examples related specifically to the regulation of a private company. Certainly, there are intersecting public and private sector implications for the regulation of biometric technology, particularly as information collected by private organisations can be obtained for law enforcement purposes.[131] In Australia, there is currently a

---

127 The NGI-IPS is the FBI's primary biometric database containing 100 million individual records, including fingerprints, facial templates and photographs, iris scans and palm prints: Federal Bureau of Investigations, 'Next Generation Identification. FBI Announces Biometrics Suite's Full Operational Capability', *FBI News* (online), 23 September 2014 <https://www.fbi.gov/news/stories/fbi-announces-biometrics-suites-full-operational-capability>. See generally Ernest J Babcock, *Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System* (September 2015) Federal Bureau of Investigation <https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/interstate-photo-system>. The NGI-IPS includes a database of 30 million photographs representing 16.9 million individuals: ibid 10 n 23.

128 Ellen Nakashima, 'FBI Wants to Exempt its Huge Fingerprint and Photo Database from Privacy Protections', *The Washington Post* (online), 1 June 2016 <https://www.washingtonpost.com/world/national-security/fbi-wants-to-exempt-its-huge-fingerprint-and-photo-database-from-privacy-protections/2016/05/31/6c1cda04-244b-11e6-8690-f14ca9de2972_story.html>.

129 United States Government Accountability Office, above n 126, 18–21.

130 Ibid 34.

131 This article focuses on public sector developments and regulation; however there are also concerns about the expanding use of AFRT by private sector companies including Facebook and Google. A holistic approach to regulating AFRT should consider the private sector. One US jurisdiction has introduced legislation governing the collection, retention and use of biometric information by private companies. The Illinois *Biometric Information Privacy Act*, 740 Ill Comp Stat 14/1-99 (2008) regulates the collection, use, storage, retention and use of biometric information. Section 15(a) requires all private businesses to 'develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information'. Section 20 provides for injunctive relief or damages if an individual's data is compromised. A number of cases have been brought

regulatory gap and a limited governance framework concerning new and emerging technologies, before they are implemented and become operational. Given the above examples, prospects for biometrics oversight in Australia could involve strengthening or expanding the remit and functions of the OAIC in relation to biometric information, or the creation of a new independent statutory Biometrics Commissioner for Australia, similar to the Biometrics Commissioner model adopted in the UK.

E Recommendations

Given the significant and longstanding limitations in Australia's human rights and privacy framework, and on the basis of the findings of the international review of biometrics specific regulatory and oversight practices, a specific Commonwealth office holder, with statutory responsibilities in relation to the oversight of the collection, retention and use of biometric information should be considered. A strong, independent and sufficiently funded regulatory authority is needed to meet challenges posed by new technologies, rapid information sharing and the ease of identification provided by biometrics. Given the expanding use of biometric information by law enforcement and security agencies, and new initiatives such as the NFBMC, regulation of biometric information in Australia should be subject to a more intensive regulatory regime. Consistent with the paradigm of responsive regulation, regulatory functions should occur at multiple levels from support in the responsible use of biometric information, through to conducting audits, and applying sanctions. For example, this office holder could have powers to develop policies in relation to the collection, retention, storage, use and sharing of biometric information, assess police applications to retain biometric information, review agency compliance with relevant legislation (or advocate for the introduction of legislation or new privacy protections), provide advice and support to government when developing new policies, audit biometric databases, and review new technology prior to implementation. Another function could involve establishing a code of conduct governing biometric information, providing avenues for 'enforced self-regulation'.[132] Additional functions could include a public education and engagement role, including receiving,

against companies under the protections established in this law. For example, in June 2015 Brian Norberg sought damages from Shutterfly Inc (which operates a range of services for digital photo storage, sharing and printing), arguing that Shutterfly's use of AFRT occurred without consent, violating the Act. In April 2016, Shutterfly Inc settled with Norberg for an undisclosed amount: Kim Janssen, 'Shutterfly Settles Facial Recognition Lawsuit with Man Who Claimed Privacy Violation', *Chicago Tribune* (online), 15 January 2017 <http://www.chicagotribune.com/business/ct-facial-recognition-lawsuit-0413-biz-20160412-story.html>. Presently there is ongoing litigation between a group of Illinois citizens and Facebook in relation to Facebook's use of AFRT about whether this contravenes the statute. A May 2016 decision of the United States District Court found in favour of the citizens: *Re Facebook Biometric Information Privacy Litigation*, 185 F Supp 3d 1155 (ND Cal, 5 May 2016) (Donato J). Finally, in March 2016, Lindabeth Rivera filed a class action complaint against the use of AFRT in Google's cloud based Google Photos. At the time of writing this litigation is ongoing. For a brief summary see Christopher Zara, 'Google Gets Sued Over Face Recognition, Joining Facebook and Shutterfly in Battle Over Biometric Privacy in Illinois', *International Business Times* (online), 4 March 2016 <http://www.ibtimes.com/google-gets-sued-over-face-recognition-joining-facebook-shutterfly-battle-over-2330278>.

132 See Ayres and Braithwaite, above n 98, ch 4.

investigating and responding to enquiries or complaints from the public. This would support the responsible collection, sharing and use of biometric information in Australia (and – aligned with international standards – the personal information of those who have not been convicted of an offence). In the context of the long history of funding cuts to, and attempted abolition of, the OAIC, political will and commitments to ongoing funding are necessary to ensure sufficient resources to effectively undertake these functions. Given the limitations of the Australian privacy framework (ie, absence of constitutional privacy protections and no cause of action for serious invasion of privacy) a stronger regulatory and oversight regime is required. While increasing oversight is an important avenue for the regulation of new biometric technology, other measures (for example, introducing legal rights to enforceable remedies for serious invasions of privacy) should also be considered with the overall objective of addressing the significant gaps in Australia's privacy framework.

V CONCLUSION

This article has reviewed developments and issues associated with AFRT, including some of the ways that information is increasingly being integrated across multiple systems and shared between agencies as per the 'surveillant assemblage'.[133] AFRT is a significant development as it enables the extraction and digitisation of biometric information from routinely collected and readily available photographs, facilitating information sharing and integration. This poses new challenges for the protection of individual privacy rights, particularly in the Australian context where there is an absence of any constitutional protections or cause of action for serious invasions of privacy. However, the development, implementation and application of AFRT have not been matched with increased protections or oversight. A national facial recognition capability will be created without the introduction of new law, effectively bypassing parliamentary scrutiny. While this article has focused specifically on AFRT, issues of privacy protection and questions of oversight have broader implications for existing and emerging surveillance technologies. It is expected that with ongoing developments in technology, databases will expand and information sharing will become more efficient. Current privacy protections in Australia are at risk of becoming obsolete as a result of law enforcement exemptions and a tendency to balance individual rights against notions of collective security. Therefore, there is a need to consider the adequacy of existing privacy protections and oversight mechanisms before new technologies are implemented. Presently in Australia there is a regulatory gap: an absence of an effective regulatory regime or framework to govern the use of biometric and police technologies. This review of recent developments, case law, and international regulatory approaches has identified the development of a Biometrics Commissioner or similar independent office holder with specialisation in

133 Haggerty and Ericson, above n 7.

biometrics as international best practice, suggesting the need for a similar approach in Australia. The model that has been adopted in the UK, with the addition of powers in relation to AFRT, would be an important step towards protecting individual rights in the context of the expanding use of biometric information by law enforcement. In order to be effective this office must be sufficiently funded to be able to perform the required regulatory functions.