Robodebt and Novel Data Technologies in the Public Sector: How Human Rights Laws Plug Data Protection Gaps

Serena Syme Hildenbrand*

The recent Royal Commission into Robodebt drew Australians' attention to the risks of data technologies in the public sector. Novel data technologies, including artificial intelligence, offer potential public benefits but create risks to individuals and society. I argue that existing Australian data protection laws offer inadequate protection against the dangers posed by the use of such technologies in the public sector. Pending more tailored legislative change, I consider the extent to which specific human rights laws such as those in Queensland, Victoria and the Australian Capital Territory, together with effective application of risk assessment methodologies within a human rights culture, could be layered over data protection laws to provide ongoing technologically-neutral protection against such harms.

I Introduction

In an effort to boost the efficiency of government services and law enforcement, Australian governments are trialling and implementing novel data technologies, such as automated decision-making, artificial intelligence ('AI') and biometric technologies. Such technologies carry the promise of immense efficiency gains, but their use of personal data may significantly limit human rights. This article argues that while data protection laws (often described as privacy laws in Australia) provide an important first layer of protection in relation to such novel data technologies, challenges in keeping them current with rapidly evolving technologies result in gaps in protection. In such a context, specific human rights laws, such as those in Queensland, Victoria and the Australian Capital Territory ('ACT'), offer the potential for a further layer of protection that is more durable and principles-based. If such human rights laws are bolstered by a human rights

* PhD candidate at Deakin University and Head of Data Sharing at the Department of Transport and Planning, Victoria, overseeing driver and vehicle data. The views expressed in this article are my own and not necessarily those of the Department. I wish to thank my supervisory team of Shiri Krebs, Matthew Groves and Bruce Chen for their ongoing support and valuable input and the Victorian Public Sector Commission for its assistance in providing data. I also appreciate the very helpful comments from my reviewers.

DOI: 10.38127/uqlj.v43i2.8311

culture within the public service, they could foster an appropriately robust, analytical, risk-based approach to the application of these technologies and the protection of human rights.

One notorious novel data technology was examined by the recent Royal Commission into Robodebt, investigating the federal government's use of a poorly-designed automated decision-making algorithm to identify and pursue potentially fraudulent welfare debts against hundreds-of-thousands of Australians from 2015–20.[1] Robodebt resulted in significant injustice and harm to members of the public and a financial settlement reaching into the billions of dollars.[2] Unsurprisingly, the Royal Commission concluded that Robodebt comprehensively 'failed the public interest'.[3]

Given resourcing constraints in the public sector,[4] together with the potential benefits of novel data technologies for government tasks,[5] such technologies are likely to become ubiquitous within the Australian public sector. I am not the first commentator to suggest that existing data protection laws at the state and federal levels in Australia are inadequate to address the risks posed by novel data technologies to individuals' rights.[6] In Europe, efforts have been made, including with the *General Data Protection Regulation* ('*GDPR*') and more recent laws,[7] to develop a more appropriate level of data protection to address such

---

1 *Royal Commission into the Robodebt Scheme* (Final Report, July 2023) ('*Robodebt Report*') v.

2 Luke Henriques-Gomes, 'Robodebt: five years of lies, mistakes and failures that caused a $1.8bn scandal', *The Guardian* (online, 11 March 2023) <https://www.theguardian.com/australia-news/2023/mar/11/robodebt-five-years-of-lies-mistakes-and-failures-that-caused-a-18bn-scandal>.

3 *Robodebt Report* (n 1) iii.

4 See, eg, Josh Gordon, 'Thousands of public sector jobs face axe as state orders 10% budget cuts', *The Age* (online, 29 March 2023) <https://www.theage.com.au/national/victoria/thousands-of-public-sector-jobs-face-axe-as-state-orders-10-percent-budget-cuts-20230329-p5cwbe.html>.

5 See, eg, Fang Chen and Jianlong Zhou, 'AI in the public interest' in Cliff Bertram, Asher Gibson and Adriana Nugent (eds), *Closer to the Machine: Technological, Social and Legal Aspects of AI* (Office of the Victorian Information Commissioner, 2019) 63, 65.

6 See, eg, Margaret Jackson, 'Regulating AI' in Cliff Bertram, Asher Gibson and Adriana Nugent (eds), *Closer to the Machine: Technological, Social and Legal Aspects of AI* (Office of the Victorian Information Commissioner, 2019) 121; Kate Galloway, 'Big Data, Government, Privacy and Human Rights'in Paula Gerber and Melissa Castan (eds), *Critical perspectives on human rights law in Australia* (Thomson Reuters Australia, 2022) vol 2, 357; Moira Paterson and Maeve McDonagh, 'Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data' (2018) 44(1) *Monash University Law Review* 1.

7 *Regulation (EU) 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 ('*GDPR*'). More recent European laws include *GDPR*-type legislation for the public sector and a *Data Governance Act*: *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018*, [2018] OJ L 295/39; *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724*, [2022] OJ L 152/1 ('*Data Governance Act*'). The EU also passed an '*AI Act*', to add additional protections around the use of artificial intelligence: *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence*, [2021] OJ L 170/1 ('*AI Act*').

technologies. Without assessing whether European laws achieve this promise, I identify how Australian data protection laws fall short of an equivalent level of protection and are likely to leave citizens vulnerable in the context of public sector use of novel data technologies.

Pending the update and improvement of data protection laws, another legal framework may provide meaningful protection within relevant public sectors. Queensland, Victoria and the ACT are in the relatively unusual position in Australia of having both data protection laws[8] and specific human rights laws[9] covering their public sectors.[10] Those human rights laws offer a further valuable layer of protection over rights which may be engaged by novel data technologies, including the rights to privacy, equality, family life, property and freedoms of association, speech and movement. The laws contain conduct and decision-making obligations for public servants, requiring them to act compatibly with human rights and, in making decisions, to give proper consideration to relevant rights. Human rights laws also intentionally promote human rights culture in the public service, which is a significant element of the potential protection they offer.[11] I describe how laws such as the *Human Rights Act 2019* (Qld) ('*Qld HRA*'), *Charter of Human Rights & Responsibilities Act 2006* (Vic) ('*Victorian Charter*') and the *Human Rights Act 2004* (ACT) ('*ACT HRA*') could address the dangers posed to rights by novel data technologies. Further, any federal bill or charter of rights is likely to offer similar protection — the Commonwealth Parliamentary Joint Committee on Human Rights has recently recommended the establishment of a federal Human Rights Act following its *Inquiry into Australia's Human Rights Framework*.[12]

---

8 *Information Privacy Act 2009* (Qld) ('*Qld IPA*'); *Privacy & Data Protection Act 2014* (Vic) ('*PDPA*'); *Information Privacy Act 2014* (ACT) ('*ACT IPA*'). Note that Queensland passed the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) in November 2023, which is likely to commence on 1 July 2025. Where relevant, this article will reference this incoming legislation.

9 *Human Rights Act 2019* (Qld) ('*Qld HRA*'); *Charter of Human Rights & Responsibilities Act 2006* (Vic) ('*Victorian Charter*'); *Human Rights Act 2004* (ACT) ('*ACT HRA*').

10 The Commonwealth technically has human rights legislation in the form of the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth) which establishes the Parliamentary Joint Committee on Human Rights ('PJCHR') (s 4) and confers on the PJCHR a scrutiny and oversight function for legislation and the ability to conduct inquiries on referral (s 7). However, I am not including the Commonwealth in the jurisdictions covered by specific human rights laws because the PJCHR's legislative oversight role and narrow scope is not equivalent to human rights legislation of the type implemented in Queensland, Victoria and the ACT, which is intended to impact the daily activities and culture of public servants. There is a comprehensive summary of the PJCHR's role and effectiveness here: Australian Human Rights Commission, *Free & Equal: A Human Rights Act for Australia* (Report, December 2022), 297–303. See also the following article which raises questions about the PJCHR's impact: Laura Grenfell and Julie Debeljak, *Law Making & Human Rights* (Thomson Reuters, 2019) 42–63.

11 See, eg, Queensland, *Parliamentary Debates*, 31 October 2018, 3184 (Yvette D'Ath, Attorney-General).

12 Parliamentary Joint Committee on Human Rights, 'Inquiry into Australia's Human Rights Framework' (Report, 2024) xxi–xxii <https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/RB000210/toc_pdf/InquiryintoAustralia'sHumanRightsFramework.pdf >.

Part II briefly defines and describes the types of novel data technologies relevant to this article. Part III outlines data protection laws in Queensland, Victoria and the ACT and their origins and approach. These three jurisdictions have been selected as case studies because their specific human rights legislation offers potential for such additional protection of data subjects from the impacts of novel data technologies. Comparison of these jurisdictions' data protection laws with more modern European Union data protection laws highlights their weaknesses relative to novel data technologies. Part IV describes the additional protection offered by specific human rights legislation in the relevant jurisdictions, first, by reference to the protective effect of a human rights culture within government and, second, through express conduct and decision-making obligations. It also provides practical ways to discharge those obligations using risk management methodologies within a human rights culture. Part V illustrates the difference that this may have made had a Robodebt-style program been implemented in one of these jurisdictions rather than federally, and Part VI concludes by recommending the implementation of a risk-based rights assessment within a human rights culture to avoid a repeat of a Robodebt scenario.

II Novel Data Technologies

To understand the impact of novel data technologies on public sector decision-making and functions, we start by looking more closely at the technologies.

Figure 1: Representation of Novel Data Technologies

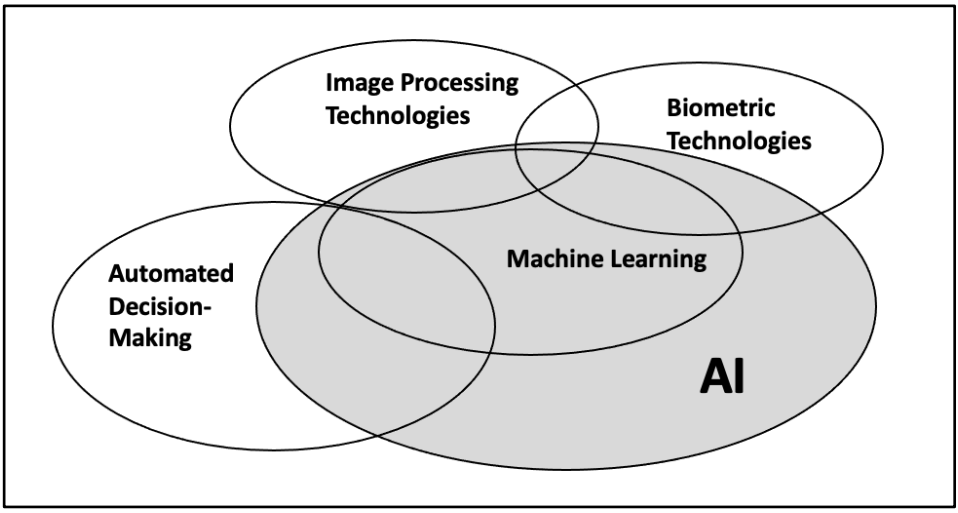


Figure 1 covers a range of data technologies, including non-novel technologies which can be combined with newer technologies such as AI to provide a wider field of operation. The most prominent category in Figure 1 is AI (shaded grey), which describes a collection of different technologies allowing computers to learn or solve problems, usually via a 'training' process involving the absorption and analysis of large quantities of data.[13] Machine learning ('ML') is a sub-set of AI, in which algorithms are trained on high volumes of data to make classifications or predictions and uncover key insights through a learning process.[14] Automated decision-making involves the application of computer-based algorithms to arrive at outcomes or recommendations — this can be powered by AI, but can also be a simpler algorithmic process (as seen in Robodebt). Biometric technologies refer to a mode of collecting biological markers (facial images, iris scans, speech patterns, gait characteristics, fingerprints) which may be digitised and analysed, by means of AI or otherwise. Image processing technologies include optical character recognition ('OCR') and processing of photos and closed-circuit television ('CCTV') images to extract information — they overlap with biometric technologies in areas such as facial recognition.

The use of all of these technologies within government offers efficiency advantages including by expanding the reach and application of limited government resources. For instance, in the context of a sharp increase in the Victorian road toll,[15] and evidence that driver distraction is a factor in at least 11 per cent of road fatalities, the Victorian government presented its AI-powered road camera enforcement solution as necessary to prevent an estimated 95 crashes resulting in death or injury each year.[16] In 2021, Queensland police conducted a trial of an algorithm using data from its Queensland Police Records Information Management Exchange ('QPRIME') police database and AI to identify likely perpetrators of domestic violence and enable police to conduct pre-emptive home visits to those individuals ('QPRIME algorithm').[17] Results of the

---

13 Toby Walsh, 'Understanding AI' in Cliff Bertram, Asher Gibson and Adriana Nugent (eds), *Closer to the Machine: Technological, Social and Legal Aspects of AI* (Office of the Victorian Information Commissioner, 2019) 7, 7–11.

14 Cliff Bertram, Asher Gibson and Adriana Nugent, 'Key Terms' in Cliff Bertram, Asher Gibson and Adriana Nugent (eds), *Closer to the Machine: Technological, Social and Legal Aspects of AI* (Office of the Victorian Information Commissioner, 2019) 3.

15 ABC Radio Melbourne, 'Road Safety Expert Calls for Change in Individual Behaviour After 'Disheartening' Jump in National Road Toll' (online, 15 May 2023) <https://www.abc.net.au/melbourne/programs/mornings/national-road-toll-spike/102345990>.

16 Daniel Andrews, 'New Driver Distraction Road Rules To Save Lives' (Media Release, 14 February 2023) <https://www.premier.vic.gov.au/new-driver-distraction-road-rules-save-lives>.

17 Ben Smee, 'Queensland Police to Trial AI Tool Designed to Predict and Prevent Domestic Violence Incidents', *The Guardian* (online, 14 September 2021) <https://www.theguardian.com/australia-news/2021/sep/14/queensland-police-to-trial-ai-tool-designed-to-predict-and-prevent-domestic-violence-incidents>.

trial pointed to a significant reduction in incidents in a cohort of high-risk offenders.[18]

These developments are not without critique, with detractors identifying the possibility of significant limitations of the human rights of data subjects and other potential harms.[19] AI and algorithmic systems are notorious for ingesting bias from the data on which they train, resulting in outcomes which may be unfair and discriminatory.[20] This may have been the case with the Suspect Target Management Program ('STMP') operated by New South Wales police, which generated predictive profiles of likely crime suspects.[21] An investigation found that 44 per cent of the individuals targeted by the system were Indigenous, a highly disproportionate outcome considering the Indigenous population comprised less than 4 per cent of the state's residents.[22] Of course, it can be difficult to prove that an algorithm is unbiased — such an assessment will generally require a detailed technical knowledge of the algorithm and the training datasets used.[23]

---

18 Teagan Westendorf, 'AI and Policing: What a Queensland Case Study Tells Us', *The Strategist* (online, 13 May 2022) <https://www.aspistrategist.org.au/ai-and-policing-what-a-queensland-case-study-tells-us/>.

19 See, eg, Paterson and McDonagh (n 6) 6–7; Galloway (n 6) 365–76. I use the term 'data subjects' to refer to individuals whose data is being shared and used, following the terminology used in the *GDPR*.

20 Katie Miller, 'Discrimination, Bias and Inequality in AI' in Cliff Bertram, Asher Gibson and Adriana Nugent (eds), *Closer to the Machine: Technological, Social and Legal Aspects of AI* (Office of the Victorian Information Commissioner, 2019) 23; New South Wales Ombudsman, *The New Machinery of Government: Using Machine Technology in Administrative Decision-Making* (Report, 29 November 2021) 35–6. The New South Wales Ombudsman report notes that algorithmic bias can comprise human biases preserved in the data (such as racism and sexism) as well as technical biases due to incomplete or distorted data: 35.

21 Michael McGowan, 'NSW Police Accused of "Oppressive" Tactics Against Subjects on Secretive Blacklist', *The Guardian* (online, 4 July 2022) <https://www.theguardian.com/australia-news/2022/jul/04/nsw-police-accused-of-oppressive-tactics-against-subjects-on-secretive-blacklist>. See also, the description of this program in Galloway (n 6) 370–1.

22 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: Technological, Social and Legal Aspects of AI* (Office of the Victorian Information Commissioner, 2019) 41, 45. For figures related to the Indigenous population of New South Wales, see: 'Census of Population and Housing - Counts of Aboriginal and Torres Strait Islander Australians', *Australian Bureau of Statistics* (Web Page, 31 August 2022) <https://www.abs.gov.au/statistics/people/aboriginal-and-torres-strait-islander-peoples/census-population-and-housing-counts-aboriginal-and-torres-strait-islander-australians/2021>. Indigenous people are already over-represented in the Australian criminal justice system: Australian Law Reform Commission, *Pathways to Justice–Inquiry into the Incarceration Rate of Aboriginal and Torres Strait Islander Peoples* (Report No 133, March 2018). So this outcome may be a perpetuation of that existing inequity preserved in the data, or it may represent new technical biases — in either case, it raises concern and warrants further investigation.

23 See, eg, *R (Bridges) v Chief Constable of South Wales Police* [2020] 1 WLR 5037, 5078–80 [193]–[201]. In that case, it was apparent that the South Wales Police had no such detailed knowledge of the facial recognition system they were employing — so while there was no evidence that the algorithm was biased, bias also could not be ruled out: 5079–80 [199]–[201].

While not all aspects of the use of novel data technologies in the public sector are regulated, they do not operate in a legal vacuum. The following section explores existing regulation governing the use of such technologies.

III Data Protection Law

Data protection law seeks to protect individuals from harms caused by information processing and accordingly can be regarded as the first line of defence against the risks of novel data technologies.[24] Data protection shares some common ground with the broader concept of privacy.[25] However, it should be understood to extend beyond a limited association with privacy rights and seen to cover prevention of a wide range of harms that might result from the processing of personal data. Viewed in such a way, data protection laws are potentially of great relevance to burgeoning novel data technologies and their impact on human rights.

Data protection has a multi-decade history in Europe where it is an established field of law and policy, but is less central to Australian legal practice.[26] Bygrave describes how data protection theories arose from significant developments in the field of personal information processing, which triggered fears not adequately addressed by other laws.[27] In some countries, data protection emerged from legal foundations quite distinct from privacy, such as information self-determination (Germany),[28] protection of liberty (France),[29] and fair information practices (the United States),[30] and had little in common with privacy

---

24 '[T]he term "data protection" is used ... to denote a set of measures (legal or non-legal) which are aimed at safeguarding persons from detriment resulting from the processing of information on them': Lee A Bygrave, 'An international data protection stocktake @2000 Part 1: regulatory trends' (2000) 6(8) *Privacy Law and Policy Reporter* 129, 129.

25 Lee A Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014) 3. While data protection can arguably protect rights in addition to privacy, privacy rights can be considered to extend further than the information privacy coverage offered by data protection laws because they include bodily, spatial, communicational, proprietary, intellectual, information, decisional, associational and behavioural privacies: see Bert-Jaap Koops et al, 'A Typology of Privacy' (2017) 38(2) *University of Pennsylvania Journal of International Law* 483.

26 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, 133, 155–7.

27 Bygrave (n 25) 8.

28 The German term *informationelle selbstbestimmung* was first used in relation to a prominent German court decision on the 1983 census, where the court recognised informational self-determination as a constitutional right: see Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25(1) *Computer Law & Security Report* 84.

29 The first French data protection law in 1978, dubbed *Informatique et Libertés*, and the relevant French regulator (the *Commission Nationale de l'Informatique et des Libertés* with its mission statement: 'to protect personal data, support innovation, preserve individual liberties') highlight the focus on liberty.

30 Bygrave (n 25) 27, 33, 115–16.

law.[31] Data protection law is also concerned with elements of data quality — the 'validity, integrity, availability, relevance, and completeness of data', which are not directly derived from privacy concerns.[32]

Data protection laws are intended 'to protect individuals from the processing of data by means of individual rights and structural guarantees'.[33] In an 'early specifically European interpretation of data protection in relation to privacy',[34] De Hert and Gutwirth contrast the 'transparent', procedural role of data protection with the more 'opaque' protection offered by privacy laws (such as secrecy provisions or restrictions on surveillance), noting that data protection laws are based on an understanding that personal information can be legitimately processed and shared, provided that certain transparency requirements and protections are applied.[35] De Hert and Gutwirth consider that the purpose of such laws is not to *prohibit* but to *allow* access, with commensurate protection.[36] Kohl notes that 'data protection law is based on the assumption that there has been a disclosure of personal information and gives individuals a degree of control to oversee and manage that disclosure'.[37] Bygrave concurs, commenting: 'data privacy legislation tends to operate with largely procedural rules that avoid fundamentally challenging the bulk of established patterns of information use. In the language of road signs, it usually posts the warning "Proceed with Care!"; it rarely orders "Stop!"'.[38] Similarly, Hustinx views data protection as a series of checks and balances rather than a prohibition, stating that data protection law 'was not designed to prevent the processing of such information or to limit the use of information technology per se… it was designed to provide safeguards'.[39] Accordingly, data protection can be viewed as a type of bargain with the public: some data will inevitably be shared, so in return protections must be applied.

The first truly international instrument addressing data protection was the non-binding 1980 *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Data* ('*OECD Guidelines*'), drafted by an expert group led by

---

31 Ibid 26–8.

32 Ibid 120.

33 Felix Bieker, *The Right to Data Protection: Individual and Structural Dimensions of Data Protection in EU Law* (Springer, 2022) 180.

34 Ibid 145.

35 Paul De Hert and Serge Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E Claes, A Duff and S Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia, 2006) 61, 77. See also support for this approach in Serge Gutwirth, Ronald Leenes and Paul de Hert, *Reforming European Data Protection Law* (Springer, 2015) 16.

36 De Hert and Gutwirth (n 35) 77.

37 Uta Kohl, 'The Right to be Forgotten in Data Protection Law and Two Western Cultures of Privacy' (2023) 72 *International Comparative Law Quarterly* 737, 748.

38 Bygrave (n 25) 122. This parallels the 'red light/green light' metaphor for administrative law popularised by Harlow and Rawlings: see, eg, Carol Harlow and Richard Rawlings, *Law and Administration* (Cambridge University Press, 4th ed, 2022) 7.

39 Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation' in Marise Cremona (ed), *New Technologies and EU Law* (Oxford University Press, 2017), 123.

Justice Michael Kirby.[40] Justice Kirby describes how even in the 1970s it was increasingly apparent that transnational technologies could not effectively be managed by national laws; it was 'the fear of new "barriers" that afforded the initial focus of the work of the expert group and of the interest of the OECD', that is, fear that national laws might impede the free flow of data and its consequent economic benefits.[41]

Data protection is most often a creature of statute or negotiated frameworks such as the *OECD Guidelines*.[42] It is defined and understood as compliance with certain 'data protection principles', which generally comprise an accepted set of minimum principles, plus newer principles introduced over time through international acceptance.[43] The key principles are that personal data must be processed fairly and lawfully, for specified purposes only.[44] The *OECD Guidelines* contained eight such principles which have been adopted throughout the world. Greenleaf regards the *OECD Guidelines* principles as offering 'the best guide to the *minimum* requirements of a data privacy law'.[45]

The *OECD Guidelines* were implemented in Australia by statute.[46] They were first reflected in the *Privacy Act 1988* (Cth) ('*Privacy Act*')[47] and then in corresponding legislation in most of the states.[48] Enforcement is primarily allocated to privacy or information commissioners in each jurisdiction, who tend to experience resourcing challenges in the face of a significant workload.[49] The Queensland and Victorian statutes contain Information Privacy Principles ('IPPs') based on the eight principles of the *OECD Guidelines*, while the ACT uses Territory Privacy Principles ('TPPs') instead (see Table 1).[50] Table 1 also includes the relevant Australian Privacy Principles ('APPs') under the *Privacy Act*; and there

---

40 Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980.

41 Michael Kirby, 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy' (2009) 20(2) *Journal of Law, Information and Science* 1, 4–5.

42 Bygrave (n 25) 3–4.

43 G W Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press, 2014) 5.

44 Bygrave (n 25) 147, 153.

45 Graham Greenleaf, 'Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories' (2014) 23(1) *Journal of Law, Information and Science* 4, 11 (emphasis in original).

46 Graham Greenleaf, 'Privacy in Australia' in James Rule and Graham Greenleaf (eds), *Global Privacy Protection: The First Generation* (Edward Elgar Publishing, 2008) 141, 151–2.

47 *Privacy Act 1988* (Cth) ('*Privacy Act*').

48 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) 161–88.

49 See, eg, the report into the effectiveness of the Queensland Office of the Information Commissioner, which broadly identified a good service limited by resourcing constraints: Department of Justice and Attorney-General, *Strategic Review of the Office of the Information Commissioner (Queensland)* (Report, 26 April 2017). Regarding resourcing challenges faced by the Office of the Australian Information Commissioner: see Anna Macdonald, 'Privacy commissioner role separated once more, needs "double funding" to do job well', *The Mandarin* (online, 23 May 2023) <https://www.themandarin.com.au/219131-information-privacy-commissioner-role-separated-once-more/>.

50 *Qld IPA* (n 8); *ACT IPA* (n 8).

is a close relationship between the APPs and TPPs, as reflected in Table 1 below.[51] It also includes the new Queensland Privacy Principles ('QPPs'), scheduled to replace the Queensland IPPs in 2025 and also modelled on the APPs.[52] Given the direct line from the *OECD Guidelines* to these Australian laws, it is reasonable to characterise them all as data protection laws, rather than privacy laws per se. All three jurisdictions have separate privacy principles covering personal information collected for health purposes,[53] but as these are similar to the more general privacy principles, and as health information is potentially less likely to be processed by novel data technologies due to its sensitivity, they will not be specifically considered.

Table 1: Implementation of OECD Guidelines in the Privacy Act and Jurisdictional Laws in Queensland, Victoria and ACT

OECD Guidelines Principle	Requirement	Qld IPP	Vic IPP	ACT TPP, Cth APP and QPP (not yet in force)
Collection Limitation	Applies limits to personal data collection, minimisation and lawful and fair collection; where appropriate with knowledge and consent.[54]	1	1	3–4
Data Quality	Data is to be relevant, complete, accurate and up to date.[55]	3, 7–9	3, 6	10
Purpose Specification	Requires notification of purposes of collection at the time and subsequent use limited to those purposes or other compatible purposes specified on each occasion where the purpose changes.[56]	2, 9–11	1–2	5–6

51 The Territory Privacy Principles ('TPPs') and Australian Privacy Principles ('APPs') are intentionally very similar but not identical. Some of the APPs have been omitted from the TPPs for irrelevance and are there are some minor drafting differences, but numbering consistency has been preserved: see Office of the Australian Information Commissioner, 'Territory Privacy Principles', (Web Page) <https://www.oaic.gov.au/privacy/privacy-legislation/state-and-territory-privacy-legislation/territory-privacy-principles>.

52 The new *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces the Qld Information Privacy Principles ('IPPs') with Queensland Privacy Principles ('QPPs'), which align more closely with the APPs and are likely to come into effect on 1 July 2025.

53 *Qld IPA* (n 8) ss 30–1, sch 4; *Health Records Act 2001* (Vic) ss 19–21, sch 1; *Health Records (Privacy and Access) Act 1997* (ACT) ss 5–6, sch 1.

54 Organisation for Economic Co-operation and Development (n 40) [7].

55 Ibid [8].

56 Ibid [9].

Use Limitation[57]	Use is to be limited to the specified purpose, except with consent or where required by law.[58]	10–11	2	6
Security Safeguards	Requires data to be protected against loss, destruction or unauthorised use or disclosure by 'reasonable security safeguards'.[59]	4	4	11
Openness	Imposes openness around data practices including means to establish the existence of the data, purpose of use and identity of user.[60]	5	5	1
Individual Participation	Requires individuals to receive confirmation if data is held on them and for it to be provided to them and corrected on request, with appeal rights for refusals.[61]	5–7	6	12–13
Accountability[62]	Data controller is to be accountable for compliance with the principles.[63]	Through out	Through out	1.2

European law has now outstripped the approach set out in the *OECD Guidelines*, with the introduction of data protection laws including the *GDPR* and the *Data Governance Act*. Paterson and McDonagh undertake a useful exercise of contrasting the protection of the *Privacy Act* and the protection offered by the *GDPR* in relation to big data analytics, concluding that the *GDPR* offers additional protection in a number of areas including: clearer application of protection around online identifiers; higher bars for collection, use and disclosure; requirements for privacy by design and default; obligations to conduct data protection impact assessments; restrictions on profiling; and a right to erasure.[64] Table A1 in the Appendix compares the *GDPR* principles with the data protection principles in the relevant Australian jurisdictions, demonstrating how current

57 Note that each of the jurisdictional laws specifies allowed uses which extend beyond those permitted by the *OECD Guidelines*, namely (a) with the consent of the data subject, or (b) by the authority of law: ibid [10].

58 Ibid.

59 Ibid [11].

60 Ibid [12].

61 Ibid [13].

62 The Accountability Principle is that '[a] data controller should be accountable for complying with measures which give effect to the principles stated above': ibid [14]. This is not expressly stated in the IPPs or TPPs, but is arguably covered by the requirement that public sector agencies in those jurisdictions must comply with them, and by enforcement measures that can be taken by regulators.

63 Ibid.

64 Paterson and McDonagh (n 6) 15–25.

Australian protection omits several *GDPR* protections with specific relevance to novel data technologies. These omissions include: rights to restrict and object to data processing; protections around automated decision-making and de-identified information; and requirements for data protection by design and default and mandatory impact assessments. Several high-profile reports have identified further deficiencies in the *Privacy Act* in the context of twenty-first century data practices.[65]

A review of the *Privacy Act* commenced in 2019 and the resulting 2022 *Privacy Act Review Report* contains 116 proposals broadly weighted towards the European approach, with a number of them emulating the *GDPR*.[66] The federal government has formally agreed to implement 38 of the proposals, with 'in principle' support for a further 68 proposals, and draft legislation to be released in 2024.[67] Once reflected in legislation, those proposals may be replicated at the state level, but there is likely to be a significant delay.[68] For instance, Queensland has recently passed new privacy legislation with the key provisions expected to take effect in 2025, so is unlikely to adopt additional changes mirroring amendments to the federal *Privacy Act* in the near future.[69]

Commentary on the proposed changes suggests that, while they may not address every deficit of the *Privacy Act*, they would be landmark reforms likely to increase protection and enforcement in certain key areas.[70] The proposals helpfully introduce an overarching 'fair and reasonable' test which may promote better conduct by entities handling personal data.[71] In addition, the proposals are likely to provide a higher level of protection in relation to data processing

---

65 See, eg, Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report No 123, June 2014) 51–3 [3.50]; Australian Human Rights Commission, *Human Rights and Technology* (Final Report, 2021) 121–3; Australian Competition & Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019) 23–5.

66 Attorney-General's Department, *Privacy Act Review Report* (Report, 2022).

67 Attorney-General's Department, 'Fact Sheet: Government Response to the Privacy Act Review Report' (2023) 2. Note that 'in principle' agreement means that further consultation and an impact analysis will be undertaken before a final decision on implementation: 2.

68 Maria O'Sullivan, 'The Privacy Act Review Report 2022 — A Radical Review or Just a Re-imagining?' (2023) 51 *Australian Business Law Review* 52, 52.

69 *Information Privacy and Other Legislation Amendment Act 2023* (Qld). The Queensland review of privacy legislation arose from the 2017 statutory review of the relevant legislation, plus the 2020 findings of the Crime and Corruption Commission (Queensland) in Operation Impala, which investigated the misuse of confidential information in the Queensland Public Sector: Department of Justice and Attorney-General, 'Consultation Paper — Proposed changes to Queensland's Information Privacy and Right to Information Framework' (Report, June 2022) 3–4.

70 O'Sullivan (n 68) 55.

71 Attorney-General's Department, *Privacy Act Review Report* (n 66) 8–9. Agreed in principle: Attorney-General's Department, *Government Response — Privacy Act Review Report* (Report, 2023) 8.

activities,[72] automated decision-making activities,[73] high risk data activities,[74] and the use of de-identified data.[75]

The Appendix (Table A1) includes reference to these proposals, which are considered necessary to bring the *Privacy Act* up to an acceptable level of protection — and which, accordingly, highlight existing deficits. It illustrates that the recommendations do not cover all relevant *GDPR* protections, excluding as they do any right to restrict processing or any requirement to implement data protection by design and default. Further, even though the *GDPR* is broadly regarded as offering a high level of protection, it contains some recognised weaknesses (also reflected in the Australian laws) which are not addressed by the *Privacy Act Review Report* and continue to represent gaps in protection. For instance, the *GDPR* continues to rely on a notice and consent model, despite much evidence that the concept is heavily fraying and offers inadequate protection to individuals.[76] This weakness is somewhat offset by art 5 of the *GDPR,* which includes a fairness requirement and, as noted above, the *Privacy Act Review Report* recommends an objective 'fair and reasonable' test for handling personal data. Thus, both the *GDPR* and *Privacy Act Review Report* recommendations would reduce but not remove reliance on individual notice and consent.

The *GDPR* also restricts legal protection to personal data, defined as 'any information relating to an identified or identifiable natural person ("data subject") … who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data' or other factors.[77] Novel data technologies not only allow re-identification of anonymised data through data matching, but can apply 'individuation' to data which is technically non-identifiable (and therefore unprotected) and extract insights about individuals or groups without re-identifying the data.[78]

---

72 Attorney-General's Department, *Privacy Act Review Report* (n 66) 11. Agreed in principle: Attorney-General's Department, *Government Response — Privacy Act Review Report* (n 71) 30.

73 Attorney-General's Department, *Privacy Act Review Report* (n 66) 12. Agreed in principle: Attorney-General's Department, *Government Response — Privacy Act Review Report* (n 71) 32.

74 Attorney-General's Department, *Privacy Act Review Report* (n 66) 9. Agreed in principle: Attorney-General's Department, *Government Response — Privacy Act Review Report* (n 71) 28.

75 Attorney-General's Department, *Privacy Act Review Report* (n 66) 5. In its response, the government agreed in principle to amend and expand the definition of de-identified information, agreed to consult on introducing an offence for malicious re-identification, but only 'noted' the other recommendations: see Attorney-General's Department, *Government Response — Privacy Act Review Report* (n71) 21–2.

76 Peter Leonard, 'Data privacy in a data and algorithm enabled world' (2021) 93 *Computers & Law* 22. The 'notice and consent' model is the familiar process by which customers are given privacy notices and asked to provide their consent to use of their personal data. This model has been critiqued because it places the burden on individuals to manage their own privacy and the consent they provide is often not meaningful: see, eg, Daniel Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 (7) *Harvard Law Review* 180.

77 *GDPR* (n 7) art 4 cl 1.

78 Anna Johnston, 'Reforming privacy laws to protect against digital harms' (2021) 93 *Computers & Law* 38.

Further, the *GDPR* limits data use to a clearly defined purpose known in advance.[79] Some novel data technologies, especially AI technologies, do not operate in this way. Once the data is ingested into such an application, it may be impossible to restrict its use to a defined purpose.[80]

Accepting that current Australian data protection legislation contain gaps in effective protection, specific human rights legislation fulfils a valuable role. Data protection law targets the mechanics of information processing and accordingly is challenged by the pace of technological development. By focusing instead on the rights to be protected, human rights legislation can operate at a principles-level above current technologies, offering a truly technology-neutral approach.[81] Such protection is highly desirable given the speed of change in novel data technologies and the difficulties legislators face in keeping pace.[82] This supports the use of specific human rights legislation in Queensland, Victoria and the ACT to provide this layer of protection relative to novel data technologies and also the introduction of such legislation at the federal level and in other state jurisdictions to help future-proof protection in those jurisdictions.[83] Even if Australia's data protection laws are ultimately reformed to address existing deficits, separate technology-neutral human rights overlays will continue to be valuable, offering durable protection which spans technological developments. The next section outlines the potential contribution of human rights laws as demonstrated in Queensland, Victoria and the ACT in relation to novel data technologies in the public sector.

IV Human Rights Legislation

Queensland, Victoria and the ACT each have a specific human rights statute, setting out a range of human rights that the public sector is bound to protect and promote.[84] In this Part, I describe how the application of specific public sector obligations under those human rights laws, together with the fostering of a human rights culture in the public sector, could provide additional protection to data subjects relative to novel data technologies. There is a strong case for the introduction of a similar law at the federal level, as cogently argued in the Australian Human Rights Commission's 2022 position paper *Free & Equal: A*

---

79 See, eg, *Privacy Act* (n 47); *GDPR* (n 7) art 5 cl 1(b).

80 Alessandro Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (Springer, 2022) 9–11.

81 Galloway (n 6) 378.

82 Australian Competition & Consumer Commission (n 65) 3: 'The ACCC is concerned that the existing regulatory frameworks for the collection and use of data have not held up well to the challenges of digitalisation. The pace of technological change needs to be matched by the pace of policy review'.

83 Galloway argues that the need for technology-neutral protections for big data technologies requires the implementation of a federal bill of rights: Galloway (n 6) 378.

84 *Qld HRA* (n 9); *Victorian Charter* (n 9); *ACT HRA* (n 9).

Human Rights Act for Australia,[85] and as recently recommended by the Parliamentary Joint Committee on Human Rights.[86] Should such a law be introduced, it is likely to extend the protections to the Commonwealth public sector also.

The *Qld HRA*, *Victorian Charter* and *ACT HRA* share similar origins, given their common inspiration from the *Human Rights Act 1998* (UK) and the *New Zealand Bill of Rights Act 1990* (NZ), both of which are dialogue-based parliamentary models of human rights protection.[87] Each of the Australian statutes contains conduct and decision-making obligations applicable to public servants and public sector agencies, requiring them to act compatibly with human rights and to give proper consideration to human rights.[88] Each also contains a range of rights which may be relevant to the impact of novel data technologies, including but not limited to privacy rights.[89] But in some ways their most important contribution is in seeking to build a human rights culture within the public sector of each jurisdiction, which is particularly pertinent to the complex challenges raised by the use of novel data technologies. In a fast-changing environment where legislation struggles to keep pace, a widespread awareness of human rights in the public sector and inclusion of human rights in decision-making will help ensure that the capabilities of technology do not outstrip the needs of citizens.

A *Importance of a Human Rights Culture*

On presentation of the Queensland Human Rights Bill to Parliament, Attorney-General Yvette D'Ath noted that '[t]he primary aim of the bill is to ensure that respect for human rights is embedded in the culture of the Queensland public sector'.[90] Victorian Attorney-General Rob Hulls made similar comments in introducing the *Victorian Charter* bill, adding that '[t]he experience in other jurisdictions that have used this model is that it is in the area of administrative compliance that the real success story of human rights lies'.[91] That is, such

---

85 Australian Human Rights Commission, *Free & Equal: A Human Rights Act for Australia* (n 10).

86 Parliamentary Joint Committee on Human Rights (n 12).

87 Victoria, *Parliamentary Debates*, Legislative Assembly, 4 May 2006, 1290 (Rob Hulls, Attorney-General) 1290. See discussion of the 'dialogue model' in the context of the *Qld HRA*: Bruce Chen, 'The "Human Rights Act 2019 (Qld)": Some perspectives from Victoria' (2020) 45(1) *Alternative Law Journal* 4, 4. Note that the UK legislation implements the European *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) ('*ECHR*') and accordingly operates in a different context than the New Zealand and Australian legislation, which is based on the *International Covenant on Civil and Political Rights* opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) ('*ICCPR*').

88 *Qld HRA* (n 9) s 58(1); *Victorian Charter* (n 9) s 38(1); *ACT HRA* (n 9) s 40B(1).

89 *Qld HRA* (n 9) s 25; *Victorian Charter* (n 9) s 13; *ACT HRA* (n 9) s 12.

90 Queensland, *Parliamentary Debates*, 31 October 2018, 3184 (Yvette D'Ath, Attorney-General).

91 Victoria, *Parliamentary Debates*, 4 May 2006, 1293, 1295 (Rob Hulls, Attorney-General).

legislation is arguably strongest in creating a culture of compliance so that human rights are not unjustifiably limited in the first place, rather than in boosting legal remedies following a breach. The development of a public sector human rights culture was also a key goal for the *Human Rights Act 1998* (UK),[92] and the *ACT HRA*.[93]

What is a human rights culture? A frequently used definition of organisational culture is formulated by Edgar Schein as 'a pattern of shared basic assumptions that was learned by a group as it solved its problems', that is then shared with new members.[94] Naylor et al note that it is more difficult to find consensus over the definition of human rights culture, but they propose the following adaptation of Schein's definition: 'shared assumptions and patterns of behaviour that are respectful of the human rights of people both within and outside the organisation, and that comply with the organisation's negative and positive obligations to promote human rights'.[95] Similarly, the Victorian Equal Opportunity and Human Rights Commission ('VEOHRC') defines a positive human rights culture as 'a pattern of shared attitudes, values and behaviours that influence the policy making, decisions and practices of government to uphold the human rights of all people'.[96]

How does such a culture evolve in practice? At the one year review of the *ACT HRA*, progress towards such a culture was found to be slow,[97] while the five year review identified 'a fledgling human rights culture in the ACT'.[98] After ten years of the *ACT HRA*, it was reported that cultural change had been patchy and measurement limited.[99] The outgoing ACT Human Rights Commissioner describes the ACT's 'increased human rights culture', which she considered to be strengthened by the *ACT HRA*, but she also raises the need for more resources for public service training.[100]

The mandated eight year review of the *Victorian Charter*, the 2015 *Victorian Charter Review* ('Eight Year Review'), included a strong focus on building a human rights culture in Victoria, noting that such a culture is not an end in itself but 'a

---

92 United Kingdom, *Parliamentary Debates*, House of Commons, 21 October 1998, vol 981021, col 1320 (Mike O'Brien, Parliamentary Under-Secretary of State for the Home Department).

93 ACT, *Parliamentary Debates*, 23 October 2003, 4032 (Jon Stanhope, Chief Minister and Attorney-General).

94 Edgar H Schein, *Organizational Culture and Leadership* (Jossey-Bass, 4th ed, 2010) 17.

95 Bronwyn Naylor, Julie Debeljak and Anita Mackay, 'A Strategic Framework for Implementing Human Rights in Closed Environments' (2015) 41(1) *Monash University Law Review* 218, 261.

96 Victorian Equal Opportunity and Human Rights Commission, *2018 Report on the Operation of the Charter of Human Rights and Responsibilities* (Report, November 2019) 14.

97 ACT Department of Justice and Community Safety, *Human Rights Act 2004: Twelve-Month Review* (Report, June 2006), 34–6.

98 The ACT Human Rights Act Research Project, *The Human Rights Act 2004 (ACT): The First Five Years of Operation* (Report, 2009) 7.

99 ACT Human Rights Commission, *Look Who's Talking: 10 years of the Human Rights Act* (Report, 2014) 15–16.

100 Helen Watchirs, 'Reflections on the ACT's Human Rights Bill 20 Years On — Lessons for the National Inquiry' (2023) 268 *Ethos: Law Society of the ACT Journal* 26, 28, 36.

means to better government decision making'.[101] The Eight Year Review identified some strong progress in cultural change,[102] but also a deprioritisation of the *Victorian Charter* in recent years, which had restrained progress.[103] This serves as a reminder that the process of building culture needs to be consistent and ongoing. It is noteworthy that the VEOHRC submission to that review identifed a positive cultural shift but also considerable fragility in that change.[104] A 2018 report prepared by VEOHRC included a survey of 35 public authorities, finding a strong commitment to a human rights culture but also key areas for improvement, noting that progress was demonstrably weaker in municipal councils and large government agencies than in government departments and small government agencies.[105]

The Victorian government measures the impact of the *Victorian Charter* on public sector culture by including human rights questions in its annual survey of public sector staff. One such question has been consistent across the period 2008–23, namely, 'I understand how the Charter of Human Rights and Responsibilities applies to my work'. In analysing responses to this survey to assess the growth of a human rights culture, VEOHRC commented in 2018 that 'the Commission expects to see a steady decline in the number of employees in the 'neither agree nor disagree' categories of the Victoria Public Sector Commission survey, and an increase in the number of affirmative responses'.[106] Figure 2 shows data and trend lines for the 'neither agree or disagree' category (formerly 'don't know') and total affirmative responses ('strongly agree' plus 'agree') across the 15 year period for the question stated above.[107]

---

101 Michael Brett Young, Victorian Equal Oppurtunity & Human Rights Commission, *From Commitment to Culture: The 2015 Review of the Charter of Human Rights and Responsibilities Act 2006* (Report, 2015) 20.

102 Ibid 32–3.

103 Ibid 23, 39.

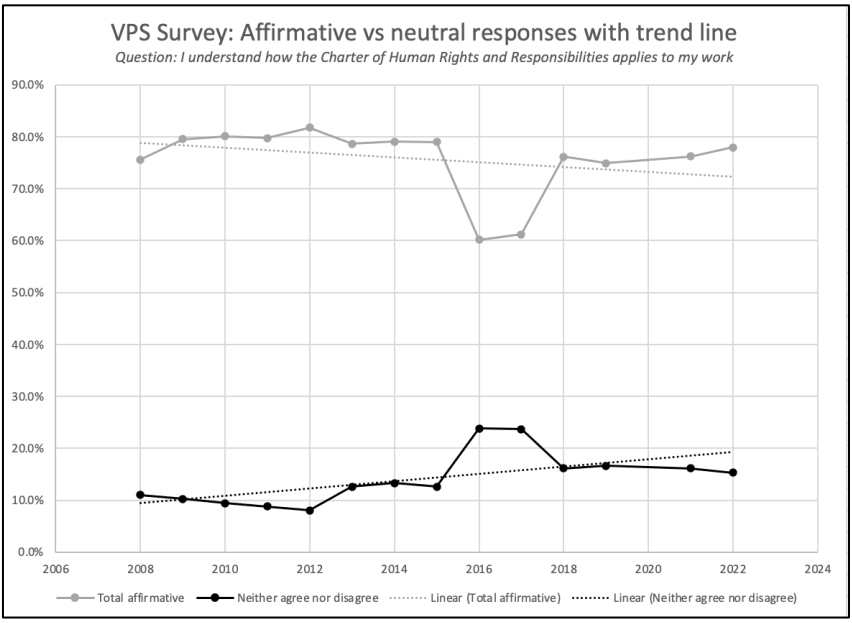
104 Victorian Equal Opportunity & Human Rights Commission, *Submission to the Eight-Year Review of the Charter of Human Rights and Responsibilities Act 2006* (Report, 2015). 'We have also seen, however, that when support for the Charter is waning, or where there was a possibility it might be repealed, that enthusiasm for meeting Charter obligations waned correspondingly': 13.

105 Victorian Equal Opportunity & Human Rights Commission, *2018 Report on the Operation of the Charter of Human Rights and Responsibilities* (n 96) 17. There was a particularly large divide in whether leadership was engaged in human rights, with high scores for engaged leadership in government departments (83 per cent) and small agencies (79 per cent), but much lower for municipal councils (48 per cent) and large agencies (37 per cent): 22.

106 Victorian Equal Opportunity and Human Rights Commission, *2017 report on the operation of the Charter of Human Rights and Responsibilities* (Report, August 2018) 49.

107 The questions are asked using a five-point Likert scale for responses. From 2008–15, the responses were 'Strongly agree — Agree — Don't know — Disagree — Strongly disagree'. From 2016 to present, the responses were 'Strongly agree — Agree — Neither agree nor disagree — Disagree — Strongly disagree'. While this change in naming the third point may have contributed to the 2016 effects seen in Figure 2, it is unlikely alone to have caused the sharp change in the 'Strongly agree — Agree' combined affirmative response.

Figure 2: Victorian Public Sector Survey Responses 2008–22[108]



First, it is worth noting the high proportion of respondents answering the question affirmatively.[109] These relatively high ratings are broadly in line with survey responses regarding other public sector values, such as integrity and accountability.[110] Second, there appears to be an abrupt change in the data in 2016, which is maintained in 2017 before correcting in 2018. It is notable that following the Eight Year Review, the Victorian government reaffirmed in 2017 its commitment to the *Victorian Charter* and provided new funding for a Charter Education Program to develop and provide targeted Charter education programs to public servants.[111] It is likely that this investment caused a meaningful

---

108 The Victorian Public Sector Commission kindly supplied the author with all human rights questions and responses used in the surveys in the period 2008–22, and percentage responses to those questions ('VPSC Raw Data 2008–22'). See Table A2 in the Appendix for the relevant data. Note that no survey was conducted in 2020 due to the Covid-19 pandemic.

109 Victoria Public Sector Commission, 'Past Releases', *Victorian Public Sector Commission* (Web Page, 10 May 2021) <https://vpsc.vic.gov.au/data-and-research/past-releases/>. Additional and more complete data for the period 2008–23 was included in the VPSC Raw Data 2008–22.

110 Victoria Public Sector Commission, 'Public Sector Values', *Victorian Public Sector Commission* (Web Page, 24 April 2023) <https://vpsc.vic.gov.au/data-and-research/people-matter-survey-data/public-sector-values/>.

111 Victorian Equal Opportunity and Human Rights Commission, *2017 Report on the Operation of the Charter of Human Rights and Responsibilities* (n 106) 45. The education program was still operating

improvement in the development of a human rights culture in Victoria.[112] Third, the 15-year trend lines do not yet demonstrate the clear progress that VEOHRC was seeking, showing both a gradual decline in affirmative responses, and a gradual increase in neutral responses. The 2021–2 results look encouraging and a continued trajectory might demonstrate the overall growth VEOHRC is seeking, but these findings suggest that there is still work to be done to solidly embed a human rights culture in the Victorian public sector. This data appears to support the positive findings on human rights culture in the Eight Year Review and VEOHRC analysis, but also suggests that progress is fragile and requires ongoing commitment and support.

Queensland and ACT have no published metrics around their public sector human rights culture.[113] Surveys of the broader Queensland population following the implementation of the *Qld HRA* showed strong support for the importance and personal relevance of human rights, and such community support is likely to have a positive impact on public sector human rights culture.[114] Overall, the specific human rights laws appear to have had some success in developing stronger human rights cultures, but those cultures may need further encouragement to mature. The following section addresses the obligations under the specific human rights laws, which form a key component of the human rights culture.

B *Obligations under Human Rights Legislation*

The conduct and decision-making obligations require public sector agencies to take human rights into account in meaningful ways for each administrative action or decision, including a decision to implement novel data technologies. Table 2 sets out the relevant obligations under each human rights statute:

in 2022: Victorian Equal Opportunity and Human Rights Commission, *2022 Report on the Operation of the Charter of Human Rights and Responsibilities* (Report, August 2023) 37. See also the description of these interventions here: Grenfell and Debeljak (n 10) 225–6.

112 Grenfell and Debeljak draw a similar conclusion from the 2017 and 2018 data: Grenfell and Debeljak (n 10) 226.

113 'The [ACT] HR Act's impact on bureaucratic practices and culture remains difficult to assess, due in part to the absence of any ongoing or systematic initiative by the government to measure the HR Act's influence in this area': ibid 190.

114 Sarah Joseph, Chris Lane and Susan Harris Rimmer, 'What did Queenslanders Think of Human Rights in 2021? An Attitudinal Survey' (2022) 41(3) *The University of Queensland Law Journal* 363, 420.

***Table 2: Conduct and Decision-Making Obligations of the* Qld HRA, Victorian Charter *and* ACT HRA**

s 58(1) *Qld HRA*	s 38(1) *Victorian Charter*	s 40B(1) *ACT HRA*
It is unlawful for a public entity — (a) to act or make a decision in a way that is not compatible with human rights; or (b)in making a decision, to fail to give proper consideration to a human right relevant to the decision.	Subject to this section, it is unlawful for a public authority to act in a way that is incompatible with a human right or, in making a decision, to fail to give proper consideration to a relevant human right.	It is unlawful for a public authority — (a) to act in a way that is incompatible with a human right; or (b) in making a decision, to fail to give proper consideration to a relevant human right.[115]

The drafting similarities mean that Queensland courts tend to view cases considering s 38(1) of the *Victorian Charter* as relevant to their own conduct and decision-making obligations under s 58(1) of the *Qld HRA*.[116]

Generally, each provision is considered to consist of two obligations:[117]

- The substantive obligation: did the public authority act (and in Queensland, make a decision) compatibly with a human right, in terms of the substance or outcome?
- The procedural obligation: did the public authority give proper consideration to a relevant human right in making a decision?

Each obligation is 'an additional, or supplementary obligation, upon public authorities in the exercise of their statutory powers', such that a failure to discharge them renders the decision unlawful.[118]

For completeness, I will briefly discuss the interpretive obligations under each of the specific human rights laws, which require courts and agencies to

---

115 Inserted by the *Human Rights Amendment Act 2008* (ACT), modelled on s 38(1) of the *Victorian Charter* and s 6 of the *Human Rights Act 1998* (UK): Explanatory Statement, Human Rights Amendment Bill 2007 (ACT) 5.

116 See, eg, *Owen-D'Arcy v Chief Executive, Queensland Corrective Services* (2021) 9 QR 250, 298 [135]–[137] (Martin J) ('*Owen-D'Arcy*'). There is a more extensive body of Victorian precedent considering the relevant conduct and decision-making obligations than in Queensland or the ACT.

117 *Bare v Independent Broad-based Anti-Corruption Commission* (2015) 48 VR 129, 205 [245] (Tate JA) ('*Bare*'). See also Queensland Human Rights Commission, *Queensland's Human Rights Act 2019: A Guide for Public Entities* (Report, 2019) 12; ACT Human Rights Commission, *Human Rights Research Paper: Public Authorities* (Report, 2010) 3.

118 *Bare* (n 117) 234 [323] (Tate JA). It is worth noting that under s 40C of the *ACT HRA*, these obligations may be enforced by a direct right of action in the ACT Supreme Court. There is no equivalent under the *Qld HRA* or *Victorian Charter*, where such a claim of unlawfulness must be attached to another cause of action.

interpret (as far as possible) statutory provisions consistently with human rights.[119] In theory, the interpretive obligations could apply additional human rights protection, but that is unlikely to be the case for data privacy. Strictly, the obligations require data protection legislation (including the privacy principles) to be construed consistently with privacy rights and other applicable human rights.[120] This could support an argument that the two frameworks effectively collapse, replicating one another's effect. But courts have tended to read down these interpretive provisions, making them weaker in practice than the common law principle of legality.[121] In addition, data protection legislation is already considered to be (broadly) a form of human rights legislation,[122] intended to promote fair or responsible collection and handling of personal information.[123] So even if a court were prepared to apply the relevant interpretive obligation to the construction of data protection legislation, it may not have a major impact.[124]

The next sections outline how the conduct and decision-making obligations apply to public sector actions and decisions involving novel data technologies, which is the focus of this article.

C *Substantive Obligation*

The substantive obligation is generally applied in three steps: 'engagement, limitation, and justification'.[125] The first step assesses the relevance of the right, the second asks whether the applicant has demonstrated that the right is restricted or interfered with (construing the right broadly) and the third asks whether the defendant has established that the relevant restriction satisfies the proportionality test and is accordingly justified.[126] The proportionality test is set

---

119 *Qld HRA* (n 9) s 48; *Victorian Charter* (n 9) s 32; *ACT HRA* (n 9) ss 30–1.

120 See, eg, *Jurecek v Director Transport Safety Victoria* [2016] VSC 285, [24], [65] ('*Jurecek*'). In that case, Bell J was unable to fully explore the interaction, because the applicant did not serve the requisite notices under s 35 of the *Victorian Charter* to allow such a question of law to be adjudicated: [65]. But note that when Bell J assessed Freedom of Information ('FOI') legislation against the *Victorian Charter* right to freedom of expression in an earlier case, his Honour found the two to be inherently consistent in promoting the rights of applicants: see, eg, *XYZ v Victoria Police (General)* [2010] VCAT 255, [573] ('*XYZ*'). A similar outcome could be expected with data protection legislation, given that both data protection and FOI legislation can be considered to be human rights legislation or at least rights-supporting: see *Jurecek* (n 120) [24]; *XYZ* at [554].

121 Bruce Chen, 'Revisiting Section 32(1) of the Victorian Charter: Strained Constructions and Legislative Intention' (2020) 46(1) *Monash University Law Review* 174.

122 *Jurecek* (n 120) [24] (Bell J).

123 See, eg, *Qld IPA* (n 8) s 3; *PDPA* (n 8) s 1; *ACT IPA* (n 8) s 7.

124 In a forthcoming article I argue that courts should apply the interpretive obligation to inform their interpretation of 'unlawfully' in the privacy right — should they choose to do so, it would have a significant protective impact: Serena Hildenbrand, 'Public Sector Data Sharing: Applying State-based Human Rights Laws to Minimise Privacy Harms' (2023-24) 47(2) *Melbourne University Law Review* (advance).

125 *Austin BMI Pty Ltd v Deputy Premier* [2023] QSC 95, [306] (Freeburn J).

126 Ibid [306]–[307] (Freeburn J); *Baker (a pseudonynm) v DPP* (2017) 270 A Crim R 318, 331 [56] (Tate JA).

out in the general limitations clauses: s 13 of the *Qld HRA*, s 7(2) of the *Victorian Charter* and s 28 of the *ACT HRA*. Notably, it will not be possible for the implementation of a novel data technology to satisfy the general limitations clause if that implementation is unlawful.[127] European and New Zealand courts have construed this broadly, indicating that a measure (such as a new technology) will be considered unlawful if it does not have a clear and transparent legal basis for use, together with adequate procedural safeguards.[128] This question has been approached more narrowly in Australia, such that unlawfulness may simply mean not contravening an applicable law, such as data protection legislation.[129] I discuss this divergence further below, in exploring application of privacy rights.[130]

The substantive obligation unavoidably leads us to the question of which human rights are, or may be, engaged by a decision on the use of novel data technologies. Table 3 sets out potentially relevant rights, which are examined in more detail below, noting that in each case the relevant impacted rights may differ due to the nature of the technology. In almost all cases the text of the relevant right is essentially identical across the three jurisdictions.

Table 3: Human Rights Relevant to Novel Data Technologies in Queensland, Victoria and ACT

Right	Requirement (*Qld HRA* text)	*Qld HRA*	*Victorian Charter*	*ACT HRA*
Privacy and reputation	A person has the right — (a) not to have that person's privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and (b) not to have that person's reputation unlawfully attacked.	S 25	S 13	S 12
Recognition and equality before the law	(1) Every person has the right to recognition as a person before the law. (2) Every person has the right to enjoy the person's human rights without discrimination.	S 15(1)–(4)	S 8	S 8

127 *Thompson v Minogue* (2021) 67 VR 301, 318–19 [58] (Kyrou, McLeigh and Niall JJA) ('*Thompson*').

128 *Varga v Slovakia* (European Court of Human Rights, Chamber, Application 58361/12, 29 June 2021) [151] ('*Zoltan Varga*'), affd *Hascak v Slovakia* (European Court of Human Rights, Chamber, Application 58359/12, 24 May 2022) [89]. See also *R v Hansen* [2007] 3 NZLR 1, 62 [180] (McGrath J); *S and Marper v United Kingdom* [2009] 48 Eur Court HR 1169, 1196 [99] ('*Marper*').

129 *Thompson* (n 127) 318–19 [58] (Kyrou, McLeigh and Niall JJA).

130 I have argued that for this test of unlawfulness to offer an adequate level of protection in the face of novel data technologies, Australian courts would ideally be guided by the European and New Zealand approach and require a clear legal basis and procedural safeguards: Hildenbrand (n 124).

Right	Requirement (*Qld HRA* text)	*Qld HRA*	*Victorian Charter*	*ACT HRA*
	(3) Every person is equal before the law and is entitled to the equal protection of the law without discrimination. (4) Every person has the right to equal and effective protection against discrimination.			
Freedom of movement	Every person lawfully within [the jurisdiction] has the right to move freely within [the jurisdiction] and to enter and leave it, and has the freedom to choose where to live.	S 19	S 12	S 13
Freedom of thought	(1) Every person has the right to freedom of thought, conscience, religion and belief, including — (a) the freedom to have or to adopt a religion or belief of the person's choice; and (b) the freedom to demonstrate the person's religion or belief in worship, observance, practice and teaching, either individually or as part of a community, in public or in private.	S 20(1)	S 14(1)	S 14(1)
Freedom of expression	(1) Every person has the right to hold an opinion without interference. (2) Every person has the right to freedom of expression which includes the freedom to seek, receive and impart information and ideas of all kinds…	S 21	S 15	S 16
Peaceful assembly and freedom of association	(1) Every person has the right of peaceful assembly. (2) Every person has the right to freedom of association with others, including the right to form and join trade unions.	S 22	S 16	S 15
Taking part in public life	Every person in [the jurisdiction] has the right, and is to have the opportunity, without discrimination to participate in the conduct of public affairs, directly or through freely chosen representatives.	S 23(1)	S 18(1)	S 17
Property	A person must not be arbitrarily deprived of the person's property.	S 24(2)	S 20	–
Protection of children	Every child has the right, without discrimination, to the protection that	S 26(2)	S 17(2)	S 11(2)

Right	Requirement (*Qld HRA* text)	*Qld HRA*	*Victorian Charter*	*ACT HRA*
	is needed by the child, and is in the child's best interests, because of being a child.			

Privacy rights are likely to be engaged in any decision to adopt a novel data technology which uses or processes personal data. There have not yet been data privacy cases decided under the privacy provisions of the *Qld HRA*, and few cases in Victoria which consider privacy rights in the context of data privacy.[131] As noted above, there are significant European cases considering the use of novel data technologies such as facial recognition in the context of article 8 privacy rights under the *European Convention on Human Rights*, which differs slightly in its drafting from the Australian formulations in specifically requiring that no interference with privacy rights be permitted unless it is both 'in accordance with the law' and 'necessary in a democratic society'.[132] The settled view is that for the use of such a technology to be lawful and necessary, there must be a clear legal basis for its use, and a number of transparent safeguards in place, including to avoid the arbitrary application of any discretions.[133]

Under Australian human rights laws, a public sector agency assessing a novel data technology which may engage privacy rights is required to consider whether the proposed data use might unlawfully or arbitrarily interfere with privacy.[134] If it is considered to pose an unlawful interference (such as by contravening one or more applicable privacy principles)[135] it must not proceed to an assessment of

---

131 In the Victorian case *DPP v Kaba* (2014) 44 VR 526, the court found that the s 13 privacy right was engaged and limited by police officers' questioning of a suspect for his name and address data at a traffic stop, which is less of a data processing issue than a conventional privacy issue. Another Victorian case, relating to the retention of video footage from a protest, could be considered to involve data privacy but the Tribunal was not satisfied that the s 13 privacy right was engaged because there had been no attempt to identify the applicant from her image: *Caripis v Victoria Police* [2012] VCAT 1472.

132 *ECHR* (n 87) art 8(2).

133 See, eg, the summary of the settled position in *R (Bridges) v Chief Constable of the South Wales Police* [2020] 1 WLR 5037, [55]. In that case, the UK Court of Appeal found that the South Wales Police's safeguards around the use of facial recognition technology were inadequate: [94]. See also these European Court of Human Rights cases finding inadequate safeguards for the purposes of article 8 of the *ECHR* regarding a UK surveillance program and the use of facial recognition technology in Moscow, respectively: *Big Brother Watch v United Kingdom* (2022) 74 Eur Court HR 493; *Glukhin v Russia* (2024) 78 Eur Court HR 73.

134 The onus would not rest on the agency to demonstrate this in court; the onus would rest on a complainant to do so. But an agency discharging its conduct obligation would wish to be confident in its analysis that it could defend against such assertions.

135 If the proposal contravenes a legislated privacy principle, it is likely to be considered to be unlawful and accordingly in contravention of the privacy right: *Thompson* (n 127) 317 [49].

limitation and justification.[136] If it is assessed to arbitrarily interfere with privacy, it could potentially be justified by application of the relevant general limitations clause, discussed further below.[137] Applications of novel data technologies in the public sector that could engage and potentially limit the privacy right include AI/ML applications, image processing applications, biometric applications and automated decision-making applications, if they use or process personal data or de-identified personal data.

Rights to recognition and equality may be engaged by the use of any novel data technology application which results in differential outcomes for individuals based on attributes identified in or arising from the data. These rights are intended to include but might not be limited to protecting attributes already protected by anti-discrimination laws in the relevant jurisdictions.[138] A Robodebt-style algorithmic decision-making program might engage these rights if it is considered to systematically discriminate against vulnerable individuals or individuals in irregular employment, for example.[139] Other novel data technologies which might engage these rights include biometric technologies such as facial recognition algorithms (known to be less accurate in recognising people of colour)[140] and the use of AI or ML tools for predictive purposes, where the training data may reflect racial or socioeconomic bias.[141]

The right to freedom of movement could be impacted by any image-processing surveillance, such as CCTV analytics, given that it may have the effect of chilling movement. Similarly, the widespread use of Automated Number Plate Recognition cameras by law enforcement could engage this right. In Queensland,

---

136 In *Thompson* the Victorian Court of Appeal indicates that if the conduct is unlawful '[i]t will be impossible for the public authority to meet the justification requirement', so there is no point continuing the analysis: ibid 318–19 [58].

137 The *Thompson* court notes that while it would be technically possible to justify conduct found to be arbitrary it would 'ordinarily, be very difficult' because the tests overlap: ibid 318–19 [58].

138 See, eg, *Austin BMI Pty Ltd v Deputy Premier* [2023] QSC 95, [317]–[320]. In that case, Freeburn J notes that the *Qld HRA* and *ACT HRA* have an inclusive definition of 'discrimination' but considered the definition in the *Qld HRA* to be limited to attributes *analogous* to those protected by anti-discrimination laws: [317]–[318]. Compare the narrower definition under the *Victorian Charter*, which is restricted to attributes already protected by anti-discrimination laws.

139 Karen Yeung and Adam Harkins, 'How do "Technical" Design-Choices Made When Building Algorithmic Decision-Making Tools for Criminal Justice Authorities Create Constitutional Dangers? (Part II)' (2023) (Jul) *Public Law* 448; Miller (n 20); Natalie Sheard, 'Employment Discrimination by Algorithm: Can Anyone be Held Accountable?' (2022) 45(2) *University of New South Wales Law Journal* 617. Note that this consideration raises large questions in the context of a program like Robodebt, where a substantial proportion of affected individuals are likely to be vulnerable — but that is good grounds for exercising extra care.

140 Drew Harwell, 'Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use', *The Washington Post* (online, 19 December 2019) <https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/>.

141 Julia Dressel and Hany Farid, 'The Accuracy, Fairness, and Limits of Predicting Recidivism' (2018) 4(1) *Science Advances* 5580.

such cameras are used to detect unregistered and uninsured vehicles and automatically issue infringement notices.[142]

The rights to freedom of thought and expression may be engaged by technologies processing opinions previously expressed or inferred, including religious opinions. For instance, AI- or ML-based risk assessments and recidivism predictions in the criminal justice system may incorporate previously expressed views or activism.[143]

The rights to peaceful assembly and freedom of association would be impacted by restrictions applied to the free assembly of citizens for protests, including by means of image-processing or biometric technologies. One controversial issue has been the use of CCTV to monitor peaceful gatherings — such activity resulted in a *Victorian Charter* case, *Caripis v Victoria Police*, in which the applicant unsuccessfully asserted an infringement of her rights to freedom of expression and peaceful assembly due to retention of protest footage by law enforcement.[144]

If a technology will collect or process data from citizens under 18 years-of-age, children's rights to protection may be engaged. Public sector agencies should be conscious of the need to consider the 'best interests of the child' and make special provision to protect children when dealing with datasets including children's personal data (such as birth certificate, passport or driver licence datasets), or collection mechanisms which may capture children's images.[145] Biometric technologies may be inappropriate for use with children, due to their inability to fully consent to the potential life-long implications of the collection.

A right not to be deprived of property is included in the *Qld HRA* and *Victorian Charter* but not the *ACT HRA*. Moreover, the *Qld HRA* includes a reference to arbitrariness lacking in s 20 of the *Victorian Charter*, which only precludes unlawful deprivation of property (see Table 4). This right may be engaged more rarely in relation to novel data technologies, but may be relevant where an automated decision-maker imposes an unjust penalty or fine (see the discussion of Robodebt below in Part V).

Finally, the right to take part in public life is relevant if a data technology, such as automated cleansing of voter rolls, impacts access to voting, or engagement with political parties.

To summarise, the substantive obligation requires that the public sector agency's actions and decisions be compatible with the rights listed above. While

---

142 'Automated Number Plate Recognition Cameras', *Queensland Government* (Web Page, 15 June 2023) <https://www.qld.gov.au/transport/safety/fines/number-plate-recognition-cameras>.

143 Dressel and Farid (n 141).

144 *Caripis v Victoria Police* [2012] VCAT 1472, [76]. Since then, an applicant has been successful in a similar human rights case in the United Kingdom: *Catt v United Kingdom* (2019) 69 Eur Court HR 177.

145 The principle of protecting 'the best interests of the child' has a solid foundation in international human rights laws, deriving from the United Nations Convention on the Rights of the Child: *Convention on the Rights of the Child*, 1577 UNTS 3 (signed and entered into force 20 November 1989). See also Committee of the Rights of the Child, *General Comment No 25 on Children's Rights in Relation to the Digital Environment*, Doc No CRC/C/GC/25, 2 March 2021.

the substantive and procedural obligations are legally independent of one another,[146] effective application of the procedural obligation should assist the agency in complying with the substantive obligation, and vice versa.

D *Procedural Obligation*

Courts have tended to take a pragmatic approach to the procedural obligation, given that non-legally qualified public servants must be able to undertake this task as part of their regular work. There is a slightly more stringent approach in Queensland, where the Queensland Supreme Court case of *Owen-D'Arcy v Chief Executive, Queensland Corrective Services* ('*Owen-D'Arcy*') confirmed that due to s 58(5) of the *Qld HRA* it is necessary in that State for the agency to correctly identify all applicable rights.[147] The general test arises from the judgment of Emerton J in an early *Victorian Charter* case, *Castles v Secretary of the Department of Justice* ('*Castles*')[148]. This test was summarised in *Bare v IBAC* ('*Bare*') and re-stated by the Court of Appeal in *HJ v IBAC* ('*HJ*') to the effect that a public sector decision-maker must: (1) understand which human rights may be relevant and how the decision might impact them; (2) seriously consider the impact of the decision on those rights; (3) identify countervailing interests; and (4) balance the competing interests as part of the task of justification.[149]

In *Castles*, Emerton J emphasised the normative role of the conduct obligation, stating that it is not expected to be a 'sophisticated legal exercise'.[150] How would a public servant discharge this obligation when required to make a decision on the use of a novel data technology? As a matter of policy, public sector agencies usually prepare a written assessment to assist with discharging the procedural obligation, to demonstrate that they have given proper consideration to human rights (and acted accordingly).[151] While this goes by different names in

---

146 *Thompson* (n 127) 327 [101].

147 *Owen-D'Arcy* (n 116) 298 [136]–[137] (Martin J). This approach was affirmed and followed by the Queensland Supreme Court: *Austin BMI Pty Ltd v Deputy Premier* [2023] QSC 95, [355]–[356] (Freeburn J). A subsequent Supreme Court case appeared to soften the approach but did not clearly depart from *Owen-D'Arcy*: *BZN v Chief Executive, Department of Children, Youth Justice and Multicultural Affairs* [2023] QSC 266, [240] (Crowley J).

148 *Castles v Secretary of the Department of Justice and Others* (2010) 28 VR 141 ('*Castles*').

149 *HJ (pseudonym) v Independent Broad-based Anti-corruption Commission* (2021) 64 VR 270, 306 [155] (Beach, Kyrou and Kaye JJA), citing ibid 184 [185]–[186]; *Bare* (n 117) 198–9 [217]–[221], 218–23 [277]–[289], 297–8 [535]–[536].

150 *Castles* (n 148) 184 [185]–[186].

151 This is not required by the legislation but 'practically, such a record will be critical to meet any allegation that the public entity failed to give proper consideration to human rights as required by the "procedural limb"': Brenna Booth-Marxson and Kent Blore, 'Breathing life into the *Human Rights Act 2019* (Qld): The ethical duties of public servants and lawyers acting for government' (2022) 41(1) *University of Queensland Law Journal* 1, 26–7.

different jurisdictions,[152] I will refer to this document as a 'rights assessment'.

A rights assessment has no required format, but should identify the engagement of human rights plus any limitation of those rights, and assess whether the limitation is reasonable and justified by application of the relevant general limitations clause.[153] In the case of a novel data technology, the rights assessment should (at a minimum) outline the nature of the technology and any associated data flows, identify any human rights it might engage, and consider any limitation of those rights and possible mitigations to prevent such an impact. Should a limitation be identified, the rights assessment would need to step through the applicable general limitations clause in relation to that limitation. Unlike in Victoria and the ACT, s 58(5) of the *Qld HRA* requires that public servants consider 'whether the decision would be compatible with human rights' as part of the procedural requirement, which may make application of the general limitations clause mandatory as part of the rights assessment in Queensland.[154]

The level of consideration required will depend to a degree on the circumstances. In *Bare*, Tate JA described s 38(1) 'proper consideration' as requiring a higher standard of consideration than generally required at common law.[155] In *Certain Children (No 2) v Minister for Families & Children*, John Dixon J noted that the standard required in that case (impacting the interests of vulnerable child detainees) would be higher than for *Castles* (which concerned an adult prisoner seeking access to in vitro fertilisation services).[156] On the other hand, in *Owen-D'Arcy*, Martin J noted that '[d]ecision-makers … are not expected to achieve the level of consideration that might be hoped for in a decision given by a judge'.[157]

What should be the appropriate level of 'proper consideration' for a program involving novel data technologies? In the case of new technologies, the decision-maker arguably has a higher responsibility to understand the inherent privacy impacts of the project. The European Court of Human Rights considered in *S and*

---

[152] In Queensland, it can be a Human Rights Impact Assessment or a File Note: see, eg, Queensland Government, 'Human rights resources' (Web Page, 2020) <https://www.forgov.qld.gov.au/service-delivery-and-community-support/design-and-deliver-public-services/comply-with-the-human-rights-act/human-rights-resources>. In Victoria, it is generally called a Charter assessment: see, eg, *Loielo v Giles* [2020] VSC 722, [75], [77]. In the ACT, it is simply a documented consideration: see, eg, ACT Human Rights Commission, Achieving the Rights Outcome (2015) 4, 21–3 <https://www.hrc.act.gov.au/___data/assets/pdf_file/0005/2305481/Achieving-the-Rights-Outcome.pdf>.

[153] See, eg, this Queensland guide to the rights assessment which includes a template for agencies to complete at Appendix A: Queensland Government, *Human Rights Guide: Reviewing Policies and Procedures for Compatibility with Human Rights* (Report, 1 June 2019) 4.

[154] See (n 147).

[155] *Bare* (n 117) 203 [235].

[156] *Certain Children v Minister for Families and Children (No 2)* (2017) 52 VR 441, 584 [491] ('*Certain Children (No 2)*'). Dixon J indicated that the standard expected of the Minister was higher due to having received high-quality legal advice and due to the vulnerability of the children impacted by the decision: [203], [491]–[492].

[157] *Owen-D'Arcy* (n 116) 298 [137].

Marper v United Kingdom ('*Marper*') that a particular duty applied to European jurisdictions in relation to novel technologies in the context of the equivalent European right to privacy:

> the protection afforded by [privacy rights] would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.... [A]ny State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.[158]

While this approach has not been expressly adopted in Australian jurisdictions, the relevant human rights statutes all provide that courts may consider foreign jurisprudence on similar provisions.[159] Even though European rights to privacy do not include an equivalent procedural obligation, *Marper* provides persuasive guidance for applying a high bar to the procedural consideration of novel data technologies, where the full range of potential consequences is not well known. In this context, the next section explores how the rights assessment process for novel data technologies could be bolstered by applying contemporary risk-based methodologies.

E *Risk Management as an Approach to Discharging the Obligations*

A challenging element of assessing novel data technologies is that their full impact is not always clear at the outset, and there is often uncertainty around their design, scope, outcomes and the extent to which they engage and limit human rights.[160] Where there is potential limitation of human rights and considerable uncertainty, risk-based methodologies can be a useful tool. Further, if a novel data technology poses potentially significant risks to human rights, there is a strong basis for the application of risk management based on the precautionary principle, 'to regulate the intervention before we are sure that it presents a serious threat, and before it is released and dispersed widely'.[161] In this context, it is worth noting that risk management based on the precautionary

---

158 *Marper* (n 128) [112]. The Court made these comments in relation to the novel use of DNA technologies by United Kingdom law enforcement agencies. The Court held that the retention of DNA samples and fingerprints of suspects for an unlimited time 'constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society': [125].

159 *Qld HRA* (n 9) s 48(3); *Victorian Charter* (n 9) s 32(2); *ACT HRA* (n 9) s 31(1).

160 Yeung and Harkins helpfully explore the potential breakdown between technical goals and policy goals in the establishment of one type of novel data technology (automated decision-making algorithms) and indicate the range of uncertainty of outcomes that might accompany such a tool: Yeung and Harkins (n 139). This is emblematic of the issues across novel data technologies, where technical goals and outcomes may diverge widely from policy goals and outcomes, with neither side fully understanding the other.

161 Alan Randall, *Risk and Precaution* (Cambridge University Press, 2011) 7.

principle is not uncontroversial — opponents argue that it requires intrusive regulation, deals badly with the choice between more and less risky options, implicitly favours the 'do nothing' option, discourages innovation and encourages unfounded panic around risks which may not eventuate.[162] But where there is human rights legislation in place requiring public servants to work through the potential impact of a novel data technology on human rights, such a precautionary approach would be advantageous.

Is risk management an appropriate approach to the protection of human rights? The *GDPR* incorporates some risk management approaches in its approach to accountability obligations on data controllers,[163] which has led to critical inquiry around the relationship between risk management and fundamental rights. Gellert describes how a risk-based approach has been critiqued for being overly business-friendly and eroding rights.[164] But he considers rights-based and risk-based approaches to data protection to be fundamentally compatible, given that both are based on the proportionality principle, namely, the balancing of various rights and interests.[165] Yeung and Bygrave comment that attempts to apply risk assessment to rights can 'seem to fly in the very face of their jurisprudential structure and philosophical foundations',[166] but in attempting to reconcile this, they propose a distinction between clear violations of rights, which should not be risk-managed, and 'borderline' cases where a risk-based approach applying additional scrutiny and safeguards may produce an acceptable outcome.[167]

Italian legal scholar Alessandro Mantelero began working on the use of human rights impact assessments for AI technologies in 2018, developing the concept into a book in 2022.[168] His 'general theory on the risk-based approach' involves four documented steps, namely identifying risks posed by the technologies; analysing their impact; selecting and applying mitigation measures; and undertaking regular review of the measures' effectiveness.[169] The Australian government's recent discussion paper 'Safe and Responsible AI in Australia' identifies 'a developing international direction towards a risk-based

---

162 Ibid 17–25.

163 *GDPR* (n 7). See, eg, art 36: '[t]he controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.'

164 Raphaël Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press, 1st ed, 2020) 2.

165 Ibid 10–11.

166 Karen Yeung and Lee A Bygrave, 'Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship' (2022) 16(1) *Regulation & Governance* 137, 146.

167 Ibid.

168 Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34(4) *Computer Law & Security Review* 754; Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (n 80).

169 Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (n 80) 50.

approach for governance of AI',[170] including in the EU *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence* ('*AI Act*'),[171] and invites consideration of a risk-based approach to addressing the regulation of AI in Australia.[172] Similarly, the facial recognition model law proposed by a group from the University of Technology Sydney ('UTS Model Law') includes a human rights risk-assessment model.[173] Like Yeung and Bygrave, the UTS Model Law identifies that while some human rights are absolute and must not be limited, a risk-based model may be used with non-absolute human rights like the right to privacy.[174] All of the human rights identified in Table 3 are non-absolute under the *Qld HRA*, *Victorian Charter* and *ACT HRA* (although some aspects of the rights to recognition and to freedom of thought may be considered absolute at international law).[175]

A risk assessment may duplicate some of the elements of a proportionality analysis under human rights law,[176] but carries several practical benefits. First, the risk assessment process could be undertaken by any mid-level public servant (preferably by a member of the project team, with a close knowledge of project design), with the less familiar proportionality analysis undertaken afterwards by specialist staff: an internal legal team or a data privacy officer. Second, a risk assessment encourages more express 'quantification' of risk into categories such as high, medium and low — Mantelero outlines the importance of quantifying risk and setting a threshold for acceptability.[177] Third, a risk assessment is generally understood by project teams in a way that a legal advice may not be, and may be more likely to produce action to mitigate extreme and high risks.

Overall, a risk-based approach can appropriately add value to a rights assessment, provided it is recognised that in the face of a clear violation of rights or attempts to limit absolute rights, the use of risk management techniques will be inappropriate. Risk assessment generally involves a structured consideration of the potential consequences or severity of the action and the likelihood of each consequence occurring.[178] Qualitative risk assessments commonly use a two-

---

170 Department of Industry Science and Resources, *Safe and Responsible AI in Australia* (Discussion Paper, June 2023)16.

171 Ibid 39, citing *AI Act* (n 7).

172 Department of Industry Science and Resources (n 170) 40–1.

173 Nicholas Davis, Lauren Perry and Edward Santow, The University of Technology Sydney, *Facial Recognition Technology: Towards a Model Law* (Report, September 2022) 45–56. The risk-based assessment model proposed by this group in respect of facial recognition assessments is not dissimilar to the model I propose in this article for novel data technologies more broadly.

174 Ibid 56.

175 The relevant human rights legislation specifies that these rights may be limited: *Qld HRA* (n 9) s 13; *Victorian Charter* (n 9) s 7(2); *ACT HRA* (n 9) s 28. For non-derogable international law rights, see *ICCPR* (n 87).

176 '[W]hen we do a legal proportionality test what we do is actually much closer to risk management than the current framing of the issue allows us to imagine and/or admit': Gellert (n 164) 10.

177 Mantelero (n 80) 52.

178 International Organization for Standardization, *ISO Guide 73: Risk Management* (2009) [1.1].

variable matrix, with 'severity' on one axis and 'likelihood' of occurrence on the other (see Figure 3).

Figure 3: A Classic 5 x 5 Risk Matrix

		Severity				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost certain (76–100%)	Medium	High	High	Extreme	Extreme
	Likely (51–75%)	Medium	Medium	High	Extreme	Extreme
	Possible (31–50%)	Low	Medium	Medium	High	Extreme
	Unlikely (11–30%)	Low	Low	Medium	High	High
	Rare (0–10%)	Low	Low	Low	Medium	High

The categories of likelihood and severity should be clearly defined, to assist with consistent risk assessment.[179] Severity ratings (such as the distinction between minor and moderate) should be defined by reference to the types of projects or activities prevalent in that business area.

Despite scholarship such as Mantelero's, a structured risk assessment process is not currently a common element of rights assessments in Australia. Completed rights assessments are rarely published, so it can be difficult to draw conclusions about their use or effectiveness. Anecdotally, as illustrated by an exemplar rights assessment published by the Queensland government, rights assessments may step through the relevant rights and conclude that no rights are limited, or that any limitations to rights are justified — without recommending changes to program design or mitigations.[180] In such cases the assessment risks becoming a 'tick box' exercise. Another such example is the Victorian City of Yarra's 2022 assessment of proposed amendments to its governance rules ('City of Yarra Assessment'), which concludes in relation to each *Victorian Charter* right that the right is not engaged, or that the rules document 'imposes a reasonable

[179] See, eg, some sample severity ratings included below at n 208.

[180] Queensland Department of Education, 'Human Rights Impact Assessment: Decision Making' (Web Page, 2022) <https://ppr.qed.qld.gov.au/attachment/human-rights-impact-assessment-exemplar.docx>. As noted above, consideration of the general limitations clause may be mandatory in Queensland, so the failure of this exemplar to step through that clause is curious — particularly the failure to document possible alternative approaches in the exemplar.

limit on this human right', with no amendments proposed.[181] No specific format is prescribed for rights assessments, and neither the Queensland exemplar nor the City of Yarra Assessment describe the methodology or approach used to reach their conclusions, or propose alternative approaches.[182] The Queensland government has produced some helpful guidance for public servants around applying the substantive and procedural obligations in decision-making and asking relevant questions. However, it does not mention documenting the assessment in a structured way.[183] Such an opaque approach is not ideal in any case, but is particularly problematic when dealing with novel data technologies, where there are a range of complexities and possible outcomes and impacts that would ideally be assessed and documented. It would be unfortunate for public servants to deprive us of the benefits of novel data technologies due to misconceptions or a poor understanding of risk trade-offs, but equally undesirable for them to make overly optimistic assumptions about potential harms. Without a structured methodology, both outcomes are possible.

Introducing a more structured risk-based assessment into the rights assessment for novel data technologies may assist in building analytical skills in public servants around human rights protection, and thereby promote a stronger human rights culture. This approach aligns with UK Supreme Court justice Lord Sales' advocacy for structured *ex ante* reviews of AI technologies by public servants, including the need to develop the relevant skills within government.[184] My proposed approach, not dissimilar from Mantelero's,[185] is illustrated in Figure 4:

---

181 City of Yarra, 'Charter of Human Rights and Responsibilities Assessment: Governance Rules' (Web Page, 2022) <https://www.yarracity.vic.gov.au/-/media/files/events/council-and-pdc-meetings/2022-meetings/council-23-august-2022/item-8_1-attachment-7-governance-rules-human-rights-assessment.pdf>.

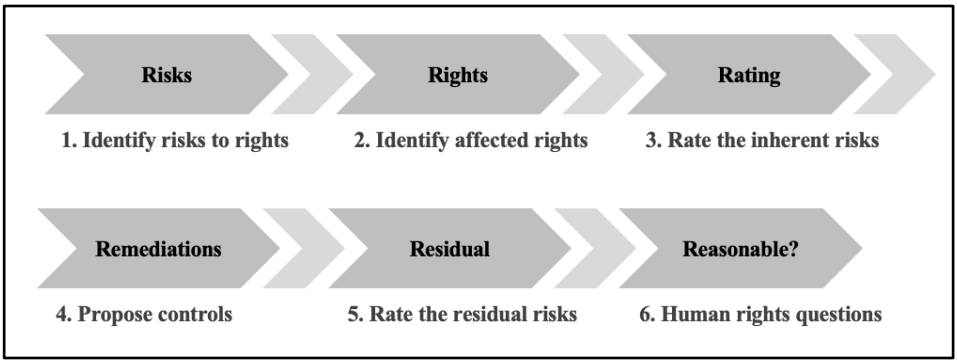
182 Ibid; Queensland Department of Education (n 180).

183 Queensland Government, 'Guide: Human Rights in Decision Making, A Guide for Queensland Government staff' (Web Page, 2020) <https://www.forgov.qld.gov.au/___data/assets/pdf_file/0024/184029/guide-human-rights-in-decision-making.pdf>.

184 Lord Sales, 'Algorithms, Artificial Intelligence and the Law' (2020) 25(1) *Judicial Review* 46, 53–4. Lord Sales was not convinced that such tasks could be resourced by existing government structures or personnel and proposed a new expert scrutiny agency to take on this role, including by allowing legal challenges to proceed prior to implementation: 54–7. See also Goldenfein's encouragement for public servants to rigorously assess new technologies: Goldenfein (n 22) 59.

185 Mantelero (n 80) 50. See also Mantelero's discussion of the likelihood and severity model and mitigation measures: 55–8.

Figure 4: The 6 'R's of Risk-Based Rights Assessment



The first two steps would generally be done together — identifying risks to rights (step one) and the corresponding rights (step two). The 'risk' is the potential undesirable outcome (eg personal information could be shared without adequate justification) and the 'affected right' is the relevant impacted human right (eg, privacy). This should involve scrutiny of the proposed technology and a degree of ethical imagination to work through potential consequences — this needs to be within the reach of mid-level public servants.[186] The importance of a human rights culture was outlined above, and that mindset and those associated skills within a public sector agency will be useful in this context. A table such as Table 4 would ideally be used to record the outputs, as part of the rights assessment.

Table 4: Risk Assessment Table, Showing Corresponding Step Number from Figure 4

1. Risk	2. Affected right	3a. Likeli-hood	3b. Severity	3c. Inherent risk	4. Control	5a. Likeli-hood	5b. Severity	5c. Residual risk

Once the relevant risks are identified and recorded, the Figure 3 matrix can be used to identify the likelihood and severity of the risk and therefore its inherent rating (step three) — where the inherent rating is the applicable risk level (low, medium, high or extreme) in the absence of any mitigation measures. Public agencies are likely to have a risk framework documenting acceptable risk levels. The acceptance of a risk rated higher than 'medium' is likely to depend on the benefits of the program and require senior-level approval. If the inherent rating is not acceptable with regard to the agency's risk appetite, it will be necessary to

186 Goldenfein (n 22) 59.

apply mitigation measures (step four) to produce a reduced *residual* risk. Appropriate mitigation measures for risks arising from the use of novel data technologies may include:

a) **Structural compliance mechanisms**: such as regular testing, auditing, or certification of the technology if available.[187]

b) **Privacy-by-design:** incorporating privacy protective measures in the design, such as by minimising the use of personal data.

c) **Security-by-design:** incorporating security controls in the design, such as encryption, security testing, and a security governance framework.

d) **Prototyping and pilots:** using a prototype or pilot approach (processing test data only), so that any impact on human rights can be explored and better understood.

e) **Human in the loop/oversight assessments:** despite well-founded concerns over reliance on 'human in the loop' to address AI risks,[188] it may be appropriate to embed an element of meaningful human review and oversight.[189]

Once the relevant mitigation measures are defined and inserted into the rights assessment, the next step is to determine a residual risk rating for each risk, based on the adjusted likelihood and severity ratings as a result of the treatment (step five). If any residual risks remain unacceptably high, additional mitigation measures can be added. While this approach should assist in reducing risks and producing a better project design to minimise impact on human rights, it may not eliminate such impacts. Because human rights are not absolute under Australian state or territory human rights legislation and can be limited in reasonable ways, the final step (step six) involves a proportionality analysis, essentially an evaluation of whether the limitations are reasonable by applying the relevant general limitations clause: s 13 of the *Qld HRA*, s 7(2) of the *Victorian Charter* or s 28 of the *ACT HRA*.[190]

While the wording of the general limitations clauses across the three jurisdictions varies slightly, they are similar and the variations are unlikely to result in substantial differences in effect. Blore asserts that the s 13 elements in

---

187 Ibid 51.

188 Reuben Binns, 'Human Judgment in Algorithmic Loops: Individual Justice and Automated Decision-Making' (2022) 16(1) *Regulation & Governance* 197. 'Human in the loop' is the concept of including human oversight of algorithmic decision-making systems to ensure a just outcome; but reliance on this as a safeguard has been critiqued because humans may apply their discretion in unfair ways, and may influence or by influenced by the technology: 207–8.

189 The discussion paper 'Safe and Responsible AI in Australia' proposes this as a risk control: Department of Industry Science and Resources (n 170) 40.

190 Victorian Equal Opportunity and Human Rights Commission, *The Charter of Human Rights and Responsibilities: A guide for Victorian public sector workers* (Report, June 2019) 16.

the *Qld HRA* reflect the four elements contained in the 'structured proportionality analysis' used in human rights systems internationally, and that each is necessary and sufficient to that goal: '[e]ach step tests the reasonableness of the limit on human rights from a slightly different angle, such that skipping a step means failing to test the reasonableness of the measure from that angle'.[191] Blore describes those four sequential elements, reflected in each of the general limitations clauses, as follows:[192]

(i) the limit has a proper purpose;

(ii) there is a rational connection between the limit and that purpose;

(iii) the limit is necessary to achieve its purpose, in the sense that the purpose cannot be achieved without limiting the human right or by limiting it to a lesser extent; and

(iv) the limit strikes a fair balance between the need to achieve its proper purpose and the human right at stake.[193]

There is one additional element covered in each of the general limitation clauses, namely the requirement that the limitation be lawful.[194] Table 5 shows these five elements as questions tailored for the use of a novel data technology.

---

191 Kent Blore, 'Proportionality under the *Human Rights Act 2019* (Qld): When Are the Factors in s 13(2) Necessary and Sufficient, and When Are They Not?' (2022) 45(2) *Melbourne University Law Review* 419, 421.

192 Ibid 435.

193 Blore also refers to the 'seminal' Canadian case *R v Oakes* [1986] 1 SCR 103, a noted authority on structured proportionality: Ibid 426. Speaking for the Supreme Court in *R v Oakes*, Dickson CJ summarises the elements as (1) the measures must be rationally connected to the objective; (2) the means should limit rights as little as possible; and (3) there must be 'a proportionality' between the impact of the measures and a sufficiently important objective: [70].

194 *Victorian Charter* (n 9) s 7(2); *Qld HRA* (n 9) s 13(1); *ACT HRA* (n 9) s 28.

Table 5: Human Rights Questions for Novel Data Technologies (Arising from General Limitations Clauses)

	If there is potential limitation of human rights by the technology:	***Qld HRA***	***Victorian Charter***	***ACT HRA***
1	Is there a clear legal basis for the use of the technology?	13(1):subject under law'	7(2): 'subject under law'	28(1): 'set by laws'
2	Does the use of the technology have a proper purpose?	13(2)(b): 'nature of the purpose' and 13(2)(e): 'the importance of the purpose of the limitation'.	7(2)(b): 'importance of the purpose'	28(2)(b): 'importance of the purpose'
3	Is there a rational connection between any potential limitation on human rights and that purpose?	13(2)(c): 'the relationship between the limitation and its purpose'	7(2)(d): 'the relationship between the limitation and its purpose'	28(2)(d): 'the relationship between the limitation and its purpose'
4	Is the limitation necessary to achieve the purpose (or is there an alternative approach which would be less restrictive?)	13(2)(d): 'any less restrictive and reasonably available ways to achieve the purpose'	7(2)(e): 'any less restrictive means reasonably available to achieve the purpose'	28(2)(e): 'any less restrictive means reasonably available to achieve the purpose'
5	Does the limitation strike a fair balance between the proper purpose and the human right?	13(2)(g): 'the balance between the matters' [the importance of the limitation and of preserving the right]	7(2): 'such reasonable limits as can be demonstrably justified in a free and democratic society'	28(2): 'whether a limit is reasonable'

This may appear repetitive, given that some elements of Table 5 will no doubt be considered during the first five steps in Figure 4. Those first steps should be viewed as preparing the best proposal possible, minimising human rights impacts. In most cases, this should be undertaken by staff with a close understanding of the project, preferably staff on the project team — who would ideally also prepare an overview of the proposed use of the technology as an introduction to the rights assessment.[195] Step six is more likely to be undertaken by a legal team or data privacy officer exercising oversight, providing a check on the work done by the project team to reduce human rights impacts. For smaller projects, it should be feasible to complete the first five steps and record the outputs in Table 4 in a relatively short timeframe — the rights assessment is not expected to be a polished piece of work, simply a documented record of reasonable considerations. Some might wonder why the program's legal basis is not fully considered until step six, given that legality is a threshold question (as already noted, an illegal program cannot be justified under human rights laws). The project team working on the first five steps is unlikely to feel comfortable assessing legal basis, which may be best handled by specialist staff (lawyers or data privacy professionals). But those specialist staff will benefit from having the detail of the proposal and technology fleshed out by the project team before they do an overall assessment of proportionality. Accordingly, the deferral of this consideration until step six is a practical matter, rather than a comment on its importance in the assessment.

The next section works through the steps using a hypothetical situation, to demonstrate how the application of this approach may layer meaningful safeguards over potentially inadequate legal frameworks regarding the use of novel data technologies.

V Application to a Robodebt-Type Program

The Australian government's Robodebt program did not use AI but employed automated processes to evaluate personal data,[196] so it can be viewed as the use of a novel data technology. Hypothetically, we will relocate that program to a state-based program in Queensland, and consider how the *Qld HRA* and the risk-based assessment process outlined above may have resulted in a different outcome.

For our purposes, it is useful to examine the Robodebt elements that were apparent during program design and pre-implementation, because this is the period when public servants would ideally have identified and controlled relevant

---

195 Such an introduction is usually prepared for any privacy impact assessment and could be re-used for the rights assessment with minor modifications. A reliable overview of the project, data flows and technologies will assist the specialist staff to efficiently and accurately undertake step 6.

196 *Robodebt Report* (n 1) 472.

risks. According to the Royal Commission, the 'five significant differences' introduced by Robodebt compared to previous debt recovery programs were:

a) the use of unconfirmed wage data as the basis for earned income;

b) the provision of unconfirmed information as a debt, with the onus on the recipient to dispute it (a reversed onus of proof) or accept the estimated debt plus an automatic 10 per cent 'recovery fee';

c) income-averaging used as a default approach to calculate the debt for each fortnight;

d) an almost entirely automated online process with minimal human involvement or assistance; and

e) retrospective effect reaching back five years, instead of the previous process that only reached back 12 months.[197]

Early legal advice raised questions about the legal basis for income-averaging and recommended legislative change to support the program, but was ignored.[198] In addition to the lack of a legal basis for income-averaging, the Royal Commission noted the lack of a basis for the 10 per cent penalty, the onus placed on recipients and the purportedly compulsive demands to recipients to provide information.[199] Easily-anticipated fairness issues arose from the fact that welfare recipients had not been told to retain more than six months of employment data, so would struggle to access employment records reaching back five years. Such issues also arise from: the complexity of the online system and the lack of available assistance for a vulnerable population; the use of outdated recipient contact information preventing many from receiving notifications of their 'debt'; and a lack of adequate explanation of the process.[200] In terms of the calculation, '[t]here was no meaningful human intervention in the calculation and notification of debts'[201] and it later emerged that the calculation error rate was at least 27 per cent.[202]

From a privacy perspective, the program relied on data-matching under the *Data-matching Program (Assistance and Tax) Act 1990* (Cth).[203] The Office of the

197 Ibid xxiv–xxv.

198 Ibid 26–7. The Royal Commission notes that had this advice been followed and legislative change sought, the required changes 'would certainly have encountered parliamentary and public opposition': ibid xxv.

199 Ibid xxv–xxvi.

200 Ibid xxvi–xxvii. In relation to the retention of work documentation, the target population could be expected to have a higher incidence of casual work and health challenges than the general population, so it was foreseeable that they would find these requirements particularly difficult and unfair.

201 Ibid 477.

202 Bill Shorten, 'Questions without notice on the Royal Commission into Robodebt' (Web Page, 7 February 2023) <https://ministers.dss.gov.au/transcripts/10181>.

203 'Centrelink Data Matching Activities' *Services Australia* (Web Page, 3 March 2022) <https://www.servicesaustralia.gov.au/centrelink-data-matching-activities>.

Australian Information Commissioner ('OAIC') prepared voluntary *Guidelines on data matching in Australian government administration* ('Guidelines') under the *Privacy Act* for application in such situations.[204] The Guidelines are voluntary but considered best practice and they contemplate the development of a Protocol for each data matching program; Centrelink had developed a Protocol in 2004 and lodged it with the OAIC.[205] According to the Royal Commission, the Robodebt program was inconsistent with the 2004 Protocol in a number of ways, including around data retention and the role of manual checking.[206] A new 2017 Protocol replaced the 2004 Protocol during the Robodebt program, but Robodebt did not comply with this new protocol's data retention requirements either.[207]

If we were to relocate a proposed Robodebt program to Queensland, a Queensland public agency would be required to complete a rights assessment before approving the program to proceed. Public servants assessing the program design in the light of the *Qld HRA* would be well-advised to step through the Figure 4 approach, recording the results in their rights assessment in a table like Table 6 below. In terms of methodology, Table 6 applies the Figure 3 risk matrix, using the likelihoods defined in Figure 3 and simple severity definitions.[208] (Most government departments and agencies would have their own organisational risk matrix with definitions appropriate to their portfolio, which they should apply.)

---

204 Office of the Australian Information Commissioner, 'Guidelines on data matching in Australian Government administration' (Web Page, 18 June 2014) <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/government-agencies/guidelines-on-data-matching-in-australian-government-administration>. This is the latest version of the Guidelines, but versions have been in place since 1992: *Robodebt Report* (n 1) 449.

205 *Robodebt Report* (n 1) 449.

206 Ibid 458.

207 Ibid 456, 458.

208 For the purposes of Table 6, I applied the following simple severity definitions, which are simply an attempt to divide potential consequences into five sequential levels:
Severe: loss of life, severe impact to more than 100 individuals, some impact to over 10,000 individuals, major litigation, major adverse media attention or reputational damage and/or severe impact on program delivery.
Major: personal injury, severe impact to 10–100 individuals, some impact to 1000–10,000 individuals, litigation, significant reputational impact, and/or major impact on program delivery.
Moderate: severe impact to fewer than 10 individuals, some impact to 100–1000 individuals, limited reputational impact and/or moderate impact on program delivery.
Minor: some impact to 10–100 individuals and/or minor impact on program delivery.
Insignificant: some impact to fewer than 10 individuals and no other disruptive impacts of any significance.

Table 6: Risk Assessment for Proposed Robodebt-Style Debt Recovery Program

1 Risk to human rights	Income-averaging may result in unequal and unjust outcomes for those with irregular income	Data matching does not comply with the relevant privacy-protecting Protocol	Personal information could be shared without adequate awareness of participants	Notifications from the program may not reach impacted individuals, resulting in penalties/ fines	Individuals impacted by the program may have inadequate avenues for complaint and appeal about impacts on their rights	The algorithm may not work as intended and produce arbitrary results	Payment obligations or fines may be incorrectly calculated	Vulnerable customers may not be resourced to engage with the program
2 Human Right	Equality, Property	Privacy	Privacy	Privacy, Property	Privacy, Equality, Fair Hearing[209]	Privacy, Equality, Property	Property	Equality
3a Likelihood	Almost certain	Likely	Likely	Likely	Likely	Likely	Possible	Possible
3b Severity	Severe	Moderate	Moderate	Moderate	Moderate	Severe	Severe	Major
3c Inherent Risk	Extreme	High	High	High	High	Extreme	Extreme	High
4. Control	Consider whether effective alternative approaches are available, or remove this feature.	Adjust processes for consistency with Protocol, especially regarding data retention and checking	Provide clear public explanation of use, notify participants and seek consent	Update contact details where possible, use multiple notification methods. Do not enforce where notification effectiveness unclear.	Create meaningful customer service, complaints and internal review channels	Undertake extensive prototyping and testing, including regular human testing/ auditing, offer manual reworking as part of internal review	Regular manual checking of a sample of all calculations to confirm process accuracy, offer manual reworking as part of internal review	Provide complex customer support for vulnerable customers, or exclude them from debt recovery.
5a Likelihood	?	Unlikely	Unlikely	Unlikely	Unlikely	Rare	Unlikely	Unlikely
5b Severity	?	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
5c. Residual Risk	?	Medium	Medium	Medium	Medium	Medium	Medium	Medium

209 Fair hearing principles under the human rights legislation might be engaged if affected individuals were parties to a civil proceeding, but are unlikely to be so engaged in this case because the processes are internal to government, not court processes. However, administrative law principles will be relevant.

Due to the size and scope of the program it would be difficult to mitigate residual risks to lower than 'medium', but the approach outlined in Table 6 would still have offered very significant practical improvements and mitigation measures. First, it would have obliged the project team to consider alternatives to income-averaging. It would also have prompted clear public information provision, consistency with the privacy Protocol, multiple methods to notify customers, accessible customer service, complaints and internal review channels including support for vulnerable customers, extensive algorithmic checking and regular manual checking and auditing of calculations, as well as an ability and willingness to retract demands as required. The residual (remaining) risks would include the possibility of miscalculation, failed notification and error, but in each case customers would have a review pathway.

The residual risks of limitations on human rights would then be subjected to step six (the Table 5 questions), to be assessed by specialist staff:

1. **Is there a clear legal basis for the use of the technology?** A legal basis can be identified for the program as whole (data matching and welfare enforcement), but not for the income-averaging approach, financial penalties, retrospectivity, reversed onus of proof or compulsive information demands. These elements would therefore need to be removed from the program, or supporting legislation passed, to avoid breaching human rights. Also, an administrative recovery proceeding must comply with applicable administrative law principles — while detailed consideration of those principles is beyond the scope of this article, specialist staff reviewing the program should turn their minds to them, such as by ensuring adequate channels for customers to seek internal review.

2. **Does the use of the technology have a proper purpose?** The overall goal of enforcement of eligibility and reduction of fraud in a welfare system is a proper purpose, including efforts to preserve public funds. But the driving purpose for Robodebt may have been achieving substantial and specific reductions in welfare entitlements for budget repair regardless of eligibility, arguably not a proper purpose.[210] If a clear and consistent proper purpose is not identified, the project would not pass this element of the test.

3. **Is there a rational connection between any potential limitation on human rights and that purpose?** Assuming a legitimate purpose, the next consideration is whether the limitations on the rights to privacy and

[210] *Robodebt Report* (n 1) 28–31. According to the Report, public servants were pressured to find substantial cost savings calculated without reference to any estimate of fraud or wrongdoing in the program: 'the estimated $1.2 billion in savings was not a number "that had come out of a methodology, but that the number itself was a goal of the process"': 28.

equality for welfare recipients and property rights are rationally connected to a program to reduce misuse of welfare funds. But this depends on the program being accurate: limitations on human rights due to inaccurate calculations would not be rationally connected to a legitimate purpose. Any inaccuracies would need to be addressed to satisfy this test.

4. **Is the limitation necessary to achieve the purpose (or is there an alternative approach which would be less restrictive)?** The inherent risks identified in Table 6 above were clearly too restrictive to human rights. However, the mitigation measures proposed in Table 6 (which are alternative approaches) are likely to significantly reduce these risks. Provided the program has a proper purpose, an amended program including these additional mitigation measures might reasonably be considered necessary to achieve that purpose.

5. **Does the limitation strike a fair balance between the proper purpose and human rights?** On the initial design, no. With the re-design proposed in Table 6 including accurate calculations plus a proper legal basis, it is arguable that a fair balance is struck, with numerous mitigation measures and checks and balances to ensure fairness.

It is likely that if such a process were undertaken with genuine intent and within a human rights culture, the issues that emerged with Robodebt and caused considerable harm and damage would have been identified and corrected or controlled, or the project abandoned. [211] Such an approach would have resulted in a different program design and additional review avenues and supports for vulnerable customers. A rights assessment such as the above is clearly likely to satisfy the procedural obligation, and go a long way to satisfying the substantive obligation. [212]

With the increasing adoption of novel data technologies, public servants need to become skilled at interrogating such proposed uses and improving them. A greater depth of questioning and deliberation would be prompted by an approach such as the one outlined above, within a positive human rights culture.

---

[211] See the comments of the President and Human Rights Commissioner of the ACT Human Rights Commission: 'I think that with a national Human Rights Act that Robodebt would have been prevented or at least remedied earlier': Watchirs (n 100) 28.

[212] Of course, such a result would require that legal and policy advice impacting human rights not be hidden from key decision-makers, as reported by the Robodebt Royal Commission: *Robodebt Report* (n 1) 106–7.

VI Conclusions

In this article I have considered Australian data protection legislation and concluded that it leaves a gap in protection in relation to novel data technologies. In Queensland, Victoria and the ACT, one way to plug that gap without law reform is to apply specific human rights legislation using a risk-based approach. This will be most effective where there is a human rights culture within the public service which is attuned to asking appropriate questions in the face of novel data technologies. The proposed approach may assist in mitigating weaknesses in the data protection legislation and further promoting and encouraging human rights cultures in the relevant public sectors, helping them mature. The rights assessment would ideally grow to encompass a genuine engagement with human rights risks, effective mitigation measures and structured proportionality, adding considerable value in an increasingly complex technological landscape.

The Commonwealth Robodebt program demonstrated a shocking lack of checks and balances. I illustrate above how a risk-based rights assessment of such a program could improve it and minimise its impact on human rights. As novel data technologies become more widespread, it becomes essential to increase the public service's sophistication in engaging with the impacts of such technologies. Within the relevant public sectors, applying risk-based approaches to novel data technologies under jurisdictional human rights laws may add a layer of technology-agnostic protection, pending (and even following) law reform to update data protection legislation.

APPENDIX

Table A1: Comparison of GDPR *Principles with Jurisdictional Laws and the Privacy Act Review Report (2022), with Areas of Concern Shaded Grey*

GDPR Principle[213]	*GDPR* Reference	Specific relevance to novel data technologies?[214]	Existing coverage under Qld, Vic, ACT data protection laws?	Coverage proposed under Privacy Act Review Report?[215]
Lawfulness, fairness and transparency	Art 5(1)(a)	-	Partial: covers collection only	Yes: recommends coverage of collection, use and disclosure.[216]
Purpose Limitation	Art 5(1)(b)	-	Yes	Yes: no change proposed
Data Minimisation	Art 5(1)(c)	-	Yes	Yes: no change proposed
Accuracy	Art 5(1)(d)	-	Yes	Yes: no change proposed
Storage Limitation	Art 5(1)(e)	-	Yes	Yes: no change proposed
Integrity and Confidentiality	Art 5(1)(f)	-	Yes	Yes: no change proposed
Accountability	Art 5(2)	-	Partial: accountability may be implied rather than directly addressed.	Yes: recommends increased accountability.[217]
Protection of children	Art 8	-	No	Yes: recommends additional

213 Note that there are a range of law enforcement exceptions to the *GDPR* principles: *GDPR* (n 7) art 23.

214 All the principles have relevance to novel data technologies, but this column attempts to identify those principles which have *specific relevance* in respect of these technologies, by offering protections targeted to the risks they pose.

215 Attorney-General's Department, *Privacy Act Review Report* (n 66). In each of the references to proposals from this report I indicate whether the proposal has been accepted by government in full ('agreed'), is subject to further consultation and an impact analysis ('agreed in principle') or merely 'noted': Attorney-General's Department, 'Fact Sheet: Government Response to the Privacy Act Review Report' (n 67) 2.

216 Attorney-General's Department, *Privacy Act Review Report* (n 66). Agreed in principle: Attorney-General's Department, *Government Response — Privacy Act Review Report* (n 71) 27.

217 Attorney-General's Department, *Privacy Act Review Report* (n 66) 10. Agreed in principle: Attorney-General's Department, *Government Response — Privacy Act Review Report* (n 71) 29.

GDPR Principle[213]	*GDPR* Reference	Specific relevance to novel data technologies?[214]	Existing coverage under Qld, Vic, ACT data protection laws?	Coverage proposed under Privacy Act Review Report?[215]
				protections for children.[218]
Sensitive Data	Art 9	-	Yes	Yes: no change proposed
Provision of information	Art 13	-	Partial: lack of detail regarding contents of collection notices	Yes: recommends more detailed collection notice requirements.[219]
Right of access and rectification	Art 15, 16	-	Yes	Yes: no change proposed
Right of erasure	Art 17	-	No	Yes: recommends a right of erasure.[220]
Right to restrict processing	Art 18	Yes	No	No
Right to data portability	Art 20	-	No	No: notes consumer data rights (re banking and other industries) may assist.[221]
Right to object to processing	Art 21	Yes	No	Yes: recommends a right to object.[222]
Automated decision making / profiling	Art 22	Yes	No	Yes: recommends transparency re automated decisions.[223]

218 Attorney-General's Department, *Privacy Act Review Report* (n 66) 10. Combination of 'agreed' and 'agreed in principle': Attorney-General's Department, *Government Response — Privacy Act Review Report* (n 71) 29–30.

219 Attorney-General's Department, *Privacy Act Review Report* (n 66) 8. Agreed in principle: Attorney-General's Department, *Government Response — Privacy Act Review Report* (n 71) 26.

220 Attorney-General's Department, *Privacy Act Review Report* (n 66) 11. Agreed in principle: Attorney-General's Department, *Government Response — Privacy Act Review Report* (n 71) 31.

221 Attorney-General's Department, *Privacy Act Review Report* (n 66) 166.

222 Ibid 11. Agreed in principle: Attorney-General's Department, *Government Response — Privacy Act Review Report* (n 71) 30.

223 Attorney-General's Department, *Privacy Act Review Report* (n 66) 12. Agreed: Attorney-General's Department, *Government Response — Privacy Act Review Report* (n 71) 32.

GDPR Principle[213]	*GDPR* Reference	Specific relevance to novel data technologies?[214]	Existing coverage under Qld, Vic, ACT data protection laws?	Coverage proposed under Privacy Act Review Report?[215]
Data protection by design and default	Art 25	Yes	No	No: notes that this is implied.[224]
Obligations around de-identified information	Art 25	Yes	No	Yes: recommends extending protections to de-identified datasets.[225]
Mandatory impact assessments	Art 35	Yes	No: impact assessments are recommended but not mandatory	Yes: recommends mandatory impact assessments for any 'high privacy risk activity'.[226]

Victorian Public Sector Commission Raw Data 2008–22:

Table A2: Victorian Public Sector Survey, Whole Victorian Public Sector

Question: 'I understand how the Charter of Human Rights and Responsibilities applies to my work'

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
2008	19.94%	55.68%	11.02%	11.10%	2.26%
2009	22.81%	56.77%	10.25%	8.72%	1.45%
2010	21.75%	58.35%	9.44%	8.82%	1.64%
2011	20.56%	59.19%	8.81%	9.60%	1.84%
2012	22.51%	59.28%	8.07%	8.36%	1.60%

224 Attorney-General's Department, *Privacy Act Review Report* (n 66) 145.

225 Ibid 5. Government agreed to consult on a criminal offence for malicious re-identification (proposal 4.7) and agreed in principle to amend and extend the definition of 'de-identified' (proposal 4.5), with proposals 4.6 and 4.8 noted only: Attorney-General's Department, *Government Response — Privacy Act Review Report* (n 71) 21–2.

226 Attorney-General's Department, *Privacy Act Review Report* (n 66) 9. Agreed in principle: Attorney-General's Department, *Government Response — Privacy Act Review Report* (n 71) 28.

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
2013	25.58%	53.08%	12.63%	7.30%	1.24%
2014	25.73%	53.32%	13.32%	6.51%	1.09%
2015	23.78%	55.21%	12.63%	7.10%	1.24%
2016	15.53%	44.62%	23.83%	12.06%	3.94%
2017	16.20%	44.98%	23.71%	11.64%	3.47%
2018	22.48%	53.70%	16.15%	5.71%	1.96%
2019	21.98%	52.93%	16.61%	6.53%	1.94%
2021	24.70%	51.52%	16.13%	5.79%	1.85%
2022	25.38%	52.58%	15.31%	5.19%	1.55%