FACIAL RECOGNITION TECHNOLOGY, PRIVACY AND ADMINISTRATIVE LAW

HARRY ANIULIS*

This article has two broad threads: it is descriptive of recent developments regarding facial recognition technology ('FRT'), and underpinned by a normative argument that there is utility in considering privacy regulation from an administrative law perspective. In making this argument, FRT is used to provide tangible illustrations of the difficulties in the existing framework for privacy protection. This article examines the existing framework, the substantive issues FRT can present (namely, infringement of the right to privacy and biased outcomes) and specific uses of FRT in Australia. Corresponding with these topics, the article adopts each of the 'administrative law values' articulated by Chief Justice French as heads for discussion. Lastly, proposals for reform are evaluated.

I INTRODUCTION

There have been growing calls for bans and moratoriums on the use of facial recognition technology ('FRT'). Internationally, moratoriums have been imposed in multiple United States ('US') jurisdictions,[1] and are being contemplated in the United Kingdom ('UK') and European Union.[2] IBM, Amazon, Microsoft and Google each banned the sale of the technology, though on different terms. In Australia, several organisations have called for a halt to the usage of FRT until an appropriate regulatory framework is established.[3] Implicit in these calls is

* BCom, LLB (Hons) (Monash), BCL Candidate (Oxon). I thank Dr Colin Campbell and the anonymous reviewers for their helpful comments. All errors remain my own.

1 'State Facial Recognition Policy', *Electronic Privacy Information Center* (Web Page) <https://epic.org/state-policy/facialrecognition/>.

2 See Automated Facial Recognition Technology (Moratorium and Review) Bill 2019 (UK); Samuel Stolton, 'Commission Will "Not Exclude" Potential Ban on Facial Recognition Technology', *Euractiv* (online, 3 September 2020) <https://www.euractiv.com/section/data-protection/news/commission-will-not-exclude-potential-ban-on-facial-recognition-technology/>.

3 See, eg, Australian Human Rights Commission, 'Human Rights and Technology' (Discussion Paper, December 2019) 104 (Proposal 11) ('AHRC Discussion Paper'). This was supported by multiple submitters, including: the Office of the Victorian Information Commissioner; the Australian Privacy Foundation; Queensland Council for Civil Liberties; Electronic Frontiers Australia; Liberty Victoria; New South Wales Council for Civil Liberties; the AI Now Institute; the Allens Hub for Technology, Law and Innovation; the Castan Centre for Human Rights Law; and the New South Wales Bar Association.

an assertion that the current privacy regime is inadequate to address these new challenges.

This article has two broad threads: it is descriptive of recent developments regarding FRT, and underpinned by a normative argument that there is utility in considering privacy regulation from an administrative law perspective. In making this argument, FRT is used to provide tangible illustrations of the difficulties in the existing framework. Part II explains how FRT works, and why it is unlike previous privacy-invasive technologies. Part III discusses why it is useful to consider privacy and FRT from a perspective oriented around administrative law. In Part IV, this article examines the existing Australian framework for privacy protection, ie, the *Privacy Act 1988* (Cth) ('*Privacy Act*') and the Office of the Australian Information Commissioner ('OAIC'); the substantive issues FRT can present – namely, infringement of the right to privacy and biased outcomes; and specific uses of FRT in Australia. Corresponding with these topics, the article adopts each of the 'administrative law values' articulated by Chief Justice French as 'useful heads for the discussion'.[4] In Part IV proposals for reform are evaluated.

It is acknowledged at the outset that this article takes an expansive view of administrative law, extending beyond judicial review to encompass the law of public administration. Anchoring the analysis to FRT permits targeted examination of some of the more abstract issues relevant to the current administrative law discourse, such as the enforceability of human rights, algorithmic accountability, and automated decision-making. There 'is [a] growing realisation of a significant interface' between artificial intelligence ('AI'), privacy and administrative law.[5] This interface challenges orthodox applications of foundational concepts. For example, authors have examined whether an algorithm can truly make a 'decision' for jurisdictional purposes,[6] or provide adequate reasons.[7] FRT, however, has largely sat at the periphery of this discourse. This lack of attention is understandable – it has been suggested that automation presents a graver threat for decisions with a discretionary element, and where outcomes exist upon a continuum rather than as a binary choice (eg, match or no match).[8] However, it has also been said, perhaps self-evidently, that the threat of automation depends on the seriousness of the consequences for the individuals affected.[9] Serious consequences flow from many

4 Chief Justice RS French, 'Administrative Law in Australia: Themes and Values Revisited' in Matthew Groves (ed), *Modern Administrative Law in Australia: Concepts and Context* (Cambridge University Press, 2014) 24, 48, 26 <https://doi.org/10.1017/CBO9781107445734.003> ('Themes and Values Revisited').

5 Carol Harlow and Richard Rawlings, 'Proceduralism and Automation: Challenges to the Values of Administrative Law' in Elizabeth Fisher, Jeff King and Alison L Young (eds), *The Foundations and Future of Public Law: Essays in Honour of Paul Craig* (Oxford University Press, 2019) 275, 293.

6 Justice Melissa Perry, 'iDecide: Administrative Decision-Making in the Digital World' (2017) 91(1) *Australian Law Journal* 29.

7 Will Bateman, 'Algorithmic Decision-Making and Legality: Public Law Dimensions' (2020) 94(7) *Australian Law Journal* 520.

8 Yee-Fui Ng et al, 'Revitalising Public Law in a Technological Era: Rights, Transparency and Administrative Justice' (2020) 43(3) *University of New South Wales Law Journal* 1041, 1049–50 <https://doi.org/10.53637/YGTS5583>.

9 Ibid 1049.

applications of FRT. Certain applications do not clearly involve a 'decision' in the jurisdictional sense.[10] Nevertheless, it will be argued that values underlying doctrinal administrative law concepts are of broader relevance in developing an appropriate framework to govern this technology. This article accepts the invitation that it is 'imperative to more closely scrutinise the interaction between the government's use of new technologies and administrative law frameworks … and public sector privacy laws'.[11]

It may be observed that there is a certain predictability to discussions about new privacy-invasive technologies. Characteristically, there is lament over Australia's lack of a statutory tort of invasion of privacy, or a human rights instrument at a federal level. There are references to discordant rates of technological and legal development, and to the 'unprecedented' nature of the technology at issue. And there are calls for legislative reform to address the challenges identified. Despite this predictability, many of the concerns voiced are no less sound simply because they have been dismissed before and society has accepted – or acquiesced in – the institutionalisation of technologies previously considered unpalatable.

II FRT

FRT is a biometric technology that typically utilises three parts: a camera to capture a digital image, a database of stored images for comparison, and an algorithm which creates a faceprint from the captured image and compares it with the database of images.[12] Critically, the camera and database are capable of substitution with a variety of sources, including: public surveillance technologies (such as closed-circuit television ('CCTV')), government databases (such as those

---

10 NB: Arguments could be raised that the decision should properly be characterised as the decision to use facial recognition technology ('FRT'), or decisions consequential upon a match. The Comprehensive Review of the Legal Framework of the National Intelligence Community ('Richardson Review') noted that 'the principles of administrative law… will shape [National Intelligence Community ('NIC')] agencies' development and implementation of AI. Although much of the NIC's intelligence work is not concerned with the making of administrative decisions, its work contributes to the making of such decisions': Dennis Richardson, Attorney-General's Department (Cth), *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Report, 4 December 2019) vol 3, 176 ('*Richardson Review Report*'). Many acts of intelligence officers are explicitly excluded from review under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) schedule 1(d) ('*AD(JR) Act*'). However, police officers and Australian Security Intelligence Organisation ('ASIO') staff have been held to be officers of the Commonwealth for the purposes of jurisdiction under section 75(v) of the *Australian Constitution*: see, eg, *Coward v Allen* (1984) 52 ALR 320; *Church of Scientology v Woodward* (1982) 154 CLR 25, 65 (Murphy J). The arguments for extending administrative law principles to law enforcement agencies have been further explored in the United States ('US'): see Christopher Slobogin, 'Policing as Administration' (2016) 165(1) *University of Pennsylvania Law Review* 91; Christopher Slobogin, 'Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine' (2014) 102(6) *Georgetown Law Journal* 1721, 1758–70.

11 Ng et al (n 8) 1051.

12 The process can be further divided into: (1) Compiling/using an existing database of images, (2) Facial image acquisition, (3) Face detection, (4) Feature extraction, (5) Face comparison, and (6) Matching: *R (Bridges) v Chief Constable of South Wales Police* [2020] 1 WLR 5037, 5043–4 [9] ('*Bridges*').

containing licence and passport information), and websites (such as Facebook). FRT is predominantly used for verification, identification or classification. Errors take the form of false positives (incorrectly matching a face) or false negatives (incorrectly rejecting a match).[13]

FRT presents unique challenges. Its potential pervasiveness derives from the combination of its capabilities, namely, it 'give[s] the government the ability to ascertain the identity (1) of multiple people; (2) at a distance; (3) in public space[s]; (4) absent notice and consent; and (5) in a continuous and on-going manner'.[14] FRT may be understood as converging characteristics of previous technologies within a single algorithm. With sufficient CCTV infrastructure, it effectively permits tracking across locations, akin to global positioning systems. It can identify individuals, like DNA and fingerprint matching, but without the need for physical contact and processing time. Developments are underway for automated lip-reading capacities to enable the interpretation of speech.[15] However, unlike DNA or fingerprint matching, Global Positioning System and telecommunications interception devices, no legislation specifically governs the use of FRT. Whilst the risks associated with FRT use are certainly contextual, it is generally accepted that identification is more risky than verification or uses that simply distinguish faces from other objects.[16]

FRT's widespread adoption magnifies concerns about the dangers of ubiquitous surveillance[17] and the issue of protecting privacy in public places.[18] It has been said that government surveillance 'distorts the power relationships between the

13 For an accessible overview of the technical operation of FRT systems, see Joy Buolamwini et al, *Facial Recognition Technologies: A Primer* (Report, 29 May 2020).

14 Laura K Donohue, 'Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age' (2012) 97 *Minnesota Law Review* 407, 415.

15 Triantafyllos Alfouras et al, 'Deep Audio-Visual Speech Recognition' [2018] *IEEE Transactions on Pattern Analysis and Machine Intelligence* 30582526:1–11 <https://doi.org/10.1109/TPAMI.2018.2889052>.

16 See also Erik Learned-Miller et al, *Facial Recognition Technologies in the Wild: A Call for a Federal Office* (White Paper, 29 May 2020) 23–30; Amba Kak, 'The State of Play and Open Questions for the Future' in Amba Kak (ed), *Regulating Biometrics: Global Approaches and Urgent Questions* (AI Now Institute, September 2020) 16, 30 ('State of Play').

17 See, eg, Neil M Richards, 'The Dangers of Surveillance' (2013) 126(7) *Harvard Law Review* 1934; Konrad Lachmayer and Normann Witzleb, 'The Challenge to Privacy from Ever Increasing State Surveillance: A Comparative Perspective' (2014) 37(2) *University of New South Wales Law Journal* 748; Julie E Cohen, 'What Privacy Is For' (2013) 126(7) *Harvard Law Review* 1904; Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79(1) *Washington Law Review* 119; David J Phillips, 'Beyond Privacy: Confronting Locational Surveillance in Wireless Communication' (2003) 8(1) *Communication Law and Policy* 1 <https://doi.org/10.1207/S15326926CLP0801_01>; Christopher Slobogin, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity' (2002) 72(1) *Mississippi Law Journal* 213 <https://doi.org/10.2139/ssrn.364600>; Kevin D Haggerty and Richard V Ericson, 'The Surveillance Assemblage' (2000) 51(4) *British Journal of Sociology* 605 <https://doi.org/10.1080/00071310020015280>; Alan Westin, *Privacy and Freedom* (Ig Publishing, 1967) 31.

18 See, eg, Moira Paterson, 'Regulating Surveillance: Suggestions for a Possible Way Forward' (2018) 4(1) *Canadian Journal of Comparative and Contemporary Law* 193; Moira Paterson, *Freedom of Information and Privacy in Australia: Information Access 2.0* (LexisNexis Butterworths, 2nd ed, 2015) 26 ('*FOI and Privacy in Australia*'); Moira Paterson, 'Surveillance in Public Places: the Regulatory Dilemma' in Normann Witzleb et al (eds), *Emerging Challenges in Privacy Law* (Cambridge University Press, 2014) 201, 201–55 <https://doi.org/10.1017/CBO9781107300491.015>.

watcher and the watched, enhancing the watcher's ability to blackmail, coerce and discriminate against the people under its scrutiny'.[19] In 1983, the Australian Law Reform Commission ('ALRC') observed that privacy interests were under threat from, inter alia, the extension of powers granted to administrative officials, allowing an ever-increasing range of persons in addition to police to enter the 'personal place' or 'personal space', to interfere with private communications, to engage in secret surveillance or to gain access to a personal file and rapid development of technological means for penetrating 'place' and 'space'.[20] Despite the subsequent passing of the *Privacy Act* these concerns are equally apposite now. Arguably in current practice, the degree of protection against a technology 'often does not turn on how problematic or invasive it is, but on the technicalities of how the surveillance fits into the law's structure'.[21]

The academic origins of the right to privacy are commonly traced to Samuel Warren and Louis Brandeis.[22] Notwithstanding the subsequent disagreement over privacy's definitional boundaries,[23] this article can proceed without committing to a particular definition. The *Privacy Act* does not define privacy, and the ALRC has recognised that 'privacy is not less valuable or deserving of legal protection simply because it is hard to define'.[24] Avoiding its definitional instability is arguably desirable. Instead, as Daniel Solove advocates, '[w]e should conceptualize privacy by focusing on the specific types of disruption and the specific practices disrupted rather than looking for the common denominator that links all of them'.[25]

III PRIVACY AND ADMINISTRATIVE LAW

Though privacy law is commonly accepted to be an independent area of law deserving of specialised scholarship, tracing its Australian history reveals administrative law origins. The *Privacy Act* has been described as a subset of

19 Richards (n 17) 1936.

20 Australian Law Reform Commission, *Privacy* (Report No 22, December 1983) vol 1, 37 ('*ALRC Report 22*').

21 Daniel J Solove, 'Reconstructing Electronic Surveillance Law' (2003) 72(6) *George Washington Law Review* 1701, 1740 <https://doi.org/10.2139/ssrn.445180>.

22 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193 <https://doi.org/10.2307/1321160>.

23 See Daniel Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477 <https://doi.org/10.2307/40041279>; David Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29(1) *Melbourne University Law Review* 131; Daniel Solove, 'Conceptualizing Privacy' (2002) 90(4) *California Law Review* 1087 <https://doi.org/10.2307/3481326> ('Conceptualizing'); Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89(3) *Yale Law Journal* 421, 465 <https://doi.org/10.2307/795891>; Stanley Benn, 'The Protection and Limitation of Privacy' (1978) 52(11) *Australian Law Journal* 601; Charles Fried, 'Privacy' (1968) 77(3) *Yale Law Journal* 475 <https://doi.org/10.2307/794941>; Edward Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39(6) *New York University Law Review* 962; William L Prosser, 'Privacy' (1960) 48(3) *California Law Review* 383 <https://doi.org/10.2307/3478805>.

24 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report No 123, September 2014) 31 ('*ALRC Report 123*').

25 Solove, 'Conceptualizing' (n 23) 1130. Cf Raymond Wacks, 'The Poverty of "Privacy"' (1980) 96(1) *Law Quarterly Review* 73.

broader reforms constituting the 'new administrative law'[26] and positioned as an administrative law requirement.[27] Indeed, a number of contemporary Australian texts on administrative law have dedicated chapters to privacy.[28]

As understandings of – and threats to – privacy have developed, so too has the need to regulate both public *and* private entities. Relatedly, the threats posed by FRT are not isolated to use by governmental agencies, but can extend to the private sector. But as Chief Justice Allsop observed: '[p]ower is power, it might be said. Yet there is something super-added, something meaningful, sometimes something menacing in the presence of state authority'.[29] The power that FRT places in governmental hands takes on added significance for two primary reasons. First, the collective departments of government hold vast amounts of personal information that is (at least hypothetically) capable of being linked with one's face. Justice Kirby, recounting the reason why information rights were developed for the public sector, explained that '[t]his is natural, for it is in that sector that critical information affecting all citizens exists'.[30] Second, the increasing powers of officialdom render governmental deployment of FRT significant. As noted above, a driving force behind the introduction of the *Privacy Act* was the expansion of 'the government's claim to intrusive powers' and corresponding need for 'proper checks and impartial scrutiny if privacy is not to be unduly eroded'.[31] Additionally, 'individuals are rarely in a strong bargaining position when it comes to the collection and use of their personal information by government'.[32] In the UK, the former Biometrics Commissioner recently said:

> This rapid growth of both AI and biometrics has meant their use is being widely explored across both the public and private sectors … the new technologies are now part of high politics across government and not just a niche issue for policing

26 See, eg, Robin Creyke, 'The Performance of Administrative Law in Protecting Rights' in Tom Campbell, Jeffrey Goldsworthy and Adrienne Stone (eds), *Protecting Rights without a Bill of Rights* (Ashgate Publishing, 2006) 101, 110; Kim Rubenstein, 'Erring on the Side of Destruction? Administrative Law Practices Under the *Archives Act 1983* (Cth)' (1997) 4(2) *Australian Journal of Administrative Law* 78, 79.

27 See, eg, Greg Weeks, 'Attacks on Integrity Offices: A Separation of Powers Riddle' in Greg Weeks and Matthew Groves (eds), *Administrative Redress in and out of Courts*: *Essays in Honour of Robin Creyke and John McMillan* (Federation Press, 2019) 25; Attorney-General's Department (Cth), 'Australian Administrative Law' (Policy Guide, 2011) 6; John McMillan, 'Ten Challenges for Administrative Law' (2008) 61 *Australian Institute of Administrative Law Forum* 23, 23; John McMillan and Neil Williams, 'Administrative Law and Human Rights' in David Kinley (ed), *Human Rights in Australian Law: Principles, Practice and Potential* (Federation Press, 1998) 63, 68; Graham Greenleaf, 'Australian Approaches to Computerising Law: Innovation and Integration' (1991) 65(11) *Australian Law Journal* 677, 677.

28 See Robin Creyke et al, *Control of Government Action* (LexisNexis Butterworths, 5th ed, 2019) ch 20, 1171–94; Moira Paterson, 'Privacy' in Matthew Groves (ed), *Modern Administrative Law in Australia* (Cambridge University Press, 2014) 370 <https://doi.org/10.1017/CBO9781107445734.020>; LexisNexis, *Australian Administrative Law* (online at October 2020) (Chapter 8: Privacy Legislation).

29 Chief Justice James Allsop, 'Values in Public Law' (2017) 91(2) *Australian Law Journal* 118, 118 ('Values in Public Law').

30 Justice Michael D Kirby, 'Access to Information and Privacy: The Ten Information Commandments' (1987) 55(3) *University of Cincinnati Law Review* 745, 756 <https://doi.org/10.1016/0740-624X(86)90031-6>.

31 *ALRC Report 22* (n 20) vol 1, 38.

32 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 2, 1572 ('*ALRC Report 108*').

> and the Home Office, although the police use of technology will always require particular attention … the new technologies are developing at a speed that politics, government and legislation has not kept up with.[33]

The vast information held by government and the unparalleled powers exercised by public officials reinforce the appropriateness of focusing on FRT associated with governmental functions.[34] The ALRC in 1983 observed that privacy may be indirectly protected through an orthodox judicial review framework.[35] Ultimately though, it was recognised that the Ombudsman, Administrative Appeals Tribunal ('AAT') and judicial review 'are limited as protectors of "information privacy" because [that] is not their primary purpose'.[36] Hence the need to develop a specific statutory guardian for privacy protection – now called the OAIC. The OAIC is an independent statutory agency, which has privacy functions under the *Privacy Act*.[37] The OAIC fits within a theme of increasing recognition of the importance of non-judicial accountability mechanisms as 'the engine room of Australian administrative law'.[38] However, it should be noted that recognition of the importance of administrative infrastructures has a long history, with other authors having grappled with how law is made in the administrative state dating back as far as nineteenth-century Britain and its colonies.[39] Lessons can be learned from this history.

Arthurs rejects a narrow, centralist understanding of administrative law, instead asserting that its pluralistic nature should be appreciated. His contention is that administrative law has developed in light of the influence of different fields of social activity and technology, and that law and legal ideologies not only embody, but shape or create the values of the societies in which they operate.[40] He explains that administrators – 'carriers of legal values' – have been necessary in particular fields of activity where there is rapid technical innovation and unpredictable problems arising in the application of legislation.[41] He also acknowledges that 'all

---

33 Paul Wiles, 'Biometrics Commissioner's Address to the Westminster Forum' (Speech, Westminster Forum, 5 May 2020).

34 Note also that the Federal Government was the most complained about sector for privacy complaints in 2019–20: Office of the Australian Information Commissioner, *Annual Report 2019–20* (Report, 2020) 36.

35 For example, where personal information is an irrelevant factor taken into account in making a decision, or where requirements of natural justice protect information privacy interests: *ALRC Report 22* (n 20) vol 1, 375.

36 Ibid vol 1, 467.

37 *Australian Information Commissioner Act 2010* (Cth) section 9 definition of 'privacy function' also includes functions under the *Crimes Act 1914* (Cth) pt VIIC div 5; *Data-Matching Program (Assistance and Tax) Act 1990* (Cth) ss 12–14; *National Health Act 1953* (Cth) s 135AA; *Telecommunications Act 1997* (Cth) s 309.

38 Weeks (n 27) 29.

39 See Oliver MacDonagh, 'The Nineteenth-Century Revolution in Government: A Reappraisal' (1958) 1(1) *Historical Journal* 52 <https://doi.org/10.1017/S0018246X58000018>; HW Arthurs, *'Without the Law': Administrative Justice and Legal Pluralism in Nineteenth-Century England* (University of Toronto Press, 1985); Keally McBride, *Mr Mothercountry: The Man Who Made the Rule of Law* (Oxford University Press, 2016) <https://doi.org/10.1093/acprof:oso/9780190252977.001.0001>.

40 Arthurs' account traces the emergence of 'New Administrative Technology' to the *Factories Act 1833* and provision for inspectors to make rules, regulations and orders needed to implement the act – as representing 'a shift from the former reliance upon the criminal law to primary reliance upon administrative regulation': Arthurs (n 39) 105.

41 Arthurs (n 39) 156.

administrative activity has its roots in a statute', but that the 'normative language in regulatory statutes is often vague and uninformative'. In light of this, there is a compelling necessity for the administration to give meaningful specificity to such statutes and to create and embed norms within their instructional structure.[42] He concludes that '[h]ow to make norms into law in this sense is the secret of good administration. Beside this secret other issues pale into relative insignificance'.[43] It has recently been observed that failing to provide an account of the administrative landscape (which encompasses a diversity of administrative materials and institutions) limits understanding for the possible roles for law.[44] A detailed account of the OAIC will be provided in Part V(B).

IV ADMINISTRATIVE LAW VALUES

Recognising the interrelationship between privacy and administrative law is useful because foundational values of administrative law refined over decades can be revisited to provide guidance in addressing new challenges presented by FRT.[45] Australian courts have yet to evaluate FRT. The absence of Australian case law on FRT is part of the reason why a 'values' lens is useful to assess how Australia's privacy regime can respond to FRT. Justice French, writing extra-curially, lists the values of administrative law to be: *accountability*, *participation*, *accessibility*, *lawfulness*, *fairness*, *rationality*, *openness* and *good faith*.[46] These values can be understood as elements of administrative justice.[47] Aronson, Groves and Weeks have articulated a comparable list of 'ideals', acknowledging that 'judicial review is often marginal to the attainment of administrative law's ideals at the systemic level', and that other components of administrative law are often better suited to tackling these ideals.[48] Taggart similarly observed that administrative law values have transcended the limited and uncertain contours of judicial review 'to cast a long shadow over the recently levelled terrain of what was once called public

42 Ibid 202, 204.

43 Ibid 214.

44 Elizabeth Fisher, 'The Open Road? Navigating Public Administration and the Failed Promise of Administrative Law' in Elizabeth Fisher, Jeff King, Alison L Young (eds), *The Foundations and Future of Public Law* (Oxford University Press, 2020) 209, 227 <https://doi.org/10.1093/oso/9780198845249.003.0011>.

45 It has been argued some of these values originate in legislative reforms and are then affirmed by courts: see, eg, Mark Aronson, 'Public Law Values in the Common Law' in Mark Elliott and David Feldman (eds), *The Cambridge Companion to Public Law* (Cambridge University Press, 2015) 134, 145 <https://doi.org/10.1017/CCO9781139342551.008> ('Public Law Values').

46 Justice Robert French, 'Administrative Law in Australia: Themes and Values' in Matthew Groves and HP Lee (eds), *Australian Administrative Law: Fundamentals, Principles and Doctrines* (Cambridge University Press, 2007) 15, 16 <https://doi.org/10.1017/CCO9781139342551.008>. His Honour has restated these values elsewhere: Chief Justice Robert French, 'Public Law: An Australian Perspective' (Speech, Scottish Public Law Group, 6 July 2012) 16; French, 'Themes and Values Revisited' (n 4) 26.

47 French, 'Themes and Values Revisited' (n 4) 37.

48 Mark Aronson, Matthew Groves and Greg Weeks, *Judicial Review of Administrative Action and Government Liability* (Thomson Reuters, 6th ed, 2017) 4–5.

administration'.[49] Chief Justice French's list has been selected to guide this article as there is significant commonality across it and the various taxonomies of values suggested by other authors.[50] Moreover, it is not the purpose of this article to evaluate the most 'correct' list (assuming such an endeavour is even possible).

Recourse to overarching values carries with it an inevitable risk of uncertainty. The precise meaning of these values is not settled. One might question whether they could provide a workable way to understand or apply a notion such as administrative justice.[51] However, these values are not designed to displace existing legal requirements or to refashion older doctrines under new labels. Indeed, as Chief Justice Allsop observed extra-curially, '[a]dministrative law is an area in which legal theory *and* values play vital roles'.[52] The utility of considering these values here is twofold. First, they provide a thematic backdrop against which the current issues associated with FRT may be explored. Specifically, these values will be used to examine the existing framework for privacy protection (namely the *Privacy Act* and the OAIC), and applied to case studies concerning current applications of FRT (namely Live Automated Facial Recognition technology by the police in public spaces, the Australian Government's National Facial Biometric Matching Capability, and the private company Clearview AI). Second, they are instructive as first principles that can assist with the development of future reforms.

The importance of administrative law values in addressing novel challenges has been recognised by various authors. Harlow and Rawlings posit 'the idea of procedures as a repository for values, and of values as an important, though often subliminal, driver of administrative procedure'[53] describing them as 'the compass points for contemporary public administration'.[54] McMillan has discussed the

---

49 Michael Taggart, 'The Province of Administrative Law Determined?' in Michael Taggart (ed), *The Province of Administrative Law* (Hart Publishing, 1997) 1, 4 ('The Province of Administrative Law Determined').

50 See, eg, Chief Justice Allsop, 'The Foundations of Administrative Law' (12th Annual Whitmore Lecture, Council of Australasian Tribunals (NSW Chapter), 4 April 2019) ('The Foundations of Administrative Law'); Allsop, 'Values in Public Law' (n 29); Paul Daly, 'Administrative Law: A Values-Based Approach' in John Bell et al (eds), *Public Law Adjudication in Common Law Systems: Process and Substance* (Hart Publishing, 2016) 23, 25 ('A Values-Based Approach'); Aronson, 'Public Law Values' (n 45); Justice Melissa Perry, 'Administrative Justice and the Rule of Law: Key Values in the Digital Era' (Speech, Rule of Law in Australia Conference, Sydney, 6 November 2010) ('Key Values in the Digital Era'); Carol Harlow, 'Global Administrative Law: The Quest for Principles and Values' (2006) 17(1) *European Journal of International Law* 187 <https://doi.org/10.1093/ejil/chi158>; Administrative Review Council, *Automated Assistance in Administrative Decision Making: Report to the Attorney-General* (Report No 46, November 2004) 3 ('*ARC Report 46*'); Peter Cane, 'Theory and Values in Public Law' in Paul Craig and Richard Rawlings (eds), *Law and Administration in Europe: Essays in Honour of Carol Harlow* (Oxford University Press, 2003) 3, 3–22; David Dyzenhaus, 'Constituting the Rule of Law: Fundamental Values in Administrative Law' (2002) 27(2) *Queen's Law Journal* 445 ('Fundamental Values in Administrative Law'); Taggart, 'The Province of Administrative Law Determined?' (n 49); Dawn Oliver, 'The Underlying Values of Public and Private Law' in Michael Taggart (ed), *The Province of Administrative Law* (Hart Publishing, 1997) 217, 217–42.

51 See Matthew Groves, 'Administrative Justice in Australian Administrative Law' (2010) 66 *Australian Institute of Administrative Law Forum* 18, 22.

52 Allsop, 'Values in Public Law' (n 29) 127 (emphasis added).

53 Harlow and Rawlings (n 5) 297.

54 Ibid.

prominence that administrative law values now take in the administrative justice system in an era of technological development.[55] Ng and O'Sullivan have argued that administrative law doctrine must evolve to meet technological advances in a way that fulfils the underlying values of administrative law more broadly.[56] Perry emphasised the importance of administrative law values in responding to the challenges and opportunities that new technologies present. In the context of the interface between administrative law and personal data, she observed:

> [T]he many avenues now available through technological advances by which personal information can be obtained without the knowledge of the person concerned … emphasise the need for vigilance in ensuring that compulsive powers are conferred and exercised in a manner consistent with fundamental administrative law values.[57]

Recently, the Comprehensive Review of the Legal Framework of the National Intelligence Community ('Richardson Review') emphasised the importance of 'the principles of administrative law … fairness, transparency and accountability … [w]here AI is being used'.[58] In the context of 'artificial administration', Daly has raised the importance of administrative norms and values in shaping emerging legal frameworks for technologies.[59] The current legal framework governing FRT is deficient. It is hoped that specifically examining each of these important, though often subliminal, values may focalise the issues and inform development of an appropriate regulatory framework.

It is not suggested that the issues addressed below under a particular value do not overlap with other values.[60] Indeed, the article's structure in combining the discussion of 'accessibility and participation' and 'fairness and rationality' reflects this. Tying the discussion of topics to specific values is intended to focus the analysis and avoid repetition, though this arguably comes at the cost of not fully exploring overlaps between all values. This alignment of values and issues is simply one approach to examining FRT through an administrative law lens, it is not an end in itself. Nor is the intention to declare particular values satisfied or unsatisfied – they are aspirational, and their degree of satisfaction exists upon a continuum.

---

55 John McMillan, 'The Impact of Technology on the Administrative Justice System' (2013) 75 *Australian Institute of Administrative Law Forum* 11, 12–13 ('The Impact of Technology on the Administrative Justice System').

56 Yee-Fui Ng and Maria O'Sullivan, 'Deliberation and Automation: When Is a Decision a "Decision"?' (2019) 26(1) *Australian Journal of Administrative Law* 21, 34.

57 Perry, 'Key Values in the Digital Era' (n 50) 9.

58 *Richardson Review Report* (n 10) vol 3, 202 [37.116].

59 Paul Daly, 'Artificial Administration: Administrative Law, Administrative Justice and Accountability Mechanisms in the Age of Machines', *Administrative Law Matters* (Blog Post, 8 July 2020) <https://www.administrativelawmatters.com/blog/2020/07/08/artificial-administration-administrative-law-administrative-justice-and-accountability-mechanisms-in-the-age-of-machines/>.

60 For example, the OAIC is considered in the context of the values of participation and accessibility, but it clearly has a vital role to play in ensuring accountability.

A Accountability: The *Privacy Act*

Accountability is arguably one of the most important values of administrative law.[61] It is a common thread in many of the articulations for the normative underpinning of administrative law.[62] Finn has stated:

> Modern administrative law has superimposed the language of 'democratic accountability' … Citizens therefore feel justified in calling 'their' government to account, via demands for information and participation, greater avenues of review and electoral sanctions. Modern conceptions of administrative law have expanded to include this broader range of forms of public accountability, but they have not altered the basic focus of those accountability mechanisms upon the doings of the state and its agents. … Administrative law … is conceived of as a defence of a cherished realm of individual privacy and freedom of action from unjustified governmental intrusion.[63]

One may question whether the *Privacy Act* and associated soft law supports this understanding of administrative law accountability defending the cherished realm of individual privacy, and whether it provides an adequate accountability framework for governing use of FRT.

The central component of Australia's privacy framework is the *Privacy Act*.[64] There is increasing recognition that this legislation requires reform to remain fit for purpose in the digital age.[65] The *Privacy Act* was enacted to regulate personal information handling by governmental departments, rather than intrusive conduct, such as surveillance.[66] Though there have been significant subsequent reforms to the *Privacy Act*, recognising its origins assists in understanding why FRT – a technology that can converge surveillance and personal information identification capacities – sits so uncomfortably within the existing regime.

In short, the requirements of the *Privacy Act* operate in relation to two categories of information: 'personal information' and 'sensitive information'. Sensitive information is a subset of personal information which receives additional

---

61 Accountability can take many forms: see *Hot Holdings Pty Ltd v Creasy* (2002) 210 CLR 438, 467. See also Richard Mulgan, '"Accountability": An Ever-Expanding Concept?' (2000) 78(3) *Public Administration* 555, 568 <https://doi.org/10.1111/1467-9299.00218>; Dawn Oliver, 'Law, Politics and Public Accountability: The Search for a New Equilibrium' [1994] (Summer) *Public Law* 238, 246.

62 See Gabriel Fleming, 'Administrative Review and the "Normative" Goal: Is Anybody Out There?' (2000) 28(1) *Federal Law Review* 61, 65 <https://doi.org/10.22145/flr.28.1.3>; Paul Craig, *Administrative Law* (Sweet & Maxwell, 8th ed 2016) 3; Jerry L Mashaw, 'Federal Administration and Administrative Law in the Gilded Age' (2010) 119(7) *Yale Law Journal* 1362, 1378 <https://doi.org/10.2139/ssrn.1499322>.

63 Chris Finn, 'The Public/Private Distinction and the Reach of Administrative Law' in Matthew Groves (ed), *Modern Administrative Law in Australia* (Cambridge University Press, 2014) 49, 67–8 <https://doi.org/10.1017/CBO9781107445734.004>.

64 This article will not consider the incidental protection afforded to privacy via general law doctrines (such as breach of confidence, defamation, injurious falsehood, nuisance, passing off and trespass) as they are tangentially relevant to most applications of FRT.

65 The Federal Government committed to reviewing whether the *Privacy Act*'s scope and enforcement mechanisms remain fit for purpose: Attorney-General's Department (Cth), 'Review of the *Privacy Act 1988* (Cth)' (Issues Paper, October 2020) 2 ('*Privacy Act* Review'). Though there have been ongoing delays with the release of the final report.

66 Lee A Bygrave, 'The *Privacy Act 1988* (Cth): A Study in the Protection of Privacy and the Protection of Political Power' (1990) 19(2) *Federal Law Review* 128, 133 <https://doi.org/10.1177/006720 5X9001900203>.

protections. Sensitive information now includes 'biometric templates' and 'biometric information that is to be used for the purpose of automated biometric verification or biometric identification'.[67] The *Privacy Act* adopts a principles-based approach, ie, it operates by reference to a set of 13 Australian Privacy Principles ('APPs'). The rationale underlying this approach is regulatory flexibility.[68] However, a disadvantage of this approach is that its ambiguity 'can undermine the system's intended protections and accountability'.[69] The APPs apply to public sector agencies. 'Agency' is defined to include, inter alia, Commonwealth departments, persons performing the duties of an office established under a Commonwealth law, and the Australian Federal Police.[70] Similar state legislation exists for state agencies but for simplicity it will not be addressed. Agencies are also subject to a code designed to enhance accountability.[71] Broadly speaking, the APPs regulate the collection, use and disclosure of personal information. Depending on the particular application of FRT, the APPs which are relevant may vary, though it is useful to canvass the *Privacy Act*'s exceptions and exemptions in general terms to illustrate its limitations in regulating FRT.

1 Exemptions and Exceptions

A significant threshold matter that can greatly curtail the accountability otherwise provided by the *Privacy Act* is the extensive nature of exemptions and exceptions to the APPs. Entire agencies are exempted from the operation of the *Privacy Act* and, therefore, from the APPs. For example, the APPs do not cover intelligence agencies[72] or the Australian Crime Commission.[73] The APPs also do not cover acts or practices of other agencies involving the disclosure of personal information to intelligence agencies, or by an agency with an intelligence role or function.[74]

The *Privacy Act* contains broad exceptions to the APPs.[75] Relevantly for 'collection' and 'use or disclosure' of personal information, exceptions apply if either: the act is 'required or authorised by law'; the individual has consented; the act is for an 'enforcement related activity'; or there is a 'permitted general

67 *Privacy Act 1988* (Cth) s 6(1) (definition of 'sensitive information' paras (d), (e)) ('*Privacy Act*').

68 *ALRC Report 108* (n 32) vol 1, 234.

69 Ibid 236.

70 *Privacy Act* (n 67) s 6(1) (definition of 'agency'). The Australian Privacy Principles ('APPs') also apply to certain private sector organisations. Covered public sector agencies and private sector organisations are collectively termed 'APP entities'.

71 *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth) s 6(b). This *Code* requires agencies to have a privacy management plan, a designated privacy officer and 'privacy champion', and to conduct Privacy Impact Assessments for high privacy risk activities and privacy training for staff.

72 *Privacy Act* (n 67) s 7(1)(f). Defined in the *Privacy Act* section 6(1) to mean: the ASIO; the Australian Secret Intelligence Service ('ASIS'); the Australian Signals Directorate; and the Office of National Intelligence.

73 *Privacy Act* (n 67) s 7(1)(h).

74 Ibid ss 7(1A)–(1B).

75 Though these exceptions are typically more stringent for sensitive information than personal information, they still provide agencies with significant discretion. Additionally, whilst biometric templates are sensitive information, the information that they may be linked with may merely be personal information, creating disjunctures in the application of APPs.

situation'.[76] The breadth of these exceptions is further extended by definitions for terms such as 'enforcement body', which goes beyond police departments to include, for example: the Immigration Department; 'another agency, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law'; and 'another agency, to the extent that it is responsible for administering a law relating to the protection of … public revenue'.[77] These agencies therefore have wide scope to collect sensitive information in carrying out these functions.

The accountability gaps created by the *Privacy Act* feed into a broader narrative of growing concern that 'legislation is increasingly empowering and exempting law enforcement and intelligence agencies' information collection capacities is undermining their social licence to access certain information.[78] Vivienne Thom, the former Inspector-General of Intelligence and Security, provided a salutary caution emphasising in general terms that 'any extra powers given to the intelligence agencies must always be balanced by appropriate safeguards for the privacy of individuals'.[79] Recently, the OAIC highlighted the breadth of the government exceptions, and foreshadowed the scope for 'additional organisational accountability measures' to be considered in the upcoming review of the *Privacy Act*.[80] There are other integrity bodies beyond the OAIC that oversee police and intelligence agencies, but without an applicable privacy framework their jurisdiction does not clearly encompass privacy-invasive uses of FRT.[81] The existence of these bodies can be distracting as it paints a veneer of oversight that does not necessarily reflect reality. The Government consistently points to the *Privacy Act* and integrity bodies as evidence of 'safeguards' when implementing

76 *Privacy Act* (n 67) s 16A. There are seven permitted general situations, these include: taking appropriate action in relation to suspected unlawful activity or serious misconduct, and performing diplomatic or consular functions. This latter exception has been criticised as it 'effectively completely exempt[s] the Department of Foreign Affairs and Trade from the APPs': Office of the Victorian Privacy Commissioner, Submission to the Senate Legal and Constitutional Affairs Committee, *Inquiry into the Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (9 July 2012) 1.

77 *Privacy Act* (n 67) s 6(1) (definition of 'enforcement body' paras (ca), (f), (g)).

78 See, eg, Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 28 February 2020, 27 (Mike Burgess, ASIO Director-General).

79 Vivienne Thom, 'Reflections of a Former Inspector-General of Intelligence and Security' (2016) 83 *Australian Institute of Administrative Law Forum* 11, 11.

80 Office of the Australian Information Commissioner, Submission No 108 to Australian Human Rights Commission, *Human Rights and Technology Discussion Paper* (6 July 2020) 7, 9 ('OAIC Submission No 108').

81 These organisations are governed by 'a weak, discretionary and ministerially privacy rules model' under the *Office of National Intelligence Act 2018* (Cth): Greg Carne, 'Designer Intelligence or Legitimate Concern?: Establishing an Office of National Intelligence and Comprehensively Reviewing the National Intelligence Community Legal Framework' (2019) 46(1) *University of Western Australia Law Review* 144, 146. Multiple submissions to the Richardson Review argued for greater application of the *Privacy Act* to intelligence agencies: *Richardson Review Report* (n 10) vol 4, 45. Ultimately though, the Richardson Review recommended a legislative requirement that intelligence agencies have legally-binding privacy guidelines or rules, which are made public: *Richardson Review Report* (n 10) vol 4, 52 (Recommendation 189).

new technologies or legislation that compromise privacy,[82] but these checks often have a mostly ancillary role in providing accountability.

This issue of balancing accountability and exemptions reflects a wider tension whereby intelligence organisations must be 'sufficiently secretive so as to adequately fulfil their primary mission, as well as sufficiently open to scrutiny to ensure accountability'.[83] On one view, such broad exemptions are necessary in the area of national security for the agencies to carry out their functions. However, this must be tempered by recognition of the fact that security bodies are not incapable of mistakes or misconduct with damaging consequences, and that the national security environment since September 11 has been characterised by a 'plethora of security laws that … affect individual rights of privacy in different ways, while diminishing the transparency of security organisations'.[84] It is hard to escape the conclusion that the Government has lost sight of the earlier understanding that national security 'may be precisely the area where additional protections for civil liberties and for individual privacy are needed as the new information technology enhances the power of security and police agencies to interfere with individual privacy'.[85] The fields of national security and defence were outside the terms of reference in the 1983 ALRC report leading to the *Privacy Act*.[86] Overall, the protection offered by the *Privacy Act* is arguably an example whereby the law 'stringently protects against minor privacy invasions yet utterly fails to protect against major ones'.[87] The notion that law enforcement and national security agencies should be provided with unhindered powers and technological capacities in performing their functions has been persuasively critiqued elsewhere. In short, it can be described as a 'rather unsophisticated form of utilitarianism embracing the new technologies as maximising aggregate social welfare' where the benefits to the common good outweigh the largely intangible costs to the individual, trumping a rights-based approach.[88]

The limited accountability provided by the *Privacy Act* in this area is particularly problematic given that national security is also often presented as an obstacle to judicial accountability mechanisms. National security matters are commonly viewed

---

82 See John McMillan, 'Privacy: A Regulator's Perspective' (2016) 83 *Australian Institute of Administrative Law Forum* 78, 79. See also Part IV(E)(3).

83 Gustav Lanyi, 'Bringing Spies to Account: The Advisory Report of the Parliamentary Joint Committee on ASIO, ASIS and DSD on the ASIO Legislation Amendment (Terrorism) Bill 2002' (2002) 10(1) *Australian Journal of Administrative Law* 68, 72 (emphasis omitted).

84 Paterson, *FOI and Privacy in Australia* (n 18) 81.

85 *ALRC Report 22* (n 20) vol 2, 206. The Australian Law Reform Commission ('ALRC') further stated at vol 2, 207: 'It may be appropriate, in time, to develop the function for the Privacy Commissioner to act as an intermediary on behalf of persons who believe they have been treated unfairly or inappropriately, as a result of national security as well as police information'. For the arguments that the *Privacy Act* should not contain any blanket exemptions, see Nigel Waters, 'Essential Elements of a New Privacy Act' (1999) 5(8) *Privacy Law and Policy Reporter* 168.

86 *ALRC Report 22* (n 20) vol 1, xxxvii.

87 Daniel J Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale University Press, 2011) 2–3.

88 Bob Hepple, 'The Right to Privacy and Crime Detection' (2009) 68(2) *Cambridge Law Journal* 253, 255 <https://doi.org/10.1017/S000819730900052X>. See also Dyzenhaus, 'Fundamental Values in Administrative Law' (n 50) 504–9.

as non-justiciable,[89] or at least subject to a flexible conception of procedural fairness that can be rendered nugatory.[90] The *Administrative Decisions (Judicial Review) Act 1997* (Cth) ('*AD(JR) Act*') is entirely inapplicable to decisions under multiple statutes related to national security.[91] Aronson has examined issues associated with the wide statutory immunities provided to intelligence agencies and legislation restricting access to information on the basis of national security, noting that in some of these circumstances 'meaningful judicial scrutiny of government action has become well-nigh impossible'.[92] Ultimately, the accountability provided by the *Privacy Act* in governing many uses of FRT is minimal. This section is not intended to suggest that there should be no exceptions to the APPs in particular circumstances. Rather, it is hoped to have illustrated that it would be naive to consider the current legislation a heavy check on governmental use of FRT. It also partly explains constraints faced by the OAIC in seeking to protect individuals' privacy.

B Accessibility and Participation: The OAIC

Accessibility and participation are distinct but interrelated concepts. Regarding accessibility, Aronson, Groves and Weeks' list explicitly outlines 'accessibility *of judicial and non-judicial grievance procedures*'.[93] McMillan and Carnell have suggested that the creation of independent review agencies, including the Privacy Commissioner, was a response to the notion that people have a 'right to complain' against a failure by an agency or its staff. This notion – which is arguably tantamount to accessibility – is said to stem from the trend of greater interaction between the community and government, including in areas (relevantly for FRT purposes) such as provision of social benefits, responding to criminal and security threats, and regulating international travel.[94]

Participation 'takes a variety of forms'[95] and has been described as 'particularly ambiguous'.[96] It has a paramount position in US administrative law, where it encompasses rule-making processes that are receptive to public participants.[97] In Australia, it has been said that the new administrative law has led to a greater

89 For a critique of this approach, see David Dyzenhaus, 'Humpty Dumpty Rules or the Rule of Law: Legal Theory and the Adjudication of National Security' (2003) 28 *Australian Journal of Legal Philosophy* 1 <https://doi.org/10.2139/ssrn.319100>.

90 Chris Finn, 'The Justiciability of Administrative Decisions: A Redundant Concept?' (2002) 30(2) *Federal Law Review* 239, 254 <https://doi.org/10.1177/0067205X0203000202>.

91 See, eg, *AD(JR) Act* (n 10) sch 1. This excludes from review decisions under the: *Australian Security Intelligence Organisation Act 1956* (Cth); *Intelligence Services Act 2001* (Cth); *Australian Security Intelligence Organisation Act 1979* (Cth); *Inspector-General of Intelligence and Security Act 1986* (Cth); *Telecommunications (Interception and Access) Act 1979* (Cth); *Telephonic Communications (Interception) Act 1960* (Cth).

92 Mark Aronson, 'Between Form and Substance: Minimising Judicial Scrutiny of Executive Action' (2017) 45(4) *Federal Law Review* 519, 528 <https://doi.org/10.22145/flr.45.4.3>.

93 Aronson, Groves and Weeks (n 48) 4 (emphasis added).

94 John McMillan and Ian Carnell, 'Administrative Law Evolution: Independent Complaint and Review Agencies' (2010) 59 *Administrative Review* 42, 44.

95 Cane (n 50) 16.

96 Harlow (n 50) 193.

97 This position is largely attributed to Richard B Stewart, 'The Reformation of American Administrative Law' (1975) 88(8) *Harvard Law Review* 1667 <https://doi.org/10.2307/1340207>.

recognition of the value of participation.[98] Before considering the capacity of the OAIC to fulfil the ideals of accessibility and participation, it is essential to understand its background and functions.

1 The OAIC

Central to the development of Australia's privacy regime was the establishment of a statutory guardian, in the form of an administrative body with the specific function of advocating privacy interests.[99] This article does not seek to reagitate arguments for or against recognition of an 'integrity branch' of government.[100] However, it would be misguided to ignore the consequences that have arisen from the OAIC's placement within the Executive. In 2014, the Federal Government sought to disband the OAIC, dividing its privacy and freedom of information ('FOI') functions between the AAT, Australian Human Rights Commission, Attorney-General's Department and Commonwealth Ombudsman. But the legislation did not pass through the Senate.[101] It has been suggested that this was an effort to neutralise the perceived threat it posed to the Executive.[102] Currently, the OAIC is facing a significant funding cut in forward estimates, from $29 million in 2021–22 to $16 million in 2024–25.[103]

The Commissioner's functions are grouped within the *Privacy Act* according to guidance, monitoring and advice.[104] The *Privacy Act* is enforced primarily via a complaints-based system, although the Commissioner also has powers to conduct compliance assessments, to direct an agency to undertake a Privacy Impact Assessment, and to recognise an external dispute resolution scheme for dealing with privacy-related complaints (after taking into account, inter alia, the

98 Justice Keith Mason, 'Sunrise or Sunset? Reinventing Administrative Law for the New Millennium' (Speech, National Administrative Law Forum, 15 June 2000) 8.

99 In 2010, the OAIC was established by amalgamating the Privacy Commissioner, Freedom of Information ('FOI') Commissioner and Information Commissioner: *Australian Information Commissioner Act 2010* (Cth). This amalgamation has been criticised and praised. For criticism, see Carolyn Adams, 'One Office, Three Champions? Structural Integration in the Office of the Australian Information Commissioner' (2014) 21(2) *Australian Journal of Administrative Law* 77. For praise, see John McMillan, 'Information Law and Policy: The Reform Agenda' (2011) 66 *Australian Institute of Administrative Law Forum* 51.

100 For support of a four-branch theory of government, see Bruce Ackerman, 'The New Separation of Powers' (2000) 113(3) *Harvard Law Review* 633, 693–6 <https://doi.org/10.2307/1342286>; Chief Justice Spigelman, 'The Integrity Branch of Government' (2004) 78(11) *Australian Law Journal* 724; John McMillan, 'Re-thinking the Separation of Powers' (2010) 38(3) *Federal Law Review* 423 <https://doi.org/10.22145/flr.38.3.7>; AJ Brown, 'The Integrity Branch: A "System", an "Industry", or a Sensible Emerging Fourth Arm of Government?' in Matthew Groves (ed), *Modern Administrative Law in Australia* (Cambridge University Press, 2014) 301 <https://doi.org/10.1017/CBO9781107445734.017>. For criticism, see Justice WMC Gummow, 'A Fourth Branch of Government?' (2012) 70 *Australian Institute of Administrative Law Forum* 19; Wayne Martin, 'Forewarned and Four-Armed: Administrative Law Values and the Fourth Arm of Government' (2014) 88(2) *Australian Law Journal* 106; Justice Stephen Gageler, 'Three is Plenty' in Greg Weeks and Matthew Groves (eds), *Administrative Redress in and out of Courts: Essays in Honour of Robin Creyke and John McMillan* (Federation Press, 2019) 12.

101 Freedom of Information Amendment (New Arrangements) Bill 2014 (Cth).

102 Weeks (n 27) 42.

103 Attorney-General's Department (Cth), *Portfolio Budget Statements 2022–23: Budget Related Paper* (Report No 1.2, 2022) 290.

104 *Privacy Act* (n 67) ss 28–28B.

scheme's accessibility, fairness and accountability).[105] An individual may complain to the Commissioner about an interference with their privacy.[106] The Commissioner must investigate a complaint, except in certain circumstances, including where the respondent has not had an adequate opportunity to deal with the complaint, or is currently dealing with the complaint.[107] The Commissioner may also instigate an own-motion investigation into privacy interferences.[108] After an investigation, the Commissioner may make determinations that can be enforced via the Federal Circuit Court or the Federal Court.[109] The *Privacy Act* permits complainants to apply for review to the AAT where they are dissatisfied with a determination made by the Commissioner.[110] However, this right is of little utility where a Commissioner decides not to make a determination.

2 Accessibility and the OAIC

As the *Privacy Act* is a principles-based regime enforcement largely rests with the Commissioner. This can present significant obstacles to the accessibility of satisfactory grievance procedures, beyond the limitations imposed by APP exceptions and funding constraints already discussed. The *Privacy Act* encourages the Commissioner to adopt a conciliatory rather than coercive approach when dealing with agencies.[111] Past commissioners have reiterated that 'we usually adopt a conciliation-focused approach',[112] and that this 'approach is often preferred because it avoids the adversarial relationships that arise when enforcement powers are used or threatened'.[113] This approach demonstrates the challenge faced by the OAIC in balancing its enforcement powers without undermining its 'softer' consultation and advice-giving functions. Clearly conciliation has merit for less serious breaches: it is less costly and more informal than courts. However, it is not clear that it should preclude individuals from accessing judicial redress.

Currently, individuals have limited access to judicial grievance mechanisms to prevent privacy interferences. If the Commissioner decides not to investigate a complaint, judicial review may be sought regarding that decision.[114] Courts,

105 Ibid ss 33C, 33D, 35A.
106 Ibid s 36.
107 Ibid s 41.
108 Ibid s 40. In 2019–20, the Commissioner received 2,673 privacy complaints and self-initiated 19 investigations: Office of the Australian Information Commissioner, *Annual Report 2019–20* (Report, 2020) 40, 35.
109 *Privacy Act* (n 67) ss 52, 55A, 62.
110 Ibid s 96(1)(c).
111 For example, the *Privacy Act* section 40A requires the Commissioner to attempt conciliation where it is reasonably possible that the complaint may be conciliated successfully.
112 Timothy Pilgrim, 'Privacy Law Reform: Challenges and Opportunities' (2012) 69 *Australian Institute of Administrative Law Forum* 35, 38.
113 Anthony Bendall, 'The Governance of Privacy: Speak Softly and Carry a Big Stick' (2008) 60 *Australian Institute of Administrative Law Forum* 39, 47. Whilst Dr Bendall is a former deputy Victorian Privacy Commissioner, his comments are of broader relevance.
114 See *Gao v Federal Privacy Commissioner* (2002) 76 ALD 447.

however, have expressed reluctance to interfere with Ombudsmen decisions.[115] It is possible that judicial concerns about a lack of net gain in tying up Ombudsmen in litigation may equally apply in the context of reviewing OAIC decisions. The UK, like Australia, adopts a principles-based regime to privacy protection. Unlike Australia, individuals also have the right to access judicial processes to seek a remedy where they consider their rights have been infringed by non-compliance in processing personal data, regardless of any action taken by the national supervisory body.[116] The utility of Australia adopting such an approach is discussed in Part V.

Recent Australian surveys have revealed public concern about the threat posed by biometrics (including FRT) and inaccessibility of redress. For example, 83% of respondents were concerned about the protection of privacy when biometrics were in use.[117] In a separate survey, 70% of respondents considered protection of personal information to be a major concern in their lives, yet 49% did not know how to protect themselves, and 78% wanted a right to seek redress in the courts.[118] Whilst survey results can vary, they do provide a useful portal into wider community concerns and understandings. Chief Justice French explained that part of the importance of administrative law values lies in the fact that 'they form a bridge of intelligibility between what administrators, judges and lawyers do in the pursuit of administrative justice and what the wider community is entitled to expect of them'.[119] It appears that the community concerns regarding misuse of personal information and FRT do not align with expectations for accessible grievance procedures.

3 Participation and the OAIC

The ALRC stated that '[a] central tension in the regulation of compliance with the *Privacy Act* is how to strike a balance between resolving individual complaints and remedying systemic issues'.[120] In some respects, the OAIC's focus on systematic issues indirectly enables participation in areas that would otherwise remain unaddressed. Stewart explains that the practical extent of participation rights can turn on the means for providing representation. Arguably, the OAIC fills a participation-gap:

---

115 See, eg, *Kaldas v Barbour* (2017) 350 ALR 292 ('*Kaldas*'). Aronson suggests *Kaldas* has relevance 'beyond Ombos', and that it is 'important in … its view that an extremely parsimonious statutory challenge mechanism served well enough as an "acceptable" trade-off for traditional judicial review': Mark Aronson, 'Retreating to the History of Judicial Review?' (2019) 47(2) *Federal Law Review* 179, 194 (citations omitted) <https://doi.org/10.1177/0067205X19831811>. Whilst *Kaldas* concerned a challenge by a respondent (not a complainant), this rationale arguably applies in both directions.

116 *Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 art 79 ('*GDPR*'); *Data Protection Act 2018* (UK) s 167.

117 Penny Jorna, Russell G Smith and Katherine Norman, *Identity Crime and Misuse in Australia: Results of the 2018 Online Survey* (Report No 19, 15 January 2020) 47.

118 Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2020* (Report, September 2020) 17, 43, 67.

119 French, 'Themes and Values Revisited' (n 4) 48.

120 *ALRC Report 108* (n 32) 1612.

> Representation of [individual] interests is especially unlikely in what may be a frequent situation in administrative law – where the impact of a decision is widely diffused so that no single individual is harmed sufficiently to have an incentive to undertake litigation, and where high transaction costs and the collective nature of the benefit sought preclude a joint litigating effort, even though the aggregate stake of the affected individuals would justify it.[121]

However, the OAIC's ability to foster participation is threatened by the inevitable compromise to resolving individual complaints which arises from pursuing systematic change. The OAIC recently stated that it seeks to ensure emerging risks are managed by 'utilising [its] full range of regulatory tools'.[122] Despite this, it may be questioned whether the 'stronger' enforcement tools such as determinations are being underutilised. For example, in 2020–21, the OAIC made a 'record' 17 determinations.[123] One may speculate as to the motivations underpinning a focus on systematic issues. Clearly the exceptions and exemptions curtail the OAIC's jurisdiction in a number of circumstances, and budgetary restraints necessitate trade-offs in resource allocation. Paradoxically, a focus on softer tools such as guidelines, education and conciliation can be less effective in achieving systematic change than fully pursuing individual complaints.[124] Paterson has said that there is 'a dearth of jurisprudence which elucidates the operation of the Act' and that 'it is necessary to rely heavily on the non-binding guidelines issued by the OAIC'.[125] Overreliance on these softer tools is problematic when such tools are ignored, leaving the OAIC to make platitudinous appeals to agencies to respect privacy.

In the context of FRT, these issues of regulators' ineffectiveness are illustrated in the UK case of *R (Bridges) v Chief Constable of South Wales Police* ('*Bridges*').[126] Though the decision will be explored in the following section, relevantly for present purposes, the police only decided to stop using the FRT after judicial review proceedings brought by an individual were upheld by the Court of Appeal. The Surveillance Camera Commissioner and Biometrics Commissioner both highlighted the fact that their efforts to draw attention to the inadequacy of the existing regulatory framework for the South Wales Police's ('SWP') use of FRT had been repeatedly ignored.[127] Prior to the judgment, both Commissioners were appointed to a Governance and Oversight Board to create a framework for the

---

121 Stewart (n 97) 1763.

122 Office of the Australian Information Commissioner, *Corporate Plan 2021–22* (Report, 2022) 11.

123 Office of the Australian Information Commissioner, *Annual Report 2020–21* (Report, 2021) 10. Note, this is a relatively small number given that 2,151 privacy complaints were lodged in the same period, though it was a considerable increase from the four determinations made in 2020: Office of the Australian Information Commissioner, *Annual Report 2019–20* (Report, 2020) 36.

124 Granted, measuring 'systematic change' is notoriously difficult: see Janina Boughey, 'Administrative Law's Impact on the Bureaucracy' in Greg Weeks and Matthew Groves (eds), *Administrative Redress in and out of Courts: Essays in Honour of Robin Creyke and John McMillan* (Federation Press, 2019) 93, 95.

125 Paterson, *FOI and Privacy in Australia* (n 18) 601.

126 *Bridges* (n 12).

127 Tony Porter, 'What Next for Automated Facial Recognition?' *Surveillance Camera Commissioner* (Blog Post, 11 August 2020) <https://videosurveillance.blog.gov.uk/2020/08/11/what-next-for-automated-facial-recognition/>; Paul Wiles, 'New Biometrics and the Police' (Frank Dawtry Memorial Lecture, University of Leeds, 11 February 2020) 1.

police use of new biometrics. However, 'the Board made no progress in developing such a framework nor provided significant oversight'.[128] Ultimately, the procedural limitations on bringing such matters to courts in Australia curtail the ability of case law to clarify the lawfulness of various applications of FRT. It is unclear whether the OAIC's focus on systematic change truly fosters participation.

C Lawfulness: The Right to Privacy

Chief Justice French defines the value of lawfulness to mean 'that official decisions are authorised by statute, prerogative or constitution'.[129] Aronson, Groves and Weeks' list instead uses the term 'legality'.[130] Harlow considers 'the principle of legality' to be an administrative law value.[131] Despite the subtle distinctions in these different articulations, each can be linked to the protection of human rights. Most directly, it has been said that the principle of legality means that '[c]ourts do not impute to the legislature an intention to abrogate or curtail certain human rights or freedoms'.[132] Less directly, Dyzenhaus locates the principle within 'the culture of justification' to mean that administrators must sufficiently justify their decisions, and that judges should adopt an attitude of deference as respect towards such justifications.[133] Importantly, however, this latter understanding still comfortably accommodates consideration of human rights, because in applying this principle of legality, 'courts are clearly (though not always explicitly) guided by international norms such as those contained in the [*European Convention on Human Rights*]'.[134] This culture of justification requires administrators to show either how their decisions conform to fundamental rights – including human rights – or that they are justifiable departures. Consideration of human rights via the principle of legality is part of the 'internationalisation of administrative law … [which] amounts to the judicial updating of the catalogue of values to which the common law subjects the administrative state'.[135] However the value is articulated, it is important to understand it as a value in this context, not simply a prescription

128 Paul Wiles, *Annual Report 2019* (Report, March 2020) 9 ('*Wiles Report*').

129 French, 'Themes and Values Revisited' (n 4) 37.

130 Aronson, Groves and Weeks (n 48) 4.

131 Harlow (n 50) 192.

132 *Al-Kateb v Godwin* (2004) 219 CLR 562, 577 (Gleeson CJ). However, in place of 'human rights', French CJ and Warren CJ use 'common law rights and freedoms', and Spigelman CJ uses 'fundamental rights and liberties': *Momcilovic v The Queen* (2011) 245 CLR 1, 50 [51] (French CJ); *WBM v Chief Commissioner of Police* (2012) 43 VR 446, 464 [76] (Warren CJ) ('*WBM*'); Chief Justice JJ Spigelman, 'Principle of Legality and the Clear Statement Principle' (2005) 79(12) *Australian Law Journal* 769, 769. The distinction between whether the principle of legality concerns *human* rights or *fundamental* rights is less consequential here if one accepts that the right to privacy may be characterised as a fundamental right: see *Commissioner of Taxation v Citibank Ltd* (1989) 20 FCR 403, 434 (French J) ('*Citibank*').

133 David Dyzenhaus, 'The Politics of Deference: Judicial Review and Democracy' in Michael Taggart (ed), *The Province of Administrative Law* (Hart Publishing, 1997) 279, 302, 306 ('Politics of Deference').

134 David Dyzenhaus, Murray Hunt and Michael Taggart, 'The Principle of Legality in Administrative Law: Internationalisation as Constitutionalisation' (2001) 1(1) *Oxford University Commonwealth Law Journal* 5, 20 <https://doi.org/10.1080/14729342.2001.11421382>.

135 Ibid 34.

to comply with positive law. Though there are different understandings of this value, each can be linked with protecting rights.

Additionally, privacy as a human right is typically qualified to protect against *unlawful* interferences. 'Human rights' are listed as a distinct value by Aronson and others.[136] McMillan has observed that the objectives of the administrative justice system have expanded to be 'values based', with a stronger focus on respect for human rights in decision-making and administration.[137] Hence, whilst human rights could accommodate a separate head of discussion, there is utility in examining privacy as a human right under the value of lawfulness.

Australian administrative law has had a more constrained role in protecting human rights than many of its foreign counterparts. In the context of judicial review, the ability to enforce international human rights instruments through the doctrine of legitimate expectations is now virtually non-existent.[138] It has been argued that absent any statutory 'rights consideration ground', judicial review will struggle to encompass adequate consideration of human rights.[139] Certain claims can be refashioned under existing grounds, but this approach is not without limitations.[140] By contrast, administrative law in the UK is said to have undergone a 'reformation' or 'reinvention', with rights at the centrepiece.[141] This is largely attributed to the passing of the *Human Rights Act 1998* (UK) ('*Human Rights Act*'), though it has been claimed that 'righting' of administrative law predated this Act[142] and that the values informing this Act were already enjoyed under common law.[143] Arguably, this right-centred focus extends past the application of the *Human Rights Act* in judicial review. For example, Aronson has explained that the *Human Rights Act* 'must … be viewed in contexts beyond its strict doctrinal reach. It was always intended to effect a culture change within the broader public sector'.[144]

---

136 Aronson, 'Public Law Values' (n 45) 144. See also Dyzenhaus, 'Fundamental Values in Administrative Law' (n 50) 453; Dame Sian Elias, 'Administrative Law for "Living People"' (2009) 68(1) *Cambridge Law Journal* 47, 59 <https://doi.org/10.1017/S0008197309000026>.

137 McMillan, 'The Impact of Technology on the Administrative Justice System' (n 55) 13.

138 *Re Minister for Immigration and Multicultural and Indigenous Affairs; Ex parte Lam* (2003) 214 CLR 1.

139 Matthew Groves, 'Judicial Review and Human Rights' (2018) 25(1) *Australian Journal of Administrative Law* 64, 72.

140 See Janina Boughey, 'The Use of Administrative Law to Enforce Human Rights' (2009) 17(1) *Australian Journal of Administrative Law* 25, 33.

141 Thomas Poole, 'The Reformation of English Administrative Law' (2009) 68(1) *Cambridge Law Journal* 142 <https://doi.org/10.1017/S0008197309000063>; Michael Taggart, 'Reinventing Administrative Law' in Nicholas Bamforth and Peter Leyland (eds), *Public Law in a Multi-layered Constitution* (Hart Publishing, 2003) 311 ('Reinventing Administrative Law'). Cf Jason NE Varuhas, 'The Reformation of English Administrative Law? "Rights", Rhetoric and Reality' (2013) 72(2) *Cambridge Law Journal* 369 <https://doi.org/10.1017/S0008197313000500>.

142 Taggart, 'Reinventing Administrative Law' (n 141) 325.

143 *A v Secretary of State for the Home Department* [2005] 2 AC 68, 130 [88] (Lord Hoffman). But see Thomas Poole, 'Harnessing the Power of the Past? Lord Hoffman and the *Belmarsh Detainees Case*' (2005) 32(4) *Journal of Law and Society* 534 <https://doi.org/10.1111/j.1467-6478.2005.00337.x>; JWF Allison, 'History to Understand, and History to Reform, English Public Law' (2013) 72(3) *Cambridge Law Journal* 526 <https://doi.org/10.1017/S000819731300069X>.

144 Aronson, 'Public Law Values' (n 45) 146.

1 Privacy as a Human Right

At the federal level, Australia lacks a constitutional or statutory Bill of Rights. The status of a general right to privacy at common law is uncertain.[145] None of the various proposals for a statutory tort for invasion of privacy have been implemented.[146] Internationally, privacy is recognised as a human right through instruments such as the *International Covenant on Civil and Political Rights* ('*ICCPR*').[147] Article 17 of the *ICCPR* provides:

> 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 the protection of the law against such interference or attacks.

In Australia, the *Privacy Act* objects include 'to implement Australia's international obligation [ie, the *ICCPR*] in relation to privacy', and 'to recognise that the protection of privacy of individuals is balanced with the interests of entities in carrying out their functions or activities'.[148] The Commissioner must have due regard to these objects in performing their functions and exercising their powers under the *Privacy Act*.[149] Privacy is also recognised as a human right under in the *Charter of Human Rights and Responsibilities Act 2006* (Vic) ('*Victorian Charter*') section 13(a), the *Human Rights Act 2004* (ACT) section 12(a) and the *Human Rights Act 2019* (Qld) section 25(a). However, the effectiveness of these Acts is reduced by the fact that they only apply at the state level, and have limited remedial utility. The *Privacy Act* is grouped by McMillan and Williams within a set of administrative law measures that protect human rights,[150] and described by Creyke as part of a broader movement in administrative law to provide Australians

---

145 *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479, 495 (Latham CJ), 517 (Evatt J); *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199. More recently, in *WBM* (n 132), Warren CJ observed that 'the question of whether such a right exists at common law, and if so, its scope, is yet to be settled by the High Court or a superior court of record': at 465 [81] (Hansen JA agreeing at 475 [133]). Bell AJA held at 482 [166] that 'for the purposes of the principle of legality, individuals have a fundamental right or liberty to personal privacy' derived from article 17 of the *International Covenant on Civil and Political Rights,* following *Citibank* (n 132) 433 (French J).

146 See *ALRC Report 123* (n 24) – supported in Australian Competition and Consumer Commission*, Digital Platforms Inquiry* (Final Report, July 2019) 36 (Recommendation 19) and 'AHRC Discussion Paper' (n 3) 10 (Proposal 4); *ALRC Report 108* (n 32); South Australian Law Reform Institute, *A Statutory Tort for Invasion of Privacy* (Final Report No 4, March 2016); Victorian Law Reform Commission, *Surveillance in Public Places* (Final Report No 18, August 2010); New South Wales Law Reform Commission, *Invasion of Privacy* (Report No 120, April 2009). For further analysis of these proposals, see Barbara McDonald, 'A Statutory Action for Breach of Privacy: Would it Make a (Beneficial) Difference?' (2013) 36(3) *Australian Bar Review* 241; Normann Witzleb, 'Another Push for an Australian Privacy Tort: Context, Evaluation and Prospects' (2020) 94(10) *Australian Law Journal* 765.

147 *International Covenant on Civil and Political Rights*, opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.

148 *Privacy Act* (n 67) ss 2(h), (b).

149 Ibid s 29.

150 McMillan and Williams (n 27) 68.

'with an array of measures through which to implement rights-protection'.[151] Others, however, have been more cynical as to the sincerity of governmental legislative commitments to privacy obligations under human rights instruments.[152]

It is useful to consider how Australian courts have approached arguments relating to the characterisation of privacy as a human right. These arguments typically arise in two contexts: where it is argued that a public authority has acted incompatibly with, or failed to give proper consideration to, the right; and where the right is raised in interpreting legislation. The focus of this section is not confined to cases considering state human rights instruments, however, some of the cases involving section 13(a) of the *Victorian Charter* are instructive as to the meaning of the 'virtually identical' article 17 of the *ICCPR*, and the 'generally similar' article 8 of the *European Convention on Human Rights* ('*ECHR*').[153] Beyond the *Victorian Charter*, the *ICCPR* arguably has broader relevance through the principle of legality. Chief Justice French observed that the content of the principle of legality might be informed by international human rights norms through the evolution of the common law.[154] It has been suggested that this should happen 'by treating the rights and freedoms in the *ICCPR* as fundamental rights and freedoms for the purposes of the principle of legality'.[155] French J (as his Honour then was) has used the principle of legality as a means of considering the right to privacy in examining the performance of a public authority's functions.[156] Whilst strictly speaking, 'the Charter has no application to a Commonwealth authority such as the [O]AIC',[157] the right to privacy under article 17 of the *ICCPR* remains relevant through the *Privacy Act*'s objects, and the principle of legality.

In *AIT18 v Australian Information Commissioner,*[158] the Full Court of the Federal Court accepted that 'the *Privacy Act* is remedial or beneficial legislation and should, in general, be construed liberally but with close attention to the relevant statutory terms which require interpretation'.[159] Even if there is no ambiguity 'the *Privacy Act* should, *as far as the statutory language permits*, be construed so as to give effect to Australia's international obligations. [However] the words of qualification which are [emphasised] are critical'.[160] The Court also held that '[t]he exceptions in the *Privacy Act* reflect the Parliament's identification of circumstances in which

151 Creyke (n 26) 110. Creyke uses the term 'rights' expansively to include – but not be limited to – human rights: at 106.

152 See, eg, Megan Richardson, *The Right to Privacy: Origins and Influence of a Nineteenth-Century Idea* (Cambridge University Press, 2017) 112–19 <https://doi.org/10.1017/9781108303972>; 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century', *Roger Clarke* (Web Page, 4 January 2000) <http://www.rogerclarke.com/DV/PP21C.html>.

153 See Moira Paterson, 'Privacy Rights and Charter Rights' in Matthew Groves and Colin Campbell (eds), *Australian Charters of Rights a Decade On* (Federation Press, 2017) 203, 206.

154 Chief Justice RS French, 'Oil and Water? International Law and Domestic Law in Australia' (Brennan Lecture, Bond University, 26 June 2009) 20.

155 *Director of Public Prosecutions v Kaba* (2014) 44 VR 526, 578 [179] (Bell J) ('*Kaba*').

156 *Citibank* (n 132) 433 (French J).

157 *Wijayaweera v Australian Information Commissioner* [2012] FCA 99, [19] (Gordon J).

158 (2018) 267 FCR 93.

159 Ibid 115 [82].

160 Ibid 117 [88] (emphasis in original) (citations omitted).

interference with a person's privacy is not arbitrary or unlawful' as contemplated by article 17 of the *ICCPR*.[161] With respect, this conflation of arbitrariness and unlawfulness is dubitable. There is strong support for the argument that arbitrary interferences can encompass interferences that are not 'unlawful' in the sense that they do not violate positive law.[162]

Whilst FRT has not received judicial consideration in Australia, cases regarding the protection provided by the right to privacy over one's personal details – such as one's name – are arguably relevant by analogy. The right to privacy can encompass the right not to provide one's details to the police. In *Director of Public Prosecutions v Kaba*[163] the Director of Public Prosecutions sought judicial review of a Magistrate's decision not to admit evidence in proceedings. Bell J quashed the Magistrate's ruling on the basis that that his Honour had erred in finding the police lacked the power to perform random licence checks. However, Bell J held that the conduct at issue had violated Mr Kaba's 'right to privacy under the common law, the *ICCPR* and the Charter'.[164] Bell J examined how the right to privacy protects attributes including an individual's name, explaining that

> there is something universal and personal about possession of a name and its connection with identity. It might be said that our name is one of our most important possessions and that, like other possessions, we have a private right to choose who to share it with or divulge it to.[165]

His Honour drew support from *Pretty v United Kingdom*,[166] where the Court explicitly included protection of a person's name as an attribute protected by article 8(1) of the *ECHR*, and other subsequent cases where the European Court of Human Rights has applied that principle to individuals' names and photographs.[167]

More recently, Bell AJA held that – separate from the question of whether the common law should recognise a cause of action for breach of privacy – 'for the purposes of the principle of legality, individuals have a fundamental right or liberty to personal privacy'.[168] And that '[a] fundamental civil right or liberty which we all possess under the common law is the right or liberty not to report to police and other officials and not to disclose personal or private information to them'.[169]

These decisions are important because they illustrate how the right to privacy may be relevant in domestic law. They also contextualise the threat posed by using

---

161 Ibid 115 [85].

162 See *ALRC Report 22* (n 20) vol 1, 267. There are differing views on the extent to which arbitrariness should be interpreted consistently with international jurisprudence. Critically, however, none of these views treat unlawfulness and arbitrariness as equivalent: see *Kracke v Mental Health Review Board* (2009) 29 VAR 1, 45 [169] (Bell J); *Nolan v MBF Investments Pty Ltd* [2009] VSC 244, [168] (Vickery J); *PJB v Melbourne Health* (2011) 39 VR 373; *WBM* (n 132) 470 [103] (Warren CJ), 490 [203] (Bell AJA); *Jurecek v Director, Transport Safety Victoria* (2016) 260 IR 327, 344 [64] (Bell J).

163 (2014) 44 VR 526.

164 *Kaba* (n 155) 646 [456].

165 Ibid 561 [123].

166 [2002] III Eur Court HR 427, discussed in *Kaba* (n 155) 562–3 [128]–[131].

167 For names: *Stjerna v Finland* (1997) 24 EHRR 195; *Stjerna v Finland* [1994] ECHR 43; *Tekeli v Turkey* (2006) 42 EHRR 53. For photographs: *Reklos v Greece* [2009] Eur Court HR 200; *Von Hannover v Germany* [2005] VI Eur Court HR 41, [50].

168 *WBM* (n 132) 482 [167].

169 Ibid 480 [160].

FRT to identify individuals – potentially violating established protections over one's name.

2 R (Bridges) v Chief Constable of South Wales Police

Despite the differences between administrative law frameworks outlined above, developments in UK law remain relevant to contemporary Australia. Rights 'drive an international discourse … [that] operates "horizontally" – between and across nation states',[170] and there is ample authority that interpretations of article 8 of the *ECHR* are relevant to understanding privacy as a human right in Australia.[171] Both Australia and the UK adopt a principles-based regime for protecting privacy. Both regimes provide additional protection for 'sensitive' information/processing (which encompasses biometric data) and contain similar law enforcement exceptions.[172]

In *Bridges*, the UK Court of Appeal considered an appeal from the High Court dismissing the appellant's claim for judicial review challenging the lawfulness of the use of live Automated Facial Recognition technology ('AFR') by the SWP. The system involved deployment of 'overt' surveillance cameras to capture a live feed of images of the public, which an algorithm then automatically processed and compared with biometric templates from images of persons on a watchlist compiled by the SWP. If a match was detected, an alert would be produced and the system operator, usually a police officer, would review the images to determine whether to make an intervention, which could include using statutory powers to stop and search or arrest the person identified. The watchlist was created from images held on databases maintained by SWP, and included:

> (1) persons wanted on warrants, (2) individuals who are unlawfully at large (having escaped from lawful custody), (3) persons suspected of having committed crimes, (4) persons who may be in need of protection (e.g. missing persons), (5) individuals whose presence at a particular event causes particular concern, (6) persons simply of possible interest to SWP for intelligence purposes and (7) vulnerable persons.[173]

---

170 Thomas Poole, 'Between the Devil and the Deep Blue Sea: Administrative Law in an Age of Rights' in Linda Pearson, Carol Harlow, Michael Taggart (eds), *Administrative Law in a Changing State: Essays in Honour of Mark Aronson* (Hart Publishing, 2008) 15, 16 (citation omitted). See also Justice James Douglas, 'England as a Source of Australian Law: For How Long?' (2012) 86(5) *Australian Law Journal* 333, 345–6; Justice Susan Kiefel, 'English, European and Australian Law: Convergence or Divergence?' (2005) 79(4) *Australian Law Journal* 220, 230–2.

171 See, eg, *PBU v Mental Health Tribunal* (2019) 56 VR 141, 179–80 [126] (Bell J); *Director of Consumer Affairs Victoria v Good Guys Discount Warehouses (Australia) Pty Ltd* (2016) 245 FCR 529, 560 [117] (Moshinsky J); *Kaba* (n 155) 562 [127], 571 [155] (Bell J); *WBM* (n 132) 470 [106]–[107], 471–2 [114] (Warren CJ, Hansen JA agreeing at 475 [133]); *Caripis v Victoria Police (Health and Privacy)* [2012] VCAT 1472, [51]–[62] (Senior Member Steele); *Director of Housing v Sudi* (2011) 33 VR 559, 580–1 [100]–[101] (Maxwell P); *Griffiths v Rose* (2011) 192 FCR 130, 143–4 [38]–[39] (Perram J); *Secretary, Department of Social Security v SRA* (1993) 43 FCR 299, 320 (Black CJ, Lockhart and Heerey JJ). Whilst section 32(2) of the *Charter of Human Rights and Responsibilities Act 2006* (Vic) explicitly provides for consideration of international law, this is not the only means through which interpretations of article 8 of the *European Convention on Human Rights* ('*ECHR*') have been considered.

172 *Privacy Act* (n 67) s 6(1) (definition of 'sensitive information' and 'enforcement related activity'); *Data Protection Act 2018* (UK) ss 35–40.

173 *Bridges* (n 12) 5047 [13].

In short, counsel for Mr Bridges argued that AFR was not compatible with article 8 of the *ECHR*,[174] data protection legislation, and the Public Sector Equality Duty under the *Equality Act 2010* (UK). In a unanimous decision, the Court held that the SWP had interfered with Mr Bridges' article 8(1) rights, and that this was not 'in accordance with the law' for the purpose of article 8(2). The legal framework (comprising the *Data Protection Act 2018* (UK), the Surveillance Camera Code of Practice, and local policies promulgated by the SWP) did not provide sufficient guidance as to *who* could be put on a watchlist, and *where* AFR could be deployed – affording too broad a discretion to the police officers.[175] The Court rejected the SWP's submission 'that the present context is analogous to the taking of photographs or the use of CCTV cameras'[176] on the basis that: AFR is a novel technology; AFR processes the digital information of a large number of members of the public, where the vast majority are of no interest to the police; AFR concerns 'sensitive' personal data; and the data is processed in an automated way.[177]

The SWP had not complied with the Public Sector Equality Duty, by not taking reasonable steps to enquire about whether the AFR Locate software had a bias on racial or sex grounds – even though there was no clear evidence it was in fact biased.[178] The issue of bias will be explored in the next section. The SWP confirmed they would not seek to appeal the judgment.

Bridges is important for several reasons. It is the only judicial consideration of FRT from a common law jurisdiction, and the facts of the case provide a useful example of an application of FRT. It can provide guidance for Australian courts with respect to its approach to issues such as bias and the right to privacy. It demonstrates both the utility of having private enforcement of APPs and some of the issues facing regulators (these topics are further examined in the discussion regarding potential reforms below). It also represents a development in the jurisprudence regarding police surveillance that has not always been amenable to protecting individual privacy.[179] The Australian Human Rights Commission has reinforced the importance of ensuring accountability for 'AI-informed decision making in areas where the human rights risk is particularly high, such as … facial recognition in policing', and promoted 'international and domestic human rights law, as well as principles such as the principle of legality and the rule of law'[180] as the means of achieving this. The European Commission has stated that, for assemblies and protests, FRT 'should only be employed where such interference can be justified based on strictly proven and proportional grounds of national security or public

174 The *Human Rights Act* incorporates rights set out in the *ECHR* into domestic British law.
175 *Bridges* (n 12) 5060–1 [91]–[96].
176 Ibid 5060 [85].
177 Ibid 5060 [86]–[89].
178 Ibid 5072–80 [163]–[202].
179 See Jake Goldenfein, 'Police Photography and Privacy: Identity, Stigma and Reasonable Expectation' (2013) 36(1) *University of New South Wales Law Journal* 256.
180 'AHRC Discussion Paper' (n 3) 89.

order and should be subject to judicial review'.[181] Nevertheless, *Bridges* should not be understood as a wholesale prohibition on the use of FRT that eliminates the need for legislative intervention, as the Court was clear in confining its analysis to the particular use of FRT at issue.

D Fairness and Rationality: FRT Biases

Chief Justice French stated that 'in the sense administered by the courts' rationality means 'that official decisions comply with the logical framework created by the grant of power under which they are made', and fairness means 'that official decisions are reached fairly, that is impartially in fact and appearance and with a proper opportunity [for] persons affected to be heard'.[182]

Fairness and rationality are connected to specific grounds of review. However, there are limitations in the protection afforded by these grounds against FRT. For example, regarding procedural fairness, courts have been reluctant to consider statistical evidence in applying the rule against bias,[183] and it has been suggested that there are potentially insurmountable difficulties in applying this rule to automated decision-makers.[184] Irrationality has been called upon to prevent discrimination in judicial review cases,[185] but the support for a standalone requirement of equal treatment is limited.[186] Nevertheless, the meaning of fairness and rationality as administrative law *values* transcends these grounds to embody something broader.[187] It is helpful to consider these values together because both are underpinned by protecting broader social interests, including preventing prejudice and bias, both substantively and procedurally.[188]

Fairness, described by Chief Justice Allsop as a 'public law value', is not 'iron-clad and immutable' but rather is 'human and contextual, taking account of the

181 European Commission for Democracy through Law and Organization for Security and Co-operation in Europe Office for Democratic Institutions and Human Rights, *Guidelines on Freedom of Peaceful Assembly (3rd Edition)*, Doc No CDL-AD(2019)017, 8 July 2019, 24.

182 French, 'Themes and Values Revisited' (n 4) 37.

183 See, eg, *CMU16 v Minister for Immigration and Border Protection* (2020) 277 FCR 201; *ALA15 v Minister for Immigration and Border Protection* [2016] FCAFC 30.

184 Sarah Lim, 'Re-thinking Bias in the Age of Automation' (2019) 26(1) *Australian Journal of Administrative Law* 35.

185 See DJ Gifford, 'Discrimination as a Ground of Ultra Vires: Why Is Canada Ahead of the Rest?' (2007) 14(4) *Australian Journal of Administrative Law* 202.

186 Aronson, Groves and Weeks (n 48) 385.

187 '[L]awfulness, fairness and rationality … lie at the heart of administrative justice': *Minister for Immigration and Citizenship v Li* (2013) 249 CLR 332, 344 [14] (French CJ) ('*Li*'). 'Rationality is an inescapable requirement of official decision-making which underpins most of the traditional grounds of review': Chief Justice French, 'Themes and Values Revisited' (n 4) 46.

188 'Uncertainty of rule or outcome and inequality in inconsistences of the exercise of power are aspects of unfairness or arbitrariness': Allsop, 'Values in Public Law' (n 29) 121. Matthew Groves has argued that the jurisdictional logic of fairness has moved towards protecting broader 'social interests' as government activity can now affect people without apparently making 'decisions' in the judicial review sense: 'The Unfolding Purpose of Fairness' (2017) 45(4) *Federal Law Review* 653, 675 <https://doi.org/10.22145/flr.45.4.8>.

human context and circumstances'.[189] A lack of fairness can be informed by notions such as justice, equality and decency.[190] Elsewhere, Chief Justice Allsop has said that fairness 'is not only to be judged by analysis of the formal considerations for its exercise set by principle, but also by the daily impact upon, and reasonable perception of fairness by, those the subject of the exercise of the power'.[191] Fairness in the context of administrative law 'is premised on the view that the state and public actors are rightly held to higher moral standards than are "private" individuals. And that must be because the state is obligated to exemplify what it is to treat all citizens as equals'.[192]

Rationality can 'attract requirements of impartiality and "a certain continuity and consistency in making decisions"'.[193] It may encompass requirements of a procedural or substantive character, such as the requirements of procedural fairness, and a proscription on bias.[194] It has been suggested that it is 'irrational … to fall back on prejudice',[195] and that decisions based on prejudice are 'properly characterised as arbitrary and capricious' as they are not grounded in rationally probative evidence.[196]

Despite the difficulties in treating a FRT match as a 'decision' for the purposes of judicial review canvassed in Part I, it is submitted that systematic bias is inconsistent with the overarching administrative law values of fairness and rationality.

1 FRT Biases

Bias in FRT has more than one dimension. The majority of FRT algorithms exhibit bias: they are generally more inaccurate for faces of women, and people of colour.[197] This is because these algorithms were trained using datasets containing predominantly white male faces.[198] Whilst it may be argued that humans similarly make mistakes in identifying individuals, that is hardly a persuasive justification for using a demonstrably biased technology. Bias can also manifest where FRT is applied using watchlists developed from police databases with pre-existing racial

189 Allsop, 'The Foundations of Administrative Law' (n 50) 14–15.
190 Ibid 16.
191 Allsop, 'Values in Public Law' (n 29) 121.
192 Dyzenhaus, 'Politics of Deference' (n 133) 301.
193 *Li* (n 187) 349 [25] (French CJ), quoting DJ Galligan, *Discretionary Powers: A Legal Study of Official Discretion* (Clarendon Press, 1986) 140.
194 Ibid 350 [26] (French CJ).
195 Geoff Airo-Farulla, 'Reasonableness, Rationality and Proportionality' in Matthew Groves and HP Lee (eds), *Australian Administrative Law: Fundamentals, Principles and Doctrines* (Cambridge University Press, 2007) 212, 214 <https://doi.org/10.1017/CBO9781139168618.016>.
196 Ibid 219.
197 Patrick Grother, Mei Ngan and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (Report, December 2019); Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 *Proceedings of Machine Learning Research* 1.
198 Irina Ivanova, 'Why Face-Recognition Technology Has a Bias Problem', *CBS News* (online, 12 June 2020) <https://www.cbsnews.com/news/facial-recognition-systems-racism-protests-police-bias>.

disparity in past-crime data.[199] This bias cannot be overcome by simply improving the algorithms' accuracy.[200] Authors have suggested that FRT could enhance equality before the law as it would 'ensure consequences apply to everyone who breaches certain rules'.[201] However, history suggests that this is an overly optimistic prediction for law enforcement practices.

It is helpful to consider bias in FRT through the lens of privacy protection. Regarding anti-discrimination legislation and algorithmic bias, '[t]here are practical challenges to applying current laws [making it] difficult, if not impossible, to establish discrimination'.[202] Therefore, privacy protection can provide an alternative means of preventing discriminatory outcomes where anti-discrimination legislation falls short. Additionally, the scope for bias is particularly acute for privacy-intrusive applications of FRT. FRT can facilitate profiling on the basis of sensitive personal information including in relation to an individual's race, sex and age.[203] To address these biases, it is necessary to understand – and to regulate – the applications of FRT that enable them.

Interferences with privacy which result from misidentification can have severely detrimental implications, and the likelihood of such interferences is disproportionately increased where FRT is biased. There are already documented instances of FRT leading to false arrests, and an incorrect media release for criminal suspects.[204] This risk could extend to other more 'administrative' areas too.[205] Whilst privacy rights were arguably formulated to preserve middle-class personality from photographic intrusion,[206] as privacy entered the domain of

---

199 See Sandra G Mayson, 'Bias In, Bias Out' (2019) 128(8) *Yale Law Journal* 2218; Clare Garvie, Alvaro M Bedoya and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Report, 18 October 2016) 56.

200 Even 'low' error rates made by FRT may be several orders of magnitude greater than those made by humans, meaning cumulative biases emerge simply as a function of scale: see Oscar H Gandy, 'Engaging in Rational Discrimination: Exploring Reasons for Placing Regulatory Constraints on Decision Support Systems' (2010) 12 *Ethics and Information Technology* 29, 39 <https://doi.org/10.1007/s10676-009-9198-6>. See also *Richardson Review Report* (n 10) vol 3, 196–8.

201 Monika Zalnieriute, Lyria Bennett Moses and George Williams, 'The Rule of Law and Automation of Government Decision-Making' (2019) 82(3) *Modern Law Review* 425, 448 <https://doi.org/10.1111/1468-2230.12412>.

202 'AHRC Discussion Paper' (n 3) 78.

203 An example of disproportionate racial targeting enabled by FRT is the Chinese Integrated Joint Operations Platform: see, eg, Human Rights Watch, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App* (Web Page, 1 May 2019) <https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass>.

204 Kashmir Hill, 'Wrongfully Accused by an Algorithm', *New York Times* (online, 24 June 2020) <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>; Antonia Noori Farzan, 'Sri Lankan Police Wrongly Identify Brown University Student as Wanted Suspect in Terror Attack', *Washington Post* (online, 26 April 2019) <https://www.washingtonpost.com/nation/2019/04/26/sri-lankan-police-wrongly-identify-brown-university-student-wanted-suspect-terror-attack/>. Most of the time, however, people are not told FRT was used.

205 FRT as a 'decision-support tool' could be 'used by a customs official at an airport [to] identify an applicant as being on a security watchlist and pull up the record of that person from a database. The official might then review information in the database, question the applicant, and decide whether to admit that person to the country': Zalnieriute, Bennett Moses and Williams (n 201) 432.

206 Raymond Wacks, *Privacy: A Very Short Introduction* (Oxford University Press, 2010) 53 <https://doi.org/10.1093/actrade/9780199556533.001.0001>.

human rights this began to change. The harms of stigmatisation were increasingly recognised through a line of article 8 *ECHR* jurisprudence.[207] Underpinning this jurisprudence was an appreciation for the seriousness of interaction with the state's criminal justice or security apparatus. Relatedly, the rationale behind the *Privacy Act* is partly to ensure 'fair-information keeping practices'.[208] However, the existing paradigm has focused upon the accuracy of databases, rather than the tools or algorithms applied to these databases. Arguably, the *Privacy Act* requirements that personal information be collected only by 'lawful and fair means',[209] and that such information collected and used is 'accurate',[210] should preclude use of FRT – though it is doubtful these terms would be construed so generously. Instead, it seems that the existing privacy paradigm is inadequate to prevent misidentification arising from FRT, both at an individual and systematic level. There is little in the privacy regime that facilitates accessing the reasoning behind a decision to contest its validity for bias. Addressing the unfairness and irrationality created by uses of FRT requires a new approach.

2 Algorithmic Accountability

In Australia, there is no explicit algorithmic accountability regime.[211] It is submitted that the values of fairness and rationality should be central in addressing issues of algorithmic accountability.[212] The Administrative Review Council ('ARC') presciently recognised that the use of expert systems in assisting decisions might raise particular considerations relating to 'administrative law values such as lawfulness, fairness and rationality', 'inherent bias' and 'privacy'.[213] The ARC concluded that where expert systems are used, it would be necessary 'to ensure that administrative law values are reflected in the decision-making process'.[214]

Defining the parameters of 'fairness', however, is more contestable than simply recognising its overarching importance. Goldenfein posits 'fairness' as a legal idea that should influence both the 'individual rights to judicial remedy and the bureaucratic infrastructure of monitoring and compliance in privacy

---

207 See *PG v United Kingdom* [2001] XI Eur Court HR 195; *Perry v The United Kingdom* [2003] VI Eur Court HR 141; *Marper v United Kingdom* [2008] V Eur Court HR 1581; *R (Wood) v Metropolitan Police Commissioner* [2009] 4 All ER 951; *R (RMC) v Commissioner of Police of the Metropolis* [2012] 4 All ER 510.

208 Paterson, *FOI and Privacy in Australia* (n 18) 108.

209 *Privacy Act* (n 67) sch 1 cl 3.5 ('*Australian Privacy Principles*').

210 *Australian Privacy Principles* (n 209) cl 10.2.

211 Jake Goldenfein, 'Algorithmic Transparency and Decision-Making Accountability: Thoughts for Buying Machine Learning Algorithms' in Cliff Bertram, Asher Gibson and Adriana Nugent (eds), *Closer to the Machine: Technical, Social, and Legal Aspects of AI* (Office of the Victorian Information Commissioner, 2019) 41, 47.

212 The ALRC is considering an inquiry into 'whether reforms are necessary to ensure that automated decisions by government agencies are fair, transparent, accountable, and timely': Australian Law Reform Commission, *The Future of Law Reform: A Suggested Program of Work 2020–25* (Report, December 2019) 24.

213 Administrative Review Council, *Automated Assistance in Administrative Decision Making: Report to the Attorney-General* (Report No 46, November 2004) 23–4, 28.

214 Ibid 48.

and data protection [and should be] incorporated into the profiling technologies themselves'.[215] He presents '[f]airness as a proxy for non-discrimination'.[216] Under this approach, achieving fairness involves 'exposing and limiting bias and prejudice in the data sets used in machine learning or produced by the working of machine learning models'.[217] Ultimately though 'fairness has to be optimised towards one outcome or another'.[218] There is a growing body of literature examining the inevitable trade-offs for particular optimisations of fairness.[219] In the context of FRT, decisions must be made regarding trade-offs in the two types of errors, ie, false matches and false mismatches (this requires adjusting acceptable similarity score thresholds, and acceptable error rates) – there is no single setting which eliminates all errors.

Relevantly for FRT purposes, three possible 'solutions' to achieving algorithmic accountability involve: training the algorithms on representative datasets, incorporating a 'human-in-the-loop', and increased transparency. But these solutions are not without difficulties.

Using representative datasets to remove discrimination in the sense of disproportionate error rates across races and genders risks justifying the proliferation of these systems and increasing their social acceptance without addressing underlying biases which they can exacerbate. Focusing on fairness in this narrow sense, whereby companies can rebrand and promote 'non-discriminatory' FRT, gives the illusion that a technological fix is within reach, and shifts accountability to the algorithms' designers.[220]

Integrating a 'human-in-the-loop' is also seen as a useful safeguard,[221] however it is not the panacea of algorithmic accountability that some suggest. The problem is that 'technologically intermediated observation may appear more "objective": it appears to attest to a victory of rational analysis'.[222] This appearance of objectivity can lead to automation bias.[223] The decision in *Bridges* reflects a firm grasp of the

---

215 Jake Goldenfein, *Monitoring Laws: Profiling and Identity in the World State* (Cambridge University Press, 2019) 115 <https://doi.org/10.1017/9781108637657>.

216 Ibid 167.

217 Ibid 129.

218 Ibid 130.

219 See, eg, Arvind Narayanan, 'Translation Tutorial: 21 Fairness Definitions and Their Politics' (Speech, Fairness, Accountability and Transparency Conference, New York, 23 February 2018); Sahil Verma and Julia Rubin, 'Fairness Definitions Explained' (Conference Paper, ACM/IEEE International Workshop on Software Fairness, May 2018) 1 <https://doi.org/10.1145/3194770.3194776>.

220 Julia Powles and Helen Nissenbaum, 'The Seductive Diversion of "Solving" Bias in Artificial Intelligence', *OneZero* (Web Page, 8 December 2018) <https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53>. Cf European Commission, 'White Paper on Artificial Intelligence: A European Approach to Excellence and Trust' (Paper, 12 February 2020) 10–11.

221 See, eg, *GDPR* (n 116) art 22; *Richardson Review Report* (n 10) vol 3, 193.

222 Antoinette Rouvroy, 'Technology, Virtuality and Utopia: Governmentality in an Age of Autonomic Computing' in Mireille Hildebrandt and Antoinette Rouvroy (eds), *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology* (Routledge, 2011) 119, 127.

223 Peter Fussey and Daragh Murray, 'Policing Uses of Live Facial Recognition in the United Kingdom' in Amba Kak (ed), *Regulating Biometrics: Global Approaches and Urgent Questions* (AI Now Institute, September 2020) 78.

issues attending reliance on a human-in-the-loop, and avowedly 'representative' datasets. Though bias was considered in the context of the Public Sector Equality Duty, the Court's findings are of broader relevance. The Court highlighted the inadequacies in the 'human failsafe' requiring humans to decide to act on a positive match before making an intervention, recognising that 'human beings can also make mistakes' – particularly in the context of identification.[224] Whilst there was no evidence of actual bias in the technology's application, the SWP 'never sought to satisfy themselves, either directly or by way of independent verification, that the software programming in this case does not have an unacceptable bias on grounds of race or sex'.[225] The SWP's reliance on the assurances of the algorithm's designer was unsatisfactory.[226]

Increased transparency is also touted as essential to achieving algorithmic accountability. For example, the Hon Robert French noted: 'AI's role in decision-making should be transparent – Each individual should have access to the rationality behind a decision being made. The process needs to be transparent and easily understood by society'.[227] However, achieving meaningful societal understanding is vexed. In the US, suggestions to increase transparency include creation of a '[Food and Drug Administration] for algorithms',[228] and 'model cards' – ie, documents accompanying algorithms that provide benchmarked evaluation in a variety of conductions, such as across different race or gender groups.[229] But in practice governments may seek to avoid transparency, sheltering behind over broad assertions of trade secrecy or claims that full disclosure may enable criminals and terrorists to circumvent the system.[230] Others have cautioned that 'we are in danger of creating a "meaningless transparency" paradigm to match the already well known "meaningless consent" trope'.[231] The meaning of transparency as an administrative law value, the limitations of consent, and government efforts to avoid full disclosure, will each be further explored in the next section.

---

224 *Bridges* (n 12) 5077 [185], referring to the 'well-known warnings which need to be given to juries in criminal trials about how identification can be mistaken, in particular where a person has never seen the person being identified before: see *R v Turnbull* [1977] QB 224'.

225 *Bridges* (n 12) 5079 [199].

226 Ibid 5078–9 [195]–[199].

227 Robert French, 'Rationality and Reason in Administrative Law: Would a Roll of the Dice be Just as Good?' (Australian Academy of Law Annual Lecture, 29 November 2017) 3 ('Rationality and Reason in Administrative Law'), quoting Big Innovation Centre, *Ethics and Legal in AI: Decision Making and Moral Issues* (Report, 27 March 2017) 6. See also Bruno Lepri et al, 'Fair, Transparent, and Accountable Algorithmic Decision-Making Processes: The Premise, the Proposed Solutions, and the Open Challenges' (2018) 31(4) *Philosophy and Technology* 611 <https://doi.org/10.1007/s13347-017-0279-x>; Bill C-11, *An Act to Enact the Consumer Privacy Protection Act and to Make Consequential and Related Amendments to Other Acts*, 2nd sess, 43rd Parl, 2020, cl 63(3); *Richardson Review Report* (n 10) vol 3, 198.

228 Andrew Tutt, 'An FDA for Algorithms' (2017) 69(1) *Administrative Law Review* 83, 109–11.

229 Margaret Mitchell et al, 'Model Cards for Model Reporting' (Conference Paper, Conference on Fairness, Accountability, and Transparency, 29 January 2019).

230 Robert Brauneis and Ellen P Goodman, 'Algorithmic Transparency for the Smart City' (2018) 20 *Yale Journal of Law and Technology* 103, 160 <https://doi.org/10.31228/osf.io/fjhw8>.

231 Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to Explanation" is Probably Not the Remedy You Are Looking For' (2017) 16(1) *Duke Law and Technology Review* 18, 23 <https://doi.org/10.31228/osf.io/97upg>.

E Openness: The Capability

There is widespread consensus that the values of administrative law include openness or transparency.[232] These terms will be used interchangeably. Though often associated with FOI provisions, such provisions are only one illustration of the value – not its sole source.[233] Transparency is of broader relevance to administrative law, through notions such as 'explainability' (which may be relevant to bias) and open government requirements for proactive publication of information.[234] The realisation of other values, such as accountability and lawfulness, is often contingent on openness. Mechanisms of the new administrative law, such as the OAIC, 'have given added vitality to [the] administrative law [value]' of transparency.[235] It has been said that '[o]ne of the best-known aspects of the rule of law is that governments must be transparent … Transparency requires publicity about the operation of the state'.[236] Clearly, governmental transparency must be balanced against other considerations in areas such as law enforcement and national security. It is, however, questionable whether the Government's current approach to implementing FRT strikes an appropriate balance. As discussed in Part IV(A), the *Privacy Act* is limited in its ability to require transparency for various government activities. Given the highly privacy-intrusive potential of FRT the countervailing need for transparency is magnified, because '[s]unlight is said to be the best of disinfectants'.[237]

1 The Capability

On 5 October 2017, the Council of Australian Governments signed an agreement to establish a National Facial Biometric Matching Capability (widely dubbed 'The Capability'). The purpose of this agreement is 'to promote the sharing and matching of identity information to prevent crime, support law enforcement, uphold national security, promote road safety, enhance community safety and improve service delivery'.[238] The Department of Home Affairs will create and maintain the facilities for government agencies to conduct one-to-one and one-to-many facial recognition matches in certain circumstances.

---

232 'Openness' is used by: Aronson, Groves and Weeks (n 48) 4; French, 'Themes and Values Revisited' (n 4) 37; Taggart, 'The Province of Administrative Law Determined' (n 49) 4. 'Transparency' is used by: Daly, 'A Values-Based Approach' (n 50) 25; Perry, 'Key Values in the Digital Era' (n 50) 2; Cane (n 50) 16. The terms are treated interchangeably by the *ARC Report 46* (n 50) 3, listing the value as 'openness (or transparency)', and by Harlow (n 50) 193 stating 'openness, or (in more fashionable terminology) transparency'.

233 Paul Craig, 'Theory and Values in Public Law: A Response' in Paul Craig and Richard Rawlings (eds), *Law and Administration in Europe: Essays in Honour of Carol Harlow* (Oxford University Press, 2003) 3, 24.

234 McMillan, 'The Impact of Technology on the Administrative Justice System' (n 55) 11.

235 Ibid 12.

236 Zalnieriute, Bennett Moses and Williams (n 201) 429–30.

237 Louis D Brandeis, *Other People's Money and How the Bankers Use It* (Fredrick A Stokes, 1914) 92.

238 Council of Australian Governments, 'Intergovernmental Agreement Identity Matching Services' (Intergovernmental Agreement, 5 October 2017) 2.

The Federal Government has sought to implement legislation underpinning The Capability.[239] But the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') did not support the Bill, stating that 'a significant amount of re-drafting and not simpl[y] amending' was required.[240] The PJCIS considered that the following broad principles 'should be used as a template for the re-drafting':

- the regime should be built around privacy and transparency,
- the regime should be subject to Parliamentary oversight and reasonable, proportionate and transparent functionality, and
- the regime should be one that requires reporting on the use of the identity-matching services.[241]

Evidently, transparency was central to the PJCIS's (and many submitters') concerns. Despite the legislation not being passed, Home Affairs has pushed ahead with a request for tender seeking service provider for The Capability.[242] Given the potentially forthcoming redrafting, this article will not rehash each of the criticisms made against the previous Bills. Nevertheless, it is useful to examine some of the concerns arising from the guiding Council of Australian Governments agreement and aspects of its implementation that are hard to reconcile with the value of transparency.

2 Transparent Implementation and Operation?

The Federal Government has sought to avoid transparency in a number of respects. Home Affairs claimed immunity under Commonwealth procurement rules not to disclose the FRT algorithm and its vendor, purportedly to reduce potential vectors of attack. Home Affairs has stated that the Bill is not intended to govern the full use of identity-matching services, ie, it 'seeks to *enable* rather than *authorise* the use of the services by various government agencies',[243] instead pointing to the *Privacy Act* as the source of relevant protections.[244] Whilst these protections are applicable to some agencies, this broad defence by reference to the *Privacy Act* is somewhat disingenuous. Home Affairs commissioned a Privacy Impact Assessment (released under FOI) which highlighted the various exemptions and exceptions for law enforcement, crime and anti-corruption agencies in the *Privacy Act*, and noted that

---

239 The Identity-Matching Services Bill 2018 (Cth) and Australian Passports Amendment (Identity-Matching Services) Bill 2018 (Cth) were not debated, and lapsed at the dissolution of Parliament on 11 April 2019. The same terms were replicated in the Identity-Matching Services Bill 2019 (Cth) and Australian Passports Amendment (Identity-Matching Services) Bill 2019 (Cth), which were introduced into the House of Representatives on 31 July 2019.

240 Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Identity-Matching Services Bill 2019 and the Australian Passports Amendment (Identity-Matching Services) Bill 2019* (Report, October 2019) 75 [5.4] ('*Report on IMS Bill*').

241 Ibid 76 [5.5].

242 Department of Home Affairs (Cth), 'Request for Tender for Permissions Capability' (Request No HOMEAFFAIRS/2054/RFT, 23 October 2020).

243 Department of Home Affairs (Cth), Submission No 12 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into the Identity-Matching Services Bill 2018* (April 2018) 5 (emphasis in original) ('DHA Submission to PJCIS').

244 Ibid 13.

> references to privacy law compliance within the FMS Data Sharing Agreement will be illusory (not to mention potentially misleading if these give an impression that an exempt or partially exempt LECAC agencies are subject to privacy legislation, regulatory oversight, and so on).[245]

Instead, if The Capability is to proceed, it would be appropriate to include proper privacy protections within the new legislation, or to establish a new framework for FRT regulation.

Whether The Capability is properly characterised as a database is dubitable. The Minister for Home Affairs stated that '[t]he hub is not a database and does not conduct any facial biometric matching. Rather, it acts like a router, transmitting matching requests … These databases conduct the matching using facial recognition software'.[246] Presumably Home Affairs consider this characterisation appropriate to distance themselves from perceptions that they oversee and control The Capability. Regardless, the Parliamentary Joint Committee on Human Rights expressed concerns that a 'centralised facility for searching such large repositories of facial images and biometric data is a very extensive limitation on the right to privacy' and raised the 'serious question as to whether [it] is the least rights restrictive approach to achieving the stated objectives of the measure'.[247]

A controversial aspect of the proposed Bill was the power for the Minister to arrange for use of computer programs to make decisions, enabling automated decision-making. The explanatory memorandum provided that this provision is intended for 'low-risk decisions',[248] and the Department of Foreign Affairs and Trade stated that in practice it would only be able to automate decisions producing favourable or neutral outcomes for the subject,[249] though it is not clear why this practice is required beyond internal policy. Other submitters conveyed concern about the lack of procedural fairness criteria included in the Bill.[250] Ultimately, the PJCIS recommended amending the provision to ensure it could only be used for favourable or neutral outcomes, and would not generate a reason to seek review.

3 Consent

There is insufficient transparency regarding the management of consent for The Capability. This compromises the administrative law value of openness because it impinges upon individuals' understanding of, and engagement with, operations of the Government directly affecting them. The particular issues regarding consent and The Capability are twofold. First, The Capability is premised upon a 're-purposing'

---

245 Bainbridge Associates, *Privacy Impact Assessment: Law Enforcement, Crime and Anti-Corruption Agency Use of the Face Matching Services, NFBMC (v.1.o)* (Report, March 2019) 37.

246 Commonwealth, *Parliamentary Debates,* House of Representatives, 7 February 2019, 486 (Peter Dutton).

247 Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Human Rights Scrutiny Report* (Report No 3, 27 March 2018) 46 [1.145].

248 Explanatory Memorandum, Australian Passports Amendment (Identity-Matching Services) Bill 2019 (Cth) 9, discussing proposed section 56A for the *Passports Act 2005* (Cth).

249 Department of Foreign Affairs and Trade, Submission No 15 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into the Australian Passports Amendment (Identity-Matching Services) Bill 2018* (April 2018) 9.

250 See Parliamentary Joint Committee on Intelligence and Security, *Report on IMS Bill* (n 240) 95–6.

of government-held images for uses outside the initial purpose of collection – relying on a dubious secondary consent. Home Affairs explained that it would be impractical to 'collect consent directly from individuals for the secondary use of their information in the identity-matching services' as it is merely the 'facilitator' of the hub.[251] However, it is doubtful that individuals would reasonably expect their information to be used for this secondary purpose.[252]

Second, in the limited instances where agencies using The Capability must obtain consent, it is ambiguous whether individuals will have a genuine choice to withhold consent if they wish to access the relevant service, and how consent will be recorded and verified. The previous Bills lacked sufficient transparency, in that 'invisible' searches could be made, and the consent and notice requirements were inadequate.[253] Arguably, 'consent is a broken regulatory mechanism for facial surveillance'.[254] It is hard to view the current approach to implementing The Capability as consistent with *Privacy Act* obligations for 'open and transparent management of personal information', but perhaps this also reflects difficulties in the current provisions' operation.[255]

4 Function Creep

Whilst Home Affairs dismissed submitters' concerns that The Capability might be used for blanket surveillance as 'infeasible',[256] there is a real risk of function creep. It is important to understand The Capability against a backdrop of increasing biometric data collection and information sharing between government agencies. FRT is already used for verification purposes by the Australian Tax Office and Australia Post,[257] and Airport 'SmartGates'.[258] The Federal Government has launched a new Enterprise Biometric Identification Services system for international travel and visa clearances, to 'become a world leader in the delivery of biometric collection, processing and matching services'.[259] The *Migration Act*

---

251 Department of Home Affairs (Cth), Submission No 12.1 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into the Identity-Matching Services Bill 2018: Supplementary Submission* (May 2018) 7 [29] ('DHA Submission to PJCIS No 12.1').

252 Cf *Australian Privacy Principles* (n 209) cl 6.1 (nor is this secondary purpose 'directly related to the primary purpose'. Cf *Australian Privacy Principles* (n 209) cl 6.2(a)(i)).

253 Parliamentary Joint Committee on Intelligence and Security, *Report on IMS Bill* (n 240) 81.

254 Evan Selinger and Woodrow Hartzog, 'The Inconsentability of Facial Surveillance' (2019) 66 *Loyola Law Review* 101, 101. The limitations of consent more broadly were recently discussed in Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (n 146) 23. Following this, the Federal Attorney-General's Department has questioned 'is consent an effective way for people to manage their personal information?': Attorney-General's Department (Cth), '*Privacy Act* Review' (n 65) 48.

255 APP 1 is broadly worded, and largely relates to privacy policies: *Australian Privacy Principles* (n 209) cl 1. For 2019–20, only 0.8% of privacy complaints to the OAIC involved APP 1: Office of the Australian Information Commissioner, *Annual Report 2019–20* (Report, 2020) 134.

256 DHA Submission to PJCIS No 12.1 (n 251) 15.

257 Digital Transformation Agency, 'Digital Identity', *Our Projects* (Web Page) <https://www.dta.gov.au/our-projects/digital-identity>.

258 Australian Border Force, 'SmartGates', *Entering and Leaving Australia* (Web Page, 23 September 2019) <https://www.abf.gov.au/entering-and-leaving-australia/smartgates>.

259 Alex Hawke, 'Enormous Boost to Australia's Biometric Capability' (Media Release, Assistant Minister for Home Affairs, 19 March 2018).

1958 (Cth) authorises immigration officials to collect biometric data from citizens and non-citizens entering or leaving Australia – this can include face images.[260] In 1983, the ALRC cautioned about the risks of 'matching', warning that 'new technology would no doubt make it easier for authoritarian control of society – provided that other factors were present'.[261] Recently, the Federal Government has announced plans for a Data Availability and Transparency Bill 2020 (Cth) for the sharing of data between the public sector. Intelligence agencies already have wide powers to access public sector information under, inter alia, the *Office of National Intelligence Act 2018* (Cth), which is 'facilitated and empowered by a weak, discretionary and ministerial based privacy rules model'.[262] These reforms feed into what Carne describes as 'a subtle reconstruction of Australian governance through an increasing elevation of security matters in the Australian polity and integration of intelligence with government decision making in even routine and mundane transactions'.[263] The difficulties of subjecting to review administrative decisions taken in the course of co-operation between governments in a federation have long been recognised.[264] Ultimately, though, apprehension regarding potential future expansions of The Capability should not distract from current uses of FRT by the public sector. The risk that government agencies will effectively outsource their functions to private companies offering FRT services has already materialised.

F Good Faith: Clearview AI

Though 'difficult to define', Chief Justice French explains that good faith 'has a core meaning, in ordinary usage, of honesty with fidelity and loyalty to something – a promise, a commitment or a trust'.[265] Elsewhere, his Honour has observed that the characterisation of conduct as done in good faith 'inevitably requires judgments which are normative or evaluative in character and cannot be explained only by the application of legal rules with logically mandated outcomes'.[266] Ombudsmen assessing whether conduct was fair and reasonable may focus on considerations such as 'integrity – including that the conduct was made or done in good faith'.[267]

---

260 *Migration Act 1958* (Cth) s 257A. See also *Migration Amendment (Strengthening Biometrics Integrity) Act 2015* (Cth).

261 *ALRC Report 22* (n 20) vol 1, 19.

262 Carne (n 81) 146.

263 Ibid 159–60. More recently, the *Richardson Review Report* (n 10) recommended that these privacy rules be amended to better deal with reference information, ie, personal information obtained or retained for performance of general agency functions: *Richardson Review Report* (n 10) vol 3, 83–110 (Recommendations 139–41). And that Intelligence Agencies 'should be required, by legislation, to have legally-binding privacy guidelines or rules' that are made public: *Richardson Review Report* (n 10) vol 4, 52 (Recommendation 189).

264 Cheryl Saunders, 'Administrative Law and Relations between Governments: Australia and Europe Compared' (2000) 28(2) *Federal Law Review* 263, 264 <https://doi.org/10.22145/flr.28.2.6>.

265 French, 'Themes and Values Revisited' (n 4) 41.

266 French, 'Rationality and Reason in Administrative Law' (n 227) 10. Good faith requires 'more than the absence of bad faith. It requires a conscientious approach to the exercise of power': *WAFV v Refugee Review Tribunal* (2003) 125 FCR 351, 371 [52] (French J).

267 Chris Wheeler, 'What Is "Fair" and "Reasonable" Depends a Lot on Your Perspective' (2014) 22(1) *Australian Journal of Administrative Law* 63, 68.

It has been said that 'the government above all other bodies in our community should lead by example; it should act, and be seen to act, fairly and in good faith with all members of the community with whom it deals in individual cases'.[268] Despite the potential breadth of the meaning of good faith, it is conceded that this alignment of an issue, ie, Clearview AI, and the final administrative law value listed by Chief Justice French is perhaps strained. However, the use of Clearview AI by government agencies, and the response from the OAIC, is worth addressing.

On 9 July 2020, the OAIC and the UK's Information Commissioner's Office opened a joint investigation into Clearview AI. Clearview AI provides a facial recognition app which allows users to upload an individual's photo and match it using over three billion images that Clearview AI 'scraped' from various social media platforms and other websites. The extent of Clearview AI's integration with public sector agencies across the world was only revealed after a data breach disclosed 2,228 public and private institutions had created accounts, and collectively performed nearly 500,000 searches – each tracked and logged by the company.[269] The data breach itself highlights the risks for governmental reliance on outsourced technological arrangements. Subsequently, multiple lawsuits have been filed in US courts.[270] In Canada, the Office of the Privacy Commissioner launched investigations into Clearview AI and the Royal Canadian Mounted Police's use of Clearview AI. On 14 October 2021, the OAIC determined that Clearview AI failed to comply with several APPs and declared it must cease the acts found to interfere with privacy and destroy all scraped images collected from individuals in Australia.[271] Curiously, the investigation was confined to Clearview's scraping of data from the internet, rather than the government agencies using the technology in Australia or the UK.[272] This is despite the fact that members of Australian police forces have run over 1,000 searches using Clearview AI, notwithstanding their initial statements to the contrary (and internal bemusement at these dishonest statements).[273]

This outsourcing of identification functions to a private company is part of an increasing governmental use of commercial proprietary software, that can enable departments to avoid proper scrutiny. This shift can be placed within a

---

268 Paul Finn and Kathryn Jane Smith, 'The Citizen, the Government and "Reasonable Expectations"' (1992) 66(3) *Australian Law Journal* 139, 146.

269 Ryan Mac, Logan McDonald and Caroline Haskins, 'Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA', *Buzzfeed News* (online, 27 February 2020) <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement>.

270 Kashmir Hill, 'Facial Recognition Start-Up Mounts a First Amendment Defense', *New York Times* (online, 11 August 2020) <https://www.nytimes.com/2020/08/11/technology/clearview-floyd-abrams.html>.

271 *Commissioner Initiated Investigation into Clearview AI, Inc (Privacy)* [2021] AICmr 54. The APPs Clearview AI failed to comply with were APP 1.2, APP 3.3–3.5, APP 5, and APP 10.2: APP (n 206).

272 Though the OAIC acknowledged that Victoria Police, Queensland Police Service and South Australia police used the tool: *Commissioner Initiated Investigation into Clearview AI, Inc (Privacy)* (n 271) [8].

273 Internal emails released under FOI revealed comments such as, '[m]aybe someone should tell the media that we are using it!' and '[o]r should we stop using it since everyone is raising the issue of approval :)': Ariel Bogle, 'Documents Reveal AFP's Use of Controversial Facial Recognition Technology Clearview AI', *ABC News* (online, 13 July 2020) <https://www.abc.net.au/news/2020-07-13/afp-use-of-facial-recocognition-sofware-clearview-ai-revealed/12451554>.

broader movement towards 'the phenomenon of … mixed administration'[274] – a phenomenon Taggart argues Australian courts have failed to properly engage with.[275] It is hard to reconcile the police forces' secretive outsourcing of functions with broader understandings of good faith. Nevertheless, Clearview AI is not the only company offering such services to the public sector, nor are these privacy-invasive FRT uses limited to police. Therefore, addressing these issues of FRT requires more than targeting individual companies. Reform is needed to provide a framework that covers both the public and private sector.

V PROPOSALS

A Another Agency?

A number of authors have suggested that the issues FRT presents should be addressed by establishing a new oversight body in Australia. There have been calls for a 'Biometrics Commissioner'[276] akin to the model used in the UK. Others have suggested an 'AI Safety Commissioner'.[277] This article, however, argues against establishing a new specialist commissioner. Instead, it is preferable to expand the remit and resourcing of existing regulatory bodies, particularly the OAIC, for a number of reasons.

First, the UK model suffers from serious deficiencies – the role is limited to oversight of *police use* of *DNA and fingerprints*.[278] Consequently, the UK Commissioner has been very constrained in affecting the implementation of new biometric technologies such as FRT.[279] Recently, the Biometrics and Surveillance Camera Commissioners have been combined as a cost-saving measure, despite objections from both current Commissioners.[280] Establishing an ineffective commissioner in Australia could be worse than having no commissioner if it creates the illusion that a rigorous accountability body exists. Second, assuming that a new

---

274 Michael Taggart, '"Australian Exceptionalism" in Judicial Review' (2008) 36(1) *Federal Law Review* 1, 24 <https://doi.org/10.22145/flr.36.1.1>.

275 Ibid 20.

276 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* 121, 143 <https://doi.org/10.53637/KAVV4291>. This has also been supported by submitters to the Parliamentary Joint Committee on Intelligence and Security, *Report on IMS Bill* (n 240) including: Future Wise and the Australian Privacy Foundation; the Law Council of Australia; the NSW Council for Civil Liberties, Liberty Victoria, Queensland Council for Civil Liberties, South Australian Council for Civil Liberties, Australian Council for Civil Liberties.

277 'AHRC Discussion Paper' (n 3) 192 (Proposal 19). This has also been supported by submitters, including: the Australian Privacy Foundation, Queensland Council for Civil Liberties, Liberty Victoria, New South Wales Council for Civil Liberties, Electronic Frontiers Australia; the Australia Institute; the University of Melbourne; Digital Rights Watch; Access Now; and the NSW Bar Association.

278 *Protection of Freedoms Act 2012* (UK) s 20.

279 *Wiles Report* (n 128) 3.

280 Samuel Rowe and Jessica Jones, 'The Biometrics and Surveillance Camera Commissioner: Streamlined or Eroded Oversight?', *Ada Lovelace Institute* (Web Page, 9 October 2020) <https://www.adalovelaceinstitute.org/the-biometrics-and-surveillance-camera-commissioner-streamlined-or-eroded-oversight/>.

commissioner's role would include oversight of FRT, the issue of multiple regulators with overlapping functions remains. This can create problems for: individuals to understand their rights and know where to enforce them; organisations who must bear greater compliance costs; and regulators who may unnecessarily duplicate effort and resource expenditure.[281] Third, and relatedly, the costs of establishing and operating such bodies are significant. For this reason, 'the proliferation of statutory authorities is not desirable'.[282] Justice Kirby cautioned that '[t]he easy thing for lawmakers to do is to establish a bureaucracy with attractive titles, set up with fanfare announcing that information is free and privacy henceforth is guaranteed'.[283] A new agency would lack the profile and governmental ties of an existing agency such as the OAIC.[284]

Many of the arguments against establishing a new agency lend support to strengthening the OAIC. Already, 'the OAIC's regulatory role includes handling complaints, conducting investigations, monitoring, advice and providing guidance on proposed uses of biometric information [and] conduct[ing] assessments of the handling of personal biometric information collected through and used in facial recognition technology'.[285] Since its inception, there has been an increase in the 'functions and powers for the Commissioner, although not always a commensurate increase in resources'.[286] The OAIC is best placed to achieve the values of accessibility and accountability, provided that underlying matters are addressed, such as its ability to address systematic issues, its potentially over-conciliatory enforcement approach, and its resourcing shortfalls.

Lessons can also be learned from the Commonwealth Ombudsman – an institution with close parallels to the OAIC. One of the strengths of Commonwealth Ombudsmen is their 'capacity to move beyond their originally conceived mandate, to attract new jurisdictions from governments and to constantly redevelop and refine their mission and purpose'.[287] For example, the Commonwealth Ombudsman's oversight functions have expanded to include inspecting Australian Federal Police and Australian Crime Commission records to ensure their use of telecommunications interceptions and surveillance devices is lawful. Extending these powers, either within the Commonwealth Ombudsman or the OAIC, to cover an auditing role for FRT is desirable. The Commonwealth Ombudsman's position as 'a generalist agency, hosting a cluster of specialities'[288] exemplifies the advantages – such as enhanced coordination, expertise in administration, and

281 *ALRC Report 108* (n 32) vol 1, 487, 506. See also AJ Brown (n 100) 308.
282 *ALRC Report 22* (n 20) vol 2, 10.
283 Kirby (n 30) 757.
284 The importance of public profile should not be understated, because it enhances accessibility and newer bodies are more susceptible to abolition: see Weeks (n 27) 43.
285 OAIC Submission No 108 (n 80) 8. Note, however, that this monitoring role does not currently extend beyond the information collected, to cover the actual FRT used.
286 *ALRC Report 108* (n 32) vol 2, 1516.
287 Rick Snell, 'Australian Ombudsman: A Continual Work in Progress' in Matthew Groves and HP Lee (eds), *Australian Administrative Law: Fundamentals, Principles and Doctrines* (Cambridge University Press, 2007) 100, 100 <https://doi.org/10.1017/CBO9781139168618.008>.
288 Ibid 111 (citations omitted).

public profile – from hosting multiple specialities within a single agency. Stuhmcke has observed that '[i]n handling complaints against agencies, in initiating own motion investigations and in auditing administrative decision-makers ombudsmen aim to embed principles of administrative law which include fairness, rationality, lawfulness, transparency and efficiency'.[289] The OAIC can similarly aim to embed these values. Nevertheless, the challenges presented by FRT cannot be overcome by total reliance on the OAIC's enforcement of the *Privacy Act.*

B Legislative Reform

1 Private Enforcement

A possible means of improving participation would be to enable individuals to privately enforce the APPs, without having to rely on the OAIC. Beyond enhancing participation, this reform would be beneficial in reducing the burden on the OAIC; providing an additional incentive for organisations to comply with APP obligations; and facilitating the development of a richer body of jurisprudence clarifying the operation of *Privacy Act*. This proposal is gaining support[290] and could potentially sidestep the legal and political quagmire besetting implementation of a statutory tort. Private enforcement of the privacy principles is possible in the UK. It has been said that the 'balance between collective security and individual data privacy rights in the UK are fairly stable because of the role of judicial review, judicial independence and the overarching scrutiny provided by commissioners'.[291]

Alternatively (or additionally) reconsideration could be given to proposals for a federal Bill of Rights, or less radically, amendment to the *AD(JR) Act* to make Australia's international human rights obligations, or a consolidated list of those obligations, a relevant consideration in government decision-making.[292]

2 A Specific Regime

There is a strong case that regulation of FRT requires a specific regime, or at least significant amendments to the *Privacy Act* to ensure FRT is used accountably. In Australia, the Richardson Review recently recommended that National Intelligence Community agencies' develop 'governance and ethical frameworks for the use of artificial intelligence capabilities', particularly given the risk that unconstrained use of technology such as FRT may enable mass surveillance.[293] There

289 Anita Stuhmcke, 'Ombudsmen and Integrity Review' in Linda Pearson, Carol Harlow, Michael Taggart (eds), *Administrative Law in a Changing State: Essays in Honour of Mark Aronson* (Hart Publishing, 2008) 349, 376.

290 See '*Privacy Act* Review' (n 65) 67–9; Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (n 146) 473–4.

291 Simon Hale-Ross, *Digital Privacy, Terrorism and Law Enforcement: The UK's Response to Terrorist Communication* (Routledge, 2019) 136.

292 National Human Rights Consultation Committee, *National Human Rights Consultation Report* (September 2009) 183. This was recently endorsed in Ng et al (n 8) 1073.

293 *Richardson Review Report* (n 10) vol 3, 190–3.

have been calls for targeted legislation in foreign jurisdictions.[294] Scotland recently passed legislation to enhance the accountability and transparency of police use of biometric data, including facial images, with a view to further expansion across the public sector.[295] Whilst the *Privacy Act* was intended to be 'technology neutral', and there are disadvantages in a fragmented patchwork for privacy protection, the unique nature of many issues associated with FRT necessitates unique solutions. For example, the issues associated with biased algorithms and misidentification are not solely issues of privacy. In any event, there already exists a number of other statutes that may be understood as providing privacy protection for specific technologies or types of information not clearly covered by the *Privacy Act*.[296]

This article does not propose to draft the minutiae of a new regime, however some key points are worth noting. A framework should operate according to classification by risk and intended use.[297] For example, the privacy intrusiveness and severity of misidentification are more significant for FRT used by law enforcement in a one-to-many live identification at a public protest, than FRT used by an individual for one-to-one verification to access their myGov account. Use of one-to-many should be restricted to serious crimes.[298] Additionally, it may be necessary to draft a regime to include remote biometrics generally, given the development of tools such as voice recognition, gait analysis, and iris analysis.

Processes should be implemented to trial and evaluate such technologies to ensure they operate in a fair and rational manner without simply relying on developers' assurances. As noted above, auditing or monitoring of higher risk FRT uses could be overseen by Ombudsmen or the OAIC – whilst 'this has hitherto not been the prime focus of attention for administrative law … it is significant that ombudsmen and other investigation offices … have moved to institute regular auditing of action by government agencies'.[299] Warrants could be required for one-to-many uses of FRT, which would be approved by an issuing authority such as members of the judiciary or the AAT. This could provide a useful accountability check, that is itself subject to judicial review, provided it does not collapse into a rubber-stamping exercise.[300]

---

294 In the United Kingdom, see Parliament of the United Kingdom, 'The Future of Biometrics' (Briefing Summary, 6 February 2019). In the US, see Jameson Spivack and Clare Garvie, 'A Taxonomy of Legislative Approaches to Face Recognition in the United States' in Amba Kak (ed), *Regulating Biometrics: Global Approaches and Urgent Questions* (AI Now Institute, September 2020) 86. In the European Union, see European Union Agency for Fundamental Rights, *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement* (Report, 21 November 2019) 33.

295 *Scottish Biometrics Commissioner Act 2020* (Scot).

296 At the Commonwealth level, examples include the: *Telecommunications (Interception and Access) Act 1979* (Cth); *Surveillance Devices Act 2004* (Cth); *Crimes Act 1914* (Cth) pt ID; *Data-Matching Program (Assistance and Tax) Act 1990* (Cth).

297 Learned-Miller et al (n 16) 23–30; Amba Kak, 'State of Play' (n 16) 30.

298 Garvie, Bedoya and Frankle (n 199) 63.

299 Creyke (n 26) 130.

300 '[F]rankly, the ambit of federal search warrants can now be so wide as to offer no practical constraints': Mark Aronson, Matthew Groves and Greg Weeks, *Judicial Review of Administrative Action and Government Liability* (Thomson Reuters, 6th ed, 2017) 368–9.

VI CONCLUSION

Concerns about the widespread implementation of FRT should not be dismissed as mere Luddism – the technology has the capacity to infringe upon individuals' right to privacy, and lead to biased outcomes. Permitting uncontrolled development because of an acceptance of technological determinism is no solution. Conversely, unconditional bans disregarding the needs of effective government, and potential applications that are in the public interest, are unworkable and undesirable. The challenge often presented by new technologies is that they ostensibly operate in a legal vacuum. By reorienting the focus to administrative law and its values, it is hoped that the novel challenges presented by FRT may be positioned within a clearer existing legal framework. This article has assumed that the merit of these administrative law values is self-evident, and that seeking to institutionalise them is beneficial. Whilst these values are not immutable, they carry a certain degree of stability that is useful in providing a consistent approach to regulating new technologies now and in the future. Legislation, adjudication and administrative structures, such as the OAIC, can facilitate the concretisation of administrative law values.