Australian Human Rights Commission

Safeguarding the right to privacy in Australia

Australian Human Rights Commission

Submission to Attorney-General's Department Privacy Act Review Report 2022

05 April 2023

ABN 47 996 232 602
Level 3, 175 Pitt Street, Sydney NSW 2000
GPO Box 5218, Sydney NSW 2001
General enquiries 1300 369 711
Complaints info line 1300 656 419
TTY 1800 620 241

Australian Human Rights Commission
www.humanrights.gov.au

Contents

1 Introduction

1. The Australian Human Rights Commission (Commission) welcomes the opportunity to make this submission to the Attorney-General's Department on the *Privacy Act 1988* (Cth) (Act) in response to the Privacy Act Review Report 2022 (Review Report).
2. The role of the Commission is to work towards an Australia in which human rights are respected, protected and promoted. In respect of the Review Report, the Commission has taken a targeted approach to this submission, reflecting the Commission's relevant expertise in certain areas, and current capacity.
3. While the Commission has expertise and knowledge in the area of human rights generally, it has also developed specific expertise with respect to the human rights risks posed by new and emerging technologies. Most recently, this can be seen in the Human Rights and Technology Project, which was a three-year, national investigation that culminated in the release of the Human Rights and Technology Project Final Report in 2021 (Final Report).
4. This submission builds on the previous work that the Commission has done to advocate for human rights-centred design and deployment of new and emerging technologies, and demonstrates a commitment to leadership in respect of human rights in digital spaces.
5. The Commission has previously submitted a child rights-specific submission to the Attorney-General's Department on the Privacy Legislation Amendment (Enhancing Online Privacy Measures) Bill 2021, preceding the Review Report. This submission predominantly focused on issues of privacy relating to children. Reiterating the importance of children's rights, the issues raised in that submission have informed proposals 16.1 to 16.5 of this submission to the Review Report.
6. The Commission has continued its work in 2023 on human rights and technology. This submission is in addition to other 2023 submissions to date, including to the:
    - Select Committee on Foreign Interference through Social Media
    - Targeted Review of Divisions 270-271 of the *Criminal Code Act 1995* (Cth) (in respect of technology facilitated crime)
    - Australian Competition and Consumer Commission's 'Digital Platform Services Inquiry – September 2023 Report on the expanding ecosystems of digital platform service providers issue paper' (pending).

7. The Commission welcomes further opportunities to provide input, and consult with the Attorney-General's Department, in respect of reforming the Act.
8. The Commission has made 36 recommendations to the Review Report, which have all been collated at the end of this submission.

2 Proposal 3.1

Amend the objects of the Act to clarify that the Act is about the protection of personal information

9. The Commission agrees with Proposal 3.1, as clarifying the role of the Act in protecting personal information is a necessary reform.

Recommendation 1: Amend the objects of the Act to clarify that the Act is about the protection of personal information.

10. However, this reform alone is insufficient in strengthening the focus on the protection of the rights of Australians. The Privacy Act Review Discussion Paper[1] (Discussion Paper) and Review Report,[2] indicate that including a positive right to privacy in the objects of the Act is superfluous to reform which aspires to place 'greater weight to the protection of individuals' privacy'.[3]
11. The Review Report discusses the right to privacy as an object in the Act,[4] but does not put this forward as a proposed reform. The Discussion Paper states that a right to privacy should not be included in s 2A of the Act as 'It is not appropriate for the objects to refer to a 'right to privacy' because, despite common parlance, Art 17 does not confer such a right, nor does it amount to absolute protection.'[5]
12. A refusal to acknowledge the right to privacy in the objects of the Act is inconsistent with not only a best practice adherence to Australia's international obligations under the *International Covenant on Civil and Political Rights* (ICCPR), but also at odds with a genuine attempt by these reforms to place 'greater weight on the protection of individuals' privacy'.[6]
13. To best protect individuals' privacy, recognising a positive and predominant right to privacy in the objects of the Act is necessary to ensure that judicial consideration of the Act is predicated on upholding the human right to privacy. The Commission strongly supports submissions which have previously called for the objects of the Act to recognise a positive right to privacy.[7]

14. The right to privacy is a human right under article 17 of the ICCPR, as well as being enshrined in a number of other applicable international human rights instruments.[8] Although the right to privacy is not an absolute right, and is one which is derogable[9] under the ICCPR, this does not mean it should be excluded in the objects of the Act– especially when the right to privacy is not fully protected in Australian law.[10]

2.1 Privacy in the 21st century

15. The right to privacy is a cornerstone human right. As noted by the Office of the Australian Information Commissioner (OAIC), it also underpins freedoms of association, thought and expression, as well as freedom from discrimination.[11]

16. The right to privacy developed over centuries. For example, in the fourth century B.C.E Aristotle drew the distinction between the public sphere of politics and the private sphere of domestic life. Thousands of years later, the 'fourth industrial revolution' is characterised by rapid technological development. These changes have arguably reinforced the central importance of the right to privacy.

17. The rapid pace of technological advancement has, in part, been paid for by the harvesting of individuals' personal data.[12] This is especially so for technologies or applications which are free to use – as the saying goes; 'if you aren't paying for the product, you are the product'.

18. In an age where digital participation is essential to modern living, users are being given an illusion of choice – agree to have data collected and used or be excluded from participating in everyday living. The Commission does not accept that digital participation should come at the expense of privacy.

19. Vint Cerf, Vice President and Chief Internet Evangelist at Google, once stated that 'privacy may actually be an anomaly'.[13] The recognised challenges to privacy protection are magnified in light of expanding interoperability, data sharing and new and emerging technologies.

20. This alarming statement which at first glance may seem hyperbolic or exaggerated. However, there is concern that the continued disintegration of the right to privacy, risks seeing this statement come to fruition.

2.2 A Human Rights Act for Australia

21. The Review Report refers to the Commission's Free and Equal: An Australian conversation on human right project.[14] Since then, the Commission launched its Position Paper: A Human Rights Act for Australia (Position Paper) on 9 March. In the Position Paper the Commission specifically recommends the

inclusion of a 'right to privacy and reputation' in the proposed Australian Human Rights Act.[15]

22. The inclusion of a positive duty to act in compliance with human rights (such as the right to privacy and reputation) in the proposed model for an Australian Human Rights Act demonstrates the importance of the right to privacy in the digital age – especially in relation to the collection and use of personal data.

23. The Commission's model includes a legislative obligation for public authorities to act compatibly with the human rights expressed in the Human Rights Act (such as the right to privacy and reputation) and consider human rights when making decisions.[16] This is known as a 'positive duty' and compliance with it would be judicially reviewable.

24. The positive duty builds upon the understanding of human rights over more than 10 years of engagement in the parliamentary scrutiny process involving statements of compatibility and review by the Parliamentary Joint Committee on Human Rights (PJCHR).[17]

25. The requirement to give 'proper consideration' to human rights applies to making decisions and implementing legislation and policy – it is a procedural obligation. The requirement to 'act compatibly' with human rights is a substantive obligation on public authorities. Under the proposed Human Rights Act, public authorities would also be required to engage in participation processes where the 'participation duty' is relevant, as part of the 'proper consideration' limb. Compliance with the positive duty would be reviewable by courts (and possibly by tribunals). The positive duty would require decision makers to consider human rights at an early stage, helping to prevent breaches from occurring.[18] Further details can be found in the Commission's Position Paper.

26. The Position Paper proposes the inclusion of an interpretive clause in the Human Rights Act stating that courts are to prefer an interpretation that is compatible with human rights, provided that this is consistent with the intention of Parliament, as expressed through the statute under analysis.[19] This approach is consistent with, and builds on, the 'principle of legality', a common law principle of statutory interpretation that presumes Parliament 'does not intend to interfere with common law rights and freedoms except by clear and unequivocal language'.[20] These approaches to interpretation reinforce the significance of including the right to privacy in the objectives of the Act as a clear indication of the intention of Parliament.

27. The proposed right to privacy and reputation outlined in the Human Rights Act states:

> *A person has the right-*

> *(a) not to have the person's privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and*
>
> *(b) not to have the person's reputation unlawfully attacked.*
>
> *Note: The right to privacy applies to the collection, processing or retention of personal data through all forms of technology, and includes state surveillance measures*.[21]

28. This proposed right to privacy and reputation implements art 17 of the ICCPR (to which Australia has signed and ratified). The proposed right is also worded closely on s 13 *Victorian Charter of Human Rights and Responsibilities Act 2006* (Vic), s 25 *Human Rights Act 2019* (Qld) and s 12 *Human Rights Act 2004* (ACT).[22]
29. Pertinently the note clarifies that privacy rights extend to technological surveillance measures, noting the increased capacity of the state collect personal data and make decisions based on that data through artificial intelligence (AI).[23]
30. The inclusion of a right to privacy in the proposed Human Rights Act is especially relevant given PJCHR findings. The PJCHR's annual report sets out the most commonly listed rights engaged by the legislation which the PJCHR examined and substantively commented on during the year. The 2020 annual report evidenced the right to privacy as the most commonly engaged with right at 28%.[24] This was also true in 2021.[25] However, as far back as 2016 the right to privacy has been one of the most commonly engaged rights each year.[26]
31. Protecting the right to privacy is increasingly important as the rapid pace of change in digital spaces elevates the risk of this right being increasingly overlooked when introducing legislation. For example, the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) was passed in 2015 – despite concerns in respect of privacy.[27] Since then, further surveillance measures have been introduced, vastly expanding executive power and limiting the right to privacy for Australians.[28]
32. Subsequent reviews of metadata retention and surveillance laws by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and the Independent National Security Legislation Monitor (INSLM) have recommended the mitigation or removal of overreaching surveillance powers. However, these recommendations are too often not implemented.[29]
33. The Commission's proposed model for a federal Human Rights Act is one way to anchor the promotion and protection of human rights in Australia. Action is also needed across all areas of law reform to ensure compliance with Australia's international human rights obligations and to reflect our commitment to fundamental human rights.

34. Without the right to privacy being included as the paramount object in s 2A of the Act, the Commission is concerned that the Act does not fully reflect Australia's commitment to this foundational human right, nor the importance of protecting this right in the 21st century.

Recommendation 2: The human right to privacy must be included as the paramount object in s 2A of the Act.

3 Proposal 4.10

Proposal 4.10 Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent. Define 'geolocation tracking data' as personal information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time.

3.1 Recognising the sensitivity of location tracking data

35. With nearly nine out of ten Australians owning a mobile phone,[30] concerns about the way location tracking data is used are increasing. Location tracking data can be collected by the user's proximity to cell phone towers, or through websites and apps.
36. Location tracking data has the potential to be misused in a way that reveals other sensitive information about individuals to third parties without their knowledge or consent.
37. The Consumer Views and Behaviours on Digital Platforms Final Report, prepared for the Australian Competition and Consumer Commission (ACCC) in 2018, revealed that 86% of survey respondents considered that monitoring of offline location and movement without consent was a misuse of personal information.[31]
38. Geolocation tracking data is currently categorised as 'personal information'. In the Commission's view, this does not fully recognise the sensitivity of this data and the significant privacy harms that can result from its misuse. This data should be designated as 'sensitive information', which is subject to more stringent requirements for its use and disclosure.[32]
39. Sensitive information is defined in the Act as including information or an opinion about a range of personal opinions, beliefs or affiliations.[33]

40. As geolocation tracking data allows inferences to be made about a person that would constitute sensitive information under the current definition, the Commission recommends that it be categorised as sensitive information.

41. The misuse of geolocation tracking data may provide the basis for unjustified discrimination and risk the safety of individuals.

42. For example, the potential for misuse of location data was highlighted by the publication of a report by consumer insight firm Mobilewalla in 2020 that used phone location data secretly collected during the Black Lives Matters protests. The firm buys mobile phone data and, at the time the article was published, had 80–90% device coverage in the United States.[34] The report published age, gender, ethnicity and location of attendees at Black Lives Matter protests in 2020.[35] The report is no longer available online.

43. There are also reports that the same company was able to use geolocation tracking data to determine how frequently people attended evangelical churches in the leadup to the American election.[36] The firm then used that data to tell people it classed as 'evangelicals' to vote, if their phone hadn't been seen near a polling place on election day.[37]

44. The use of individuals' data in this way without consent is concerning. The examples above highlight the need for voluntary and informed consent in relation to geolocation tracking data. The examples also illustrate the need for geolocation tracking data to be classified as sensitive information. The inferences drawn from geolocation data are clearly capable of meeting the definition of sensitive information in the Act.[38]

Recommendation 3: 'Geolocation tracking data' should be defined as sensitive information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time.

4 Proposal 10.1

Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable. Appropriate accessibility measures should also be in place.

45. Collection notices are often couched in language which make them difficult, if not impossible, for lay people to understand. This makes it incredibly challenging for individuals to appreciate what personal information is being collected, and how it may be used. This is supported by the ACCC's Digital

Platforms Inquiry – Final Report, which highlighted how lengthy and complex documents were exacerbating issues surrounding transparency in collection notices.[39]

46. Although many organisations may attempt to provide clear and easy-to-understand collection notices, a Deloitte survey indicated that 40% of brands still provided vague information about how data would be used in collection notices.[40] Poor collection notices not only affect many human rights, but also consumer trust in the organisations which operate in digital environments. The same survey stated that 70% of consumers previously indicated that they have greater trust in brands with transparent and clear privacy notices.[41]
47. Research has also shown the emergence of 'dark patterns' which confirms that the use of manipulative and deceptive designs can cause significant consumer harm.[42] This can lead to individuals losing control of their data or being manipulated into making choices which are not in their interests.[43]
48. Where individuals are unable to ascertain what data is being collected, for what purposes, and how it may be stored, transferred or shared, it enables organisations to evade accountability – meaning organisations can utilise information that an individual would not ordinarily have agreed to share. This may contribute to violations of the human right to privacy more broadly, but depending on the circumstances, can also have broader impacts on several human rights. The issue of how personal data can be misused to facilitate human rights abuses is canvassed throughout this submission. Having clear, up-to-date, concise and understandable collection notices is a strong step in protecting against the misuse of information.
49. Proposal 10.1 will allow individuals to regain some control of their digital lives in an era where it is very difficult to live without interacting in online spaces. Better informed individuals will have greater understanding of their rights and hopefully lead to informed decisions about their data in high-risk settings. The Commission supports Proposal 10.1.

Recommendation 4: Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable. Appropriate accessibility measures should also be in place.

50. The Commission also supports clarity of language in respect of using the term 'up-to-date' in lieu of 'current'. However, OAIC guidance on the meaning of 'up-to-date' may further assist entities in better understanding any deadlines such language places upon them.

Recommendation 5: The OAIC provides guidance on the meaning to 'up-to-date' in respect of Proposal 10.1.

4.1 Onus on individuals

51. Proposal 10.1 operates on a model which places the onus on individuals to be responsible for the protection of their data, and to make informed decisions. However, the Commission has reservations about this approach more generally.
52. Although collection notices may be improved in line with Proposal 10.1 (in addition to other reforms recommended in relation to privacy notices), the Commission questions what practical effect this will have on individuals' actual behaviour. While they may improve transparency, it is possible that such reforms will, in practice, be insufficient in providing individuals with the ability to better protect their data.
53. The Commission's concern is predicated upon several matters:
    - the 'privacy paradox'
    - lack of competition/alternatives which are more data secure
    - the illusion of choice
    - power imbalances.
54. The 'privacy paradox' refers to the phenomenon that, despite understanding the privacy risks of a product or service, there is no obvious influence upon an individual's behaviour.[44] Namely, individuals will still engage with privacy-adverse products and services even where they are highly aware of the risks. This does not mean that individuals do not care about their privacy. For example, 74% of individuals have safety concerns in relation to being targeted by products or services.[45] A further 76% consider it is unfair when personal information is to make predictions about them, while a further 85% consider it is unfair or very unfair for their personal information to be shared with other companies.[46]
55. Furthermore, even where individuals do not genuinely understand how their data is being used, people will still disapprove of its misuse. Individuals have been shown to have a very strong negative reaction when confronted with the difference between:
    - how their data is actually being used
    - versus their perception of how it is being used.[47]

56. This is particularly the case where the difference becomes explicit and too contrasting.[48] The Cambridge Analytica Data Scandal provides an apt example. Many consumers willingly shared data on Facebook, however when the use of that data by Cambridge Analytica came to light there was public outcry, with Facebook being required to appear at hearings before both the US congress and UK Parliament.[49]

57. Despite being aware of the risks, and disapproving of those risks to privacy, individuals are often unwilling, or unable, to stop using appliances or services which threaten their privacy.[50]

58. This reluctance, or inability, to avoid products or services which threaten privacy may be partly in response to a lack of effective competition or alternative. The ACCC has previously found that a lack of competition and unavailability of reasonable alternatives (which may better protect privacy) can lead consumers to accept undesirable terms of use.[51] In addition, terms of use may be provided on a 'take-it-or-leave-it' basis across interrelated services which potentially leads to excessive data collection inconsistent with the wishes of the individual consumer.[52] While it is helpful to have understandable collection notices (and privacy policies), as increasing transparency is an important goal in itself, the overall benefit to the individual in terms of protecting privacy will be severely limited if all services and products require access to the same amounts of intrusive personal data.

59. This affords individuals very little ability to 'choose' services and products which enable modern living without risking their privacy. The illusion of choice in respect of privacy is not addressed by the reforms proposed in respect of collection notices (as set out in Proposal 10.1) or privacy policies more broadly. This model of regulation places great emphasis on informed 'choice' as an effective safeguard for data and privacy.[53] While Proposal 10.1 does ensure that individuals are 'informed' it does little to enable any choice in how they can engage in modern living without signing away their data. The privacy paradox and numerous behavioural studies demonstrate that placing the onus on individuals to protect their own data is insufficient.[54]

60. Such a model also does not acknowledge the substantial power difference between large companies and individual consumers. Even where an individual understands how their data will be used, this power imbalance remains, as 'one party controls the design of applications and the other must operate within that design'.[55]

61. The privacy paradox, illusion of choice and power imbalances may all contribute to individuals being unable to engage in modern living without relinquishing their privacy. Although improved transparency in collection notices and privacy policies is a good first step, the Commission would encourage the Attorney-General's Department to consider alternative models

which do not place the onus on individuals to protect their data. By way of example only, the Commission is aware that the Consumer Policy Research Centre Working Paper, 'In whose interest? Why businesses need to keep consumers safe and treat their data with care', considers alternative models which might be useful to consider.

5 Proposal 11.1

Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.

62. The Commission agrees with Proposal 11.1.

Recommendation 6: The definition of consent be amended to provide that it must be voluntary, informed, current, specific, and unambiguous.

63. Although Proposal 11.1 largely codifies OAIC guidance,[56] in light of this proposed amendment to the Act it would also be beneficial to strengthen existing OAIC guidance to ensure that it fully reflects the National Decision-making Principles from the 2014 Australian Law Reform Commission (ALRC) Report *'Equality, Capacity and Disability in Commonwealth Laws'* (ALRC Report 124), namely that:

- All adults have an equal right to make decisions that affect their lives and to have those decisions respected.
- Persons who require support in decision-making must be provided with access to the support necessary for them to make, communicate and participate in decisions that affect their lives.
- The will, preferences and rights of persons who may require decision-making support must direct decisions that affect their lives.
- Laws and legal frameworks must contain appropriate and effective safeguards in relation to interventions for persons who may require decision-making support, including to prevent abuse and undue influence.[57]

64. Consent, as a decision, falls within these decision-making principles.

Recommendation 7: OAIC guidance should be strengthened to fully incorporate the ALRC Report 124 national decision-making principles.

6 Proposal 13.2

Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities. This work should be done as part of a broader consideration by government of the regulation of biometric technologies.

65. Facial recognition technology (FRT) can be used in simple ways, such as to unlock a phone. However, it can also be used in policing or decisions which have a legal or similarly significant effect on an individual. The Commission made various recommendations with respect to the use of FRT in the Final Report[58] and, building upon those recommendations, encourages more thorough risk assessment requirements in respect of FRT and the use of biometric information.
66. Proposal 13.2 provides that 'This work should be done as part of a broader consideration by government of the regulation of biometric technologies'. The Commission is pleased that government is conscious of the need for regulation of FRT - which collects and utilises biometric data. The use of AI in conjunction with FRT and biometric information has prompted growing concerns, amongst both experts and the general public.[59]

6.1 Facial recognition technologies

67. New and emerging technologies often bring with them a range of ethical issues as society grapples with how best to harness the prospective benefits of new technology, while mitigating the potential harms. This is especially true of FRT, which has had persistent problems with accuracy and fairness in its use – particularly in respect of racial and gender bias. These concerns have led to the technology being banned in some places, and yet it continues to be commonplace in others.[60]
68. FRT is being adopted by government and businesses in Australia at an exponential rate.[61] These tools are also increasingly being used in workplaces, schools, shopping centres and residential areas to identify members of the public and monitor behaviour.[62]
69. As the technology has become increasingly mainstream, so too have the voices raising ethical concerns and calling for greater regulation.[63] All new and

emerging technologies need to be used in a responsible and ethical way, and need a code of ethics and regulation to mitigate any harms.[64] Although this submission focuses on legislative responses to FRT, the Commission encourages greater discussion of the limitations of FRT and how developers can better manage those limitations to increase equity and fairness.[65] Regulation and legislation are only one strategy to handling risk, and not the answer to fundamental issues in the technology itself.

Recommendation 8: A parliamentary inquiry into the risks of facial recognition technologies be commenced with terms of reference which, among other things, specifically considers the human rights risks of the technologies.

4.1.1 The duality of facial recognition technology

70. Handling the risks of FRT requires a prudent approach, as the potential benefits of the technology must be measured against its potential harms. While the technology has the potential to improve public services and law enforcement (i.e. traffic congestion, pollution controls and public security), it can also be used for mass surveillance, ethnic profiling, targeted repression and privacy violations.[66]
71. As of 2019, at least 64 countries were identified as actively using some type of FRT scheme for surveillance purposes.[67] FRT is an attractive investment for many aspects of private and public organisations, as it decreases the time, effort and money needed to identify faces and tie those faces to other information (such as other pieces of personal data about an individual).[68] However, organisations and government must be cautious when considering the use of FRT and the risks that attach to this.
72. India's use of FRT is just one example of the duality that is inherent within this technology. In 2018 Delhi police used FRT to reunite nearly 3,000 children with their parents in just four days.[69] This pilot FRT programme had later reunited 10,561 missing children with their families after only 15 months in operation.[70] The profoundly positive impact this technology can have is astounding, as it can identify and match faces using one-to-many technology faster than any human is capable of. This program is one example of the potential of FRT to be used in ways that enhances human rights.[71]
73. However, there have also been criticisms of the Indian government using this same FRT technology in 2020 to facilitate the arrest of protesters of a citizenship law which critics contend marginalises Muslims.[72]

74. Examples of 'function creep', where FRT is applied beyond the initially intended purpose, can be found globally – most notably when it is used against marginalised populations,[73] such as the Muslim Uyghur minorities in China's Xinjiang Uyghur Autonomous Region.[74] The 2022 report by the Office of the United Nations High Commissioner for Human Rights that focused on human rights concerns in this region described 'an ever-present network of surveillance cameras, including deploying facial recognition capabilities' as one element of 'what has been alleged to be a sophisticated, large-scale and systematized surveillance system in practice.'[75]

75. 'Function creep' can have potentially devastating impacts for human rights. Specific regulation targeting FRT is essential to protect human rights.

76. It is likely due to the duality of FRT, which is largely unregulated, that individuals globally vary on their acceptance of the technology. For example, an online survey conducted across four countries in 2019 found that while 51% of Chinese respondents were strongly or somewhat accepting of FRT for public use, this dropped to only 37% of Americans and 38% of Germans.[76]

77. Acceptance rates of FRT may be positively influenced by factors such as:

    - trust in the government
    - concerns about specific risks, such as terrorism
    - high levels of technological affinity in a population.[77]

78. Conversely, awareness of a country's adverse use of surveillance methods in the past (and concerns in respect of privacy violations) foster a more apprehensive attitude towards FRT in public settings.[78]

79. Domestically, individuals are also concerned about the use of FRT. In a nationally representative survey, CHOICE asked respondents about the use of FRT in retail stores. 65% of respondents were concerned about stores using technology to create customer profiles which could cause them harm, while a further 78% expressed concern about the secure storage of faceprint data.[79]

80. A subsequent investigation into retailers using FRT led to the OAIC launching an investigation into both Kmart and Bunnings' use of FRT,[80] while the Good Guys chain has paused its use of FRT in stores while the OAIC investigates a complaint made by CHOICE.[81]

81. Without FRT-specific regulation, such as that proposed by the University of Technology Sydney's Model Law (Model Law),[82] it is difficult to imagine circumstances where individuals will be trusting of FRT to the point that all of its benefits can be appreciated without posing a disproportionate risk to human rights. There are undoubtedly benefits to the technology, as highlighted above with the example from India, but regulation is needed to harness these advantages in a human rights' compliant manner.

82. While it is generally undesirable to regulate a specific technology, there are exceptions to this general principle. For example, as was highlighted in the Final Report, governments have a tendency to regulate technology deemed high-risk, which helps to explain the comparatively strict laws which govern fields such as gene technology, aviation, healthcare and the energy industry.[83] It is in these areas that regulation is often applied to both the technologies themselves as well as their use. In relation to FRT, the greater the risk to human rights, the greater the need for regulation.

83. In respect of the Review Report's proposal for 'consideration by government of the regulation of biometric technologies' the Commission recommendations the following to ensure FRT is regulated to engender trust and minimise risk.

Recommendation 9: Federal, State and Territory governments should introduce legislation which specifically regulates the use of facial recognition and other biometric technologies. Such legislation should:

- **expressly protect human rights**
- **apply to the use of this technology in decision making that has a legal, or similarly significant, effect for individuals, or where there is a high risk to human rights, such as in policing and law enforcement**
- **be developed through in-depth consultation with the community, industry and expert bodies such as the Australian Human Rights Commission and the Office of the Australian Information Commissioner.**

84. The Commission provides in-principle support for the Model Law on FRT.[84] This includes the provision that FRT developers and deployers must complete a Facial Recognition Impact Assessment of the potential harms, including the potential human rights risk. This Facial Recognition Impact Assessment would be registered, publicly available and could be challenged by the regulator or interested parties.

85. The Model Law provides a significant reference point when considering how to enhance risk assessments in respect of FRT as set out in Proposal 13.2. It offers a viable framework for the regulation of FRT and ensuring human-rights-compliant impact assessments, especially in high-risk settings.

Recommendation 10: The Model Law be implemented by government, with in-depth consultations with the community, industry and expert bodies such as the Australian Human Rights Commission and the Office of the Australian Information Commissioner being held to assist before any legislation is finalised.

4.1.2 The human rights harms of facial recognition technology

86. The length of time it will necessarily take to implement FRT regulation and impact assessments means that there is a continuing risk of significant human rights harms being facilitated by FRT in both public and private spheres.

87. One example has been highlighted by the work of Dr Michal Kosinski, Associate Professor of Organizational Behaviour at Stanford University. In 2018, Kosinski and Yilun Wang published research claiming that computer-vision algorithms could predict sexuality from a single image of a person's face.[85] Kosinski published further research in 2021 claiming that computer-vision algorithms could equally predict political orientation from a single image of a person's face.[86] Either claim is troubling from a human rights perspective – regardless of whether the technology is as efficient as claimed (see below at [89]).

88. The 2020 update of the Global Legislation Overview of the State-Sponsored Homophobia Report concluded that there were 67 Member States with provisions criminalising consensual same-sex conduct, and six UN Member States that continue to impose the death penalty for consensual same-sex conduct.[87] This is in addition to the many countries where individuals continue to face persecution and violence on a daily basis because of their sexual orientation or gender identity.

89. If the FRT is accurate (Kosinski claims the technology is accurate 81% of the time for men and 74% for women),[88] this technology could provide regimes, which punish homosexuality, with the widespread ability to identify, isolate and even kill people based on an assessment of their sexual orientation made by FRT – facilitating an uncomfortable level of efficiency in human rights abuses.

90. However, Kosinski's work has been openly criticised as being inaccurate and unreliable.[89] Unfortunately, the inaccuracy of FRT tools does not necessarily reduce the risk of persecution and violence against individuals who might be targeted by this technology – whether on the basis of sexual orientation or other characteristics. If this technology is perceived to be accurate by regimes which punish homosexuality, it may still be adopted. This will result in harms

to both individuals correctly identified as being homosexual, as well as those who are incorrectly identified as homosexual.

91. Although an extreme example, the movement to develop these kinds of FRT capabilities may usher in an era of human rights discrimination and abuse facilitated by technology. FRT may exacerbate systematic discrimination on a variety of fronts, as people of colour, transgender and non-binary people are often being subject to disproportionate levels of tracking, judging and inaccurate results.[90]

92. More broadly, the Commission's Final Report highlighted concerns expressed around three particular risks:

    - the contribution of FRT to the growth in surveillance
    - the use of data derived from FRT to engage in profiling
    - the risk that errors connected to facial recognition disproportionately affect certain groups.[91]

93. This is in addition to the use of FRT in the private sector which 'raises distinct concerns as there may be a lower degree of accountability and fewer legal protections'.[92]

94. In respect of the growing use of FRT-enabled surveillance, the Commission found that this would lead to an inevitable reduction of personal privacy, and that the threat of closer security by police and government agencies can impede participation in lawful democratic processes – such as protests and meetings.[93] This raises the risk profile in protecting the rights to:

    - freedom of association and assembly
    - freedom of expression and opinion
    - freedom from unlawful and arbitrary arrest.[94]

95. Moreover, the Commission has previously raised concerns about the gathering of seemingly small and innocuous pieces of personal data (including facial data) which can, accumulatively, provide a detailed profile of an individual – dubbed the 'mosaic effect'.[95]

96. With the inclusion of additional biometric and non-biometric information, this can allow sensitive personal information to be extracted or inferred about a person, including their age, race, sex and health.[96]

97. Such information and inferences can be used in 'profiling' – where intrusive action is taken by reference to people's characteristics. An example of this kind of profiling, which may result in people of a particular racial or ethnic group being disproportionately subjected to police identity checks, has been highlighted by Human Rights Watch in the report, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App,* which

provided a detailed analysis of the technology used for mass surveillance in Xinjiang, including the aggregation of data.[97]

98. The above risks are further exacerbated by the potential for errors in the technology, as risks are at their highest where this technology is used in decision making that affects an individual's legal or similarly significant rights. This is most obvious when the technology fails.

99. For example, if an error in FRT on a smartphone causes a delay in an individual 'unlocking' their device, generally this would present little more than an annoyance. However, if a person is wrongly accused of a crime on the basis of an error in police use of FRT, the risk of harm is far greater. There have been examples reported where individuals have been falsely arrested and imprisoned due to FRT.[98]

100. Generally speaking, FRT is far from perfect and is often criticised as being less accurate when identifying women, or people from minority racial groups, as compared with other people.[99] Amazon, Microsoft and IBM have all previously announced they would stop, or pause, offering this technology to law enforcement.[100]

101. However as there is currently no legislation regulating FRT, nor a moratorium in place in the interim, others have continued to facilitate the use of FRT by government agencies and police forces globally.

102. An example of the risks that this poses for human rights can be seen in the illustrative example of the activities of Clearview AI, who scraped approximately 3 billion images of faces from publicly accessible sources (such as Facebook and Google) to create a database. The company then licensed this database to over 600 hundred law enforcement agencies (in addition to banks, private companies and schools).[101] Reports have shown that employees at law enforcement agencies in the US were running thousands of Clearview AI facial recognition searches – often without the public's knowledge or consent.[102]

103. Clearview AI's wrongful conduct has since been investigated. A determination was made by the OAIC that Cleaview AI breached Australians' privacy by scraping their biometric information from the web and disclosing it through a facial recognition tool.[103] This was preceded by a joint investigation between the OAIC and UK Information Commissioner's Office.[104]

104. Although domestic legislation on FRT and a moratorium would not entirely have prevented all of Clearview AI's activities, the Australian Information Commissioner and Privacy Commissioner, Angelene Falk, has stated that the case of Clearview AI 'reinforces the need to strengthen protection through the current review of the Privacy Act, including restricting

or prohibiting practices such as data scraping personal information from online platforms'.[105]

105. While regulating a specific kind of technology may result in delays on its uptake or the realisation of economic benefits, there are often good reasons to do so where that technology is deemed high-risk. FRT is a technology which poses an unacceptable risk to human rights without regulation.

106. In respect of the 'consideration by government of the regulation of biometric technologies', the Commission recommendations the following in response to Proposal 13.2.

Recommendation 11: Until the legislation recommended in Recommendation 9 comes into effect, Australia's federal, state and territory governments should introduce a moratorium on the use of facial recognition and other biometric technology in decision making that has a legal, or similarly significant, effect for individuals, or where there is a high risk to human rights, such as in policing and law enforcement.

107. This moratorium would not apply to all uses of facial and biometric technology. It would apply only to uses of such technology to make decisions that affect legal or similarly significant rights, unless and until specific legislation is introduced with effective human rights safeguards.

108. The Commission is not alone in recommending a moratorium on the use of FRT. For example, in June 2020 the *Facial Recognition and Biometrics Technology Moratorium Act* was introduced into US Congress. In June 2021, US senators reintroduced that same act in response to reports that US law enforcement agencies have used unregulated FRT, in addition to research indicating that approximately half of the adult US population are already in facial recognition databases.[106]

7 Proposal 16.1

Define a child as an individual who has not reached 18 years of age.

109. The Commission recommends that the amendment in Proposal 16.1 and all other proposals of the Review Report (in respect of children) be considered in light of Committee on the Rights of the Child's General Comment 25 on children's rights in relation to the digital environment, and

the 2021 Report of the Special Rapporteur on the Right to Privacy on children's privacy (Special Rapporteur).

110. Any measures that respond to children must also recognise their differing levels of decision-making ability, based on their maturity and development. A one-size fits all approach for children will not be effective in protecting their rights.

111. The primary instrument enshrining children's rights is the Convention of the Rights of the Child (CRC), which Australia has ratified. Article 1 of the CRC states that a child be defined as any individual under the age of 18.

112. Article 16 of the CRC protects the right to privacy. It states that:

> *No child shall be subject to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful interference with his or her honour and reputation.*
>
> *The child has the right to protection of the law against such interference or attacks.*

113. Of relevance are considerations around 'information privacy', which protects information created about children.[107] This may include information about 'children's identities, activities, location, communication, emotions, health and relationships'.[108] As the Committee on the Rights of the Child has recognised in General Comment 25, there are significant implications for children's privacy associated with increasingly 'routine' practices that include 'automated data processing, profiling, behavioural targeting, mandatory identity verification, information filtering and mass surveillance'.[109]

114. Children's rights are universal, indivisible, interdependent and interrelated.[110] The right to privacy is necessary for the protection of other rights, including rights to freedom of expression, thought and association (CRC arts 13, 14, 15). The Special Rapporteur has observed that 'the foundations of future intellectual, emotional and sexual life are developed in childhood and adolescence, aided by the conditions of a private life'.[111] As such, privacy is essential to children's development.

115. Children's privacy is also more complex than adults' right to privacy, due to a range of factors including:

- the particular vulnerability of children
- parental rights to raise their child
- children's changing capacities and development that affect, for example, the application of consent mechanisms.

116. Children are especially vulnerable to privacy risks and harms as they may lack necessary technical, critical and social skills to engage with digital

spaces in a safe and beneficial manner.[112] This risk is exacerbated as many online services designed to engage with children and young people may not always be safe, appropriate and privacy protective.[113]

7.1 Specific risks related to children

117. The Commission is especially concerned about the risks that children and young people face in respect of:

- how their personal information may be monetised
- the social impacts of sharing personal information on their reputation and life opportunities
- online safety risks
- the rise of surveillance of young people in everyday settings, such as in classrooms

118. Inadequate privacy protections online also risk children's rights to life, survival, and development (CRC art 6), including but not limited to:

- exposure to online exploitation or abuse, harassment, and cyberbullying
- targeting by criminal entities
- exposure to violent or sexual content.[114]

119. For example, early and frequent exposure to online pornography has been connected to a range of harms affecting children. Nearly half of children between the ages of 9–16 experience regular exposure to sexual images.[115] Studies have found that 'pornography both contributes to and reinforces the kinds of social norms and attitudes that have been identified as drivers of violence against women',[116] and that viewing pornography is 'associated with unsafe sexual health practice'.[117]

120. Insufficient privacy protections for children also creates potential for discrimination through:

- exclusion from online services
- subjection to profiling or targeting by AI systems on the basis of biased or unfairly obtained data
- receipt of hateful content on online platforms.[118]

121. The Commission also reiterates the following additional risks:

- Automated search and information filtering that 'prioritise paid content with a commercial or political motivation' and impinge upon children's autonomy and right to access information.[119]

- Behavioural techniques designed to increase engagement with platforms, which 'trigger impulsive behaviours, influence decision-making, spark fear of exclusion and override privacy concerns'.[120]

122. The rise of targeted marketing is well noted in the Review Report, and the Commission agrees with the observations made in the OAIC's submission surrounding the negative impacts such advertising can have in increasing problems such as obesity, early alcohol consumption or smoking cigarettes or e-cigarettes.[121]

123. Equally the OAIC's concern that such marketing may modify psychological or mental health surrounding body image, sexualisation of children, entrenchment of gender stereotypes, stigmatisation of poverty and reduction in parents' authority and influence is also supported by the Commission.[122] This is also true of the OAIC's submission in respect of reputational risk.[123]

124. However, the Commission emphasises the risk of surveillance more generally as threatening children's right to privacy. For example, the Commission is deeply concerned by the rise of surveillance and information harvesting by educational technology (EdTech).

7.2 EdTech as a case study for the better protection of children

125. In 2022, Human Rights Watch published a global study of the EdTech products endorsed by governments during the Covid-19 pandemic.[124] That study found that endorsement of the majority of the 163 EdTech products reviewed, 'put at risk or directly violated children's privacy and other children's rights, for purposes unrelated to their education'.[125]

126. EdTech rose to prominence during the COVID-19 pandemic as many schools were closed and classes were taught remotely. During this time children's use of EdTech apps increased by 90%.[126] Unfortunately in the rapid switch to remote learning, many governments and schools failed to check if these EdTech products sufficiently protected children's information.[127]

127. The Commission notes that many EdTech platforms were already in prolific use in Australia before the pandemic, and that there has been growing concern regarding their impact on children for many years now.[128] For example, in 2019, Class Dojo was used in 95% of classrooms in the US and over 50% in Australia.[129]

128. The Human Rights Watch study found that 89% of the Ed Tech products reviewed appeared to engage in privacy-threatening or privacy-

breaching data practices at a given point in time.[130] Such privacy intrusions facilitated by EdTech may include:

- Tracking technologies which trail children 'outside' of their virtual classrooms and across the internet over time. For example, where a child does homework via an EdTech program, but is led to click a link to another site where the harvesting of data will continue.[131]
- Granting access to children's data to third party companies, such as advertising technology firms,[132] is especially concerning as access to small pieces of data can, per the mosaic effect, provide a detailed profile about a child. This provides organisations with the ability to make informed decisions about a child's personal characteristics and interests, predict what a child might do next and how they might be influenced.[133]

129. Perhaps most significantly, Human Rights Watch found a lack of transparency on the part of governments and EdTech companies as children, parents, and teachers were kept in the dark – unable to scrutinise properly the risk to children's privacy.[134]

130. Although there are benefits to utilising technologies in the educational settings, the Commission echoes concerns regarding a lack of transparency, and notes that consent forms (asking parents to agree to the collection of data by third party online providers) appear to obfuscate what data is collected, and how it is used. Often such forms reference privacy policies which can be hundreds of pages long and impenetrable to the average person – or even the average lawyer.[135]

131. EdTech is one example of the unique privacy risks facing children, and has been used for illustrative purposes. This is not indicative of the relative importance of the particular example in comparison to other issues. Rather, it reflects the Commission's relevant expertise in certain areas, and current capacity. There are also myriad other risks.

132. While the Commission separately notes the urgent need for a comprehensive response by Federal and State and Territory governments to privacy concerns in respect of EdTech, the Commission views the inclusion of a definition of a 'child' as a necessary first step in recognising and appropriately responding to the increased risks young people face when online privacy protections are not in place.

Recommendation 12: A child be defined as an individual who has not reached 18 years of age.

8 Paragraph one of Proposal 16.2

Existing OAIC guidance on children and young people and capacity should continue to be relied upon by APP entities. An entity must decide if an individual under the age of 18 has the capacity to consent on a case-by-case basis. If that is not practical, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise.

133. As discussed throughout this submission, the online environment allows for both opportunities and risks with respect to children and their human rights. The Commission understands that what is age-appropriate depends on a range of factors, as children vary greatly in their physical, intellectual, social and emotional abilities.

134. The Special Rapporteur also urges state parties to 'adopt age-appropriate standards as regulatory instrument only with the greatest of caution when no better means exist'.[136] It should be acknowledged that material deemed 'age-appropriate' can still cause harm and pose inequalities for children with differing maturity and capacities.[137]

135. The Commission has reservations about the existing approach within the APP Guidelines that where it is not practicable or reasonable to assess the capacity of an individual under 18 on a case-by-case basis, an APP entity may presume that young people aged between 15 and 18 have capacity to consent (provided there is no evidence to suggest otherwise).

136. Such an approach places an onus on entities to consider any information regarding a young person which demonstrates they do not have that capacity. Although entities operate in data rich environments, the Commission remains concerned that this approach may incentivise entities to not look for contradictory evidence – allowing them to assume a person aged between 15 and 18 has capacity for informed consent.

137. The Commission recognises the burden that conducting such checks may have on an entity (and the risk it poses to young people's privacy). Any OAIC guidance on how to determine capacity must balance the need for genuine checks and the need to protect privacy.

9 Proposal 16.3

*Amend the Privacy Act to require that collection notices and privacy policies be clear and understandable, in particular for any information addressed specifically to a child.**

In the context of online services, these requirements should be further specified in a Children's Online Privacy Code, which should provide guidance on the format, timing and readability of collection notices and privacy policies.

**The final wording of any legislative provision will be developed through the legislative drafting process.*

138. The Commission supports amendments which require collection notices and privacy policies to be clear and understandable, especially where such information is addressed to children. This is broadly in line with the need to simplify collections notices (see above at 3). As such, consultation with children, young people and relevant stakeholders is necessary.

139. Article 12 of the CRC 'enables and informs' the child's rights under Article 16, requiring that children's views are given weight on an individual basis, and '[presents] children with an opportunity to identify issues which may interfere with their right to privacy'.[138] Children should be provided with an opportunity to participate in legislative and policy development processes on issues that affect children's privacy – including those conducted by the business community, and to have an active say in their individual lives over how their privacy is treated.[139]

140. The Commission supports amendments which require collection notices and privacy policies to be clear and understandable on the basis that further consultation is conducted with children, parents, child development experts, child-welfare advocates, industry, OAIC, the eSafety Commissioner and the Commission.

Recommendation 13: The Act be amended to require that collection notices and privacy policies are clear and understandable, in particular for any information likely to be accessed by children. This should be done in with children, parents and carers, child development experts, child-welfare advocates, industry, OAIC, the eSafety Commissioner and the Australian Human Rights Commission.

141. The use of the term 'addressed specifically' in Proposal 16.3 potentially casts a narrow net over what circumstances would carry with them an obligation to provide collection notices and privacy policies in a manner that children can easily understand. Although the Review Report contains the express caveat that the final wording of any legislation will be developed through the legislative drafting process – the Commission holds concern over the language currently proposed.

142. Broader language which realistically covers the full range of circumstances where a child or young person may come across a collection notice or privacy policy is necessary to ensure that they understand how their data may be collected and utilised. Accordingly, the Commission prefers wider language such as 'which is likely to be accessed by children'. As this may impose additional burden on business, consultation will be necessary to refine the language used.

Recommendation 14: The amendments referred to in Recommendation 13 should utilise broader language (as determined through consultations) to capture the true range of circumstances in which children may need to understand collection notices or privacy policies.

143. The Commission is broadly supportive of a Children's Online Privacy Code. In respect of Proposal 16.3, the Commission believes that including guidance on the format, timing and readability of collection notices and privacy policies in a Children's Online Privacy Code is essential.

Recommendation 15: The requirements contained within Proposal 16.3 should be further specified in a Children's Online Privacy Code, which should provide guidance on the format, timing and readability of collection notices and privacy policies.

144. However, to ensure that children understand how their personal information is utilised in respect of collection notices and privacy policies, more must be done. It is insufficient, in isolation, to provide easy to read collection notices and privacy policies if children and young people are not digitally literate.

145. Children are engaging with online services at a young age and while existing school programs may often teach children and young people digital literacy, greater investment is needed in teaching them about privacy and data in particular – especially how their information may be harvested and used for targeted advertising and profiling.

146. Young children should become familiar with the notion of a 'digital footprint' early in their primary education. Children are using online services at an incredibly young age with many becoming proficient in the use of technology relatively early in life. It is imperative that they have a rudimental understanding of a 'digital footprint' as early as possible to reflect the young age at which they first engage with digital spaces.

147. Any investment in teaching privacy and data must align with the specific ways in which collection notices and privacy policies will be provided to children. For example, schools should teach children how to read collection notices and privacy policies consistent with how notices and policies are to be drafted under the proposed reforms. This will ensure that notices and policies are not only easy to read and engage with, but that children actually understand what they are reading and how it may impact them.

Recommendation 16: Greater investment be provided to schools to enable them to teach children from the start of their primary education about how privacy and data may affect them online. Children must be taught how to read/understand collection notices and privacy policies in the prescribed format as determined by the Act and/or the Children's Online Privacy Code.

10 Proposal 16.4

Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances.

148. Online privacy and safety measures should be developed in accordance with art 3 of the CRC, which requires that the 'best interests' of the child be a primary consideration in all actions concerning them. This is one of the four guiding principles of the CRC.

149. The best interests of every child should be a primary consideration in the digital environment.[140] When considering the best interests of the child, regard should be had to 'all children's rights, including their right to seek, receive and impart information, to be protected from harm and to have their views given due weight' in addition to ensuring transparency over the criteria applied to determine best interests.[141] Where rights are limited to protect children from online harms, limitations must be lawful, necessary and proportionate. Maximising children's privacy and securing their personal data is itself a 'crucial means of acting in their best interests'.[142]

150. Children's privacy should not be construed narrowly as relating only to data protection measures, and should recognise the importance of children's autonomy and choice over their private lives. A best interests approach may require implementing clear boundaries to prevent practices that both infringe upon children's rights and are contrary to their best interests, including by curtailing routine and indiscriminate digital surveillance measures.[143]

151. Children should have access to complaint and remedial mechanisms if their right to privacy is breached, and child-friendly information tailored to children's level of maturity and development about recourses should be readily accessible.[144] To secure children's privacy it is necessary to integrate human rights-by-design into digital products and services and to require high default privacy settings for all users of online services.[145]

152. Practices such as online tracking, profiling, behavioural monitoring and 'nudging', the collection of biometric and geolocation data from children, automated decisions affecting children and the unjustifiable sale or transfer of children's personal data to third parties should be banned or heavily restricted to protect children's rights. For example, among other things, General Comment 25 requires parties to:

> [P]rohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children[146]

153. This is especially important given the Special Rapporteur estimated that the 'the online advertising market for children could be worth 1.7 billion by 2021, with more than 72 million pieces of data collected for each child by online advertising companies before the child reaches the age of 13'.[147]

154. Best interest considerations should not be based on assumptions about what is in the interests of children. Their views should be actively considered.[148] In this regard, the Special Rapporteur notes that an 'adult's interpretation of children's privacy needs can impede the healthy development of autonomy and independence, and restrict children's privacy in the name of protection'.[149] The Special Rapporteur elaborates:

> While children's dependency, hence vulnerability, can result in risks, risk does not equate to harm and navigating some risk is necessary for children to develop resilience and coping skills. Defining children by their vulnerability only, without consideration of their capacity or potential, is likely to result in overly protectionist agendas, potentially harmful to children's personality.[150]

155. In order to ensure that the Children's Online Privacy Code is not based on assumptions about children's best interests, and that children's views are properly considered, children should have an opportunity to participate in the

process of developing, implementing, monitoring and evaluating the Children's Online Privacy Code.

156. The Commission therefore recommends that the principle of the 'best interests of the child' should be used as the primary test in the Children's Online Privacy Code, ideally with a positive duty on relevant actors to demonstrate that the principle is applied as a priority in both the development and application of the instrument (in this case, the Children's Online Privacy Code). This is reinforced by the Commission's Position Paper.[151]

Recommendation 17: The principle of the 'best interests of the child' should be the primary test used across all instruments affecting children online, including the Children's Online Privacy Code, with a positive duty on relevant actors to demonstrate that the principle is applied.

11 Proposal 16.5

Introduce a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'. To the extent possible, the scope of an Australian children's online privacy code could align with the scope of the UK Age Appropriate Design Code, including its exemptions for certain entities including preventative or counselling services.

The code developer should be required to consult broadly with children, parents, child development experts, child welfare advocates and industry in developing the Code. The eSafety Commissioner should also be consulted.

The substantive requirements of the Code could address how the best interests of child users should be supported in the design of an online service.

157. The Commission is broadly supportive of the introduction of a Children's Online Privacy Code which applies to online services that are likely to be accessed by children.

158. As art 12 of the CRC states, children have a right to express their views and opinions freely in all matters impacting them, and be listened to with due weight in accordance with their level of development and circumstance. Accordingly, it is imperative that their views and experiences are included in the development, implementation, monitoring and evaluation of a Children's Online Privacy Code.

159. The Commission would reinforce the need for broad consultation and input from children, young people, parents and schools on the kinds of online services which children are likely to access. It will also be of particular

importance to include, for example, children and young people from diverse backgrounds, including those who are Aboriginal and Torres Strait Islander, culturally and linguistically diverse, living with disability, and from refugee backgrounds, to understand the full spectrum of experiences, views and opinions held by children and young people. These consultations will require child-specific methodologies.

160. This may include acknowledging that children may be accessing online services which are age restricted (services which require a user to be over 18 years old). For example, pornography is often age restricted and yet is frequently utilised by children and young people. Research has shown that 28% of children aged 11 to 12 years had seen pornography, while that same study also found that 65% of children aged 15 to 16 had seen pornography online – with 94% of those having first seen it by the age of 14.[152] Pornography is just one example of children accessing material online which is traditionally not meant to be targeted to them. There is a variety of other material, such as violent or gambling content, which is also not traditionally meant to be targeted towards children, but which children often access.

161. These sorts of online environments which children may be accessing must be considered in the development of a Children's Online Privacy Code. It is insufficient to limit the application of 'likely to be accessed by children' to just online services which traditionally target children. The application must reflect how children and young people actually engage with online services.

Recommendation 18: A Children's Online Privacy Code should adopt a broad definition of services that are 'likely to be accessed by children'.

162. The Commission stresses the need to engage with all experts that understand the lived experiences, risks and opportunities posed by the digital environment on children. As children are the experts of their own lives, they should be made a priority in consultations. Additional stakeholders, such as parents and carers, schools and children's rights experts will be beneficial in introducing a Children's Online Privacy Code. This is necessary to ensure the prioritisation of privacy and other human rights standards over commercial interests.

Recommendation 19: A Children's Online Privacy Code should be developed following consultations with children and young people, parents and carers, schools, child development/welfare experts and

both the eSafety Commissioner and the Australian Human Rights Commission.

12 Proposal 17.1

Introduce, in OAIC guidance, a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information.

163. In its 2017 report, Elder Abuse—A National Legal Response (ALRC Report 131), the ALRC recommends adult safeguarding laws should define 'at-risk adults' to mean people aged 18 years and over who:

- have care and support needs
- are being abused or neglected, or are at risk of abuse or neglect and
- are unable to protect themselves from abuse or neglect because of their care and support needs.[153]

164. The Commission proposes this definition – which is supported by key adult safeguarding agencies, such as the Victorian[154] and Queensland[155] Offices of the Public Advocate – be included in any OIAC guidance and the Act where appropriate.

Recommendation 20: The definition of 'at-risk adult', provided in ALRC Report 131, be included in any OAIC guidance, and the Act where appropriate.

Recommendation 21: OAIC guidance must set out a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information.

165. This broad definition of 'at-risk' (which also serves to define the experience of vulnerability) allows for a situational rather than intrinsic conception of vulnerability as – to use the terminology of the Review Report – 'multifaceted, not confined to mental or physical capacity,[156] nor a fixed trait associated with a specific group or identifiable threshold'.[157]

166. The above definition recognises that a person can move in and out of vulnerability, and therefore better aligns with the proposal to refer to 'people

experiencing vulnerability' rather than 'vulnerable groups' or 'vulnerable individuals'.[158]

Recommendation 22: The term 'people experiencing vulnerability' is adopted in OAIC guidance, and the Act where appropriate.

167. The nature of disability and a person's experience of disability can be varied. Simply having a disability does not necessarily equate with a person experiencing vulnerability. The Commission supports 'disability' being included in OAIC guidance along with a list of other factors that can increase the likelihood that someone experiencing vulnerability is captured by the non-exhaustive list. Any such list should be used as an indicative first step in conjunction with a more personalised assessment of an individual's circumstances and needs.

168. The NDIS Quality and Safeguards Framework provides a further useful differentiation between risks present at the individual level (e.g. due to personal characteristics) and risks based on the types of supports provided to a person (e.g. level of personal contact, in closed environments, etc.).[159]

169. In the context of privacy of information, people with disability may experience vulnerability in multiple ways, including, for example:

- In the case of some intellectual and cognitive disabilities, decreased ability to understand or prevent risks associated with how their information may be used.
- In the case of some physical or psychosocial disabilities, decreased ability (whether on a sustained, temporary, or periodic basis) to communicate their wishes with regard to their information.
- Depending on the level of assistance they may be being provided by others, people with disability may necessarily be at higher risk of exploitation by people with regards to access to their information.
- In all cases, people with disability are at risk of disability discrimination if information regarding their disability is revealed or otherwise made available to other parties who then may misuse or exploit that information.

170. Importantly, OAIC guidance should be clear to not discourage proportionate, proactive and preventative safeguarding measures to be activated if there is a perceived risk that a person is experiencing vulnerability. OAIC guidance must also be developed and co-designed with people with disability.

Recommendation 23: OAIC guidance should be clear to not discourage proactive and preventative safeguarding measures to be activated if there is a perceived risk that a person is experiencing vulnerability.

Recommendation 24: OAIC guidance concerning disability should be developed and co-designed with people with disability.

13 Proposal 17.2

OAIC guidance on capacity and consent should be updated to reflect developments in supported decision making.

171. The Commission supports this proposal. In particular, the Commission agrees that guidance should be consistent with the United Nations Convention on the Rights of Persons with Disabilities (CRPD), enable supported decision-making, and recognise the autonomy and independence of all persons with disability, including those who may require support in making decisions.

172. The guidance should align to the recommendations in ALRC Report 124,[160] and the more recent supported decision-making framework proposed by the Royal Commission into Violence, Abuse, Neglect, and Exploitation of People with Disability in its 2023 report *Diversity, dignity, equity and best practice: a framework for supported decision-making.*[161]

Recommendation 25: OAIC guidance on capacity and consent should be updated to reflect ALRC Report 124 and the *Diversity, dignity, equity and best practice: a framework for supported decision-making* report.

173. The Commission agrees that guidance on 'how third parties who give decision-making support should be recognised, and what steps entities should take to ensure that authorities, nominations and consents are valid, should be developed in consultation with affected groups'.[162]

14 Proposal 17.3

Further consultation should be undertaken to clarify the issues and identify options to ensure that financial institutions can act appropriately in the interests

of customers who may be experiencing financial abuse or may no longer have capacity to consent.

174. The Commission supports the proposal and continues to advocate for the implementation of the recommendations from ALRC Report 131 and the *National Plan to Respond to the Abuse of Older Australians 2019–2023*, which should be considered in consultations.

Recommendation 26: Further consultations should be undertaken in respect of Proposal 17.3. Such consultations should have regard for ALRC Report 131 and the *National Plan to Respond to the Abuse of Older Australians 2019–2023*.

175. Current inconsistencies in regulations and requirements regarding financial decision-making across jurisdictions cause confusion in the community, make it difficult for individuals and families to understand the rules and for experts to provide advice across jurisdictions. Consultation should focus on the issues particular to each jurisdiction, as well as the varied solutions necessary, such as greater harmonisation of enduring power of attorney laws, for example.

176. Reform in this area should enable the development of nation-wide education around the rights and responsibilities of principals and their substitute decision makers as well as to facilitate training of financial institutions and other entities required to act on enduring powers of attorney to prevent financial abuse.

Recommendation 27: A nation-wide education campaign should be enacted by the Federal government around the rights and responsibilities of principals and their substitute decision makers.

Recommendation 28: The Federal government should facilitate the training of financial institutions and other entities required to act on enduring powers of attorney to prevent financial abuse.

15 Proposal 19.1

Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights.

177. This requirement will promote transparency by entities utilising AI-informed decision-making (ADM) systems, as noted by several submitters to the Review Report.[163] Transparency about the use and operation of ADM is central to a human-rights-based approach to regulation, as this information may assist individuals in both understanding the way in which relevant decisions are made and subsequently enforcing their rights.

178. Transparency will also help to engender trust in ADM processes – as Australia must strive to reap the benefits of new and emerging technologies (such as AI), while mitigating the risks to individuals' rights. Including what types of personal information will be used in ADM systems (and therefore the fact that ADM systems may be used) is a positive first step forward towards better regulating AI.

Recommendation 29: Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights.

15.1 The role of transparency in privacy policies

179. Acknowledging the types of personal information that will be used in substantially automated decisions in an entity's privacy policy will not, of itself, prevent algorithmic bias from affecting individuals or businesses (as noted in Calabash Solution's submission to the Discussion Paper).[164] Further, the extent to which this proposal will aid transparency in practice may be doubtful in the broader context, considering many individuals may:

- not read privacy policies at all
- struggle to understand them, as organisations often obfuscate how data will be collected, maintained and utilised through complex language[165]
- be powerless to do anything, even where they understand the privacy or AI risks to their data.[166]

180. The Commission acknowledges that Proposal 19.1 fails to extend beyond aiding transparency, should individuals genuinely engage in active consideration of an entity's privacy policy. The current approach places the onus on individuals to read, understand and 'agree' to allowing an organisation to collect, maintain and utilise their information for ADM. As noted above at 4.1, there are limitations on models which place the onus on individuals to protect their own data.

15.2 Legal or similarly significant effect

181. The use of personal information by entities in ADM engages the right to privacy, under the ICCPR, UNDHR and proposed Australian Human Rights Act.[167]

182. The Commission supports the use of 'legal or similarly significant effect' in Proposals 19.1 and 19.2. The Commission uses the phrase 'legal or similarly significant' to define ADM in its Final Report.[168] The use of this phrase is consistent with the human rights approach the Commission adopts in analysing the challenges posed by ADM in its Final Report.[169] It is also utilised in the European Union's (EU) General Data Protection Regulation (GDPR) to regulate solely automated decisions.[170] The use of AI to make decisions that have legal or similarly significant effect on individuals is likely to engage human rights in a significant way – and the use of this phrase may assist in delineating the categories of decision that are likely to engage human rights more broadly.[171]

183. However, as considered in the Commission's Final Report, the use of AI engages a broader range of human rights (including both civil and political rights, and also economic, social and cultural rights).[172] For instance, the Commission provides an example of the risks of using AI in government decision-making in the criminal justice system, whereby governments employ risk assessment tools to predict the likelihood of future criminal behaviour.[173] The use of such tools in certain decisions, such as those involving sentencing, bail and post-sentence restrictions, may engage several political and civil rights, such as the right to equality and non-discrimination.[174]

184. The United Kingdom's Information Commissioners Office (UK ICO) guidance states that a decision produces 'legal effects' if it affects an individual's legal status or legal rights, such as the ability to access a social security benefit.[175]

185. The Commission considers that while the meaning of 'legal right' is sufficiently clear, further clarification should be provided to entities as to the scope of 'similarly significant effect'. While UK ICO guidance states that a decision has a 'similarly significant effect' to a legal decision if it has an

equivalent impact on an individual's circumstances, behaviour or choices,[176] it is unclear what circumstances would constitute a 'significant' effect. Several submitters to the Discussion Paper support the provision of additional clarification as to the meaning of 'similarly significant effect'.[177] The Ai Group and Business Council of Australia acknowledged that without this clarification, there remains a non-compliance risk of regulated entities using AI to support decision-making, particularly in the fields of employment and recruitment.[178] The Commission therefore also supports the proposal that OAIC guidance should be developed on the types of decisions with a 'legal or similarly significant effect'.

Recommendation 30: OAIC guidance should be developed on the types of decisions with a legal or similarly significant effect on an individual's rights.

15.3 Substantially automated decision

186. The definition of 'substantially automated' (as used in Proposal 19.1) necessarily should not capture ADM where a human decision-maker has genuine oversight of a decision, and reviews that decision before it is applied.

187. However, there is a real risk that individuals may become overly reliant on the outcomes produced by ADM and AI. This overreliance is known as 'automation bias', which is the 'tendency to use automated cues as a heuristic replacement for vigilant information seeking and processing'.[179]

188. Automation bias can have severe consequences for individuals. For example, it is not uncommon to find articles documenting individuals driving their cars into the ocean while following GPS systems, like Google Maps.[180] More concerningly is when automation bias is involved in medical settings, with one conference paper suggesting that oncologists interpreting mammograms are incorrectly accepting system advice in 33%–40% of cases.[181]

189. In determining what ADM decisions are 'substantially automated' for the purpose of Proposal 19.1, regard must be had for the role that 'automation bias' has in how human decision makers regard the outcomes of ADM and AI.

Recommendation 31: Any OAIC guidance which attempts to define 'substantially automated' decisions must give proper consideration to

the role automation bias may play in how deeply individuals scrutinise an ADM decision.

190. It is important not to limit the scope of what decisions can be considered 'substantially automated', due to the potential unfair and discriminatory impacts of ADM systems. UK ICO guidance states that the definition of 'solely automated decisions' used in the GDPR (which they acknowledge may involve human intervention) does not capture decisions whereby a human reviews the decision before it is applied.[182]

191. The Commission supports the need for greater guidance to be provided to entities as to the meaning of 'substantially automated', and that consultation will be required to ensure the parameters of 'substantially automated' are appropriately calibrated.

Recommendation 32: The OAIC should develop guidance which defines 'substantially automated' decisions. This guidance must include a non-exhaustive list of decisions considered as 'substantially automated'.

16 Proposal 19.3

Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect.

This proposal should be implemented as part of the broader work to regulate AI and ADM, including the consultation being undertaken by the Department of Industry, Science and Resources.

16.1 Right to reasons

192. The Commission broadly supports a right for individuals to request meaningful information about substantially automated decisions. The Commission also considers the need for a broader right to request reasons in respect of substantially automated decisions. A right to reasons in this context will assist in promoting fairness and transparency in the use of AI in decision-making. Furthermore, the provision of reasons enables individuals

who are the subject of automated decisions to exercise other rights, such as the right to object and the right to remedy.

193. This proposal extends further than that of Proposal 19.3 in terms of protecting human rights, as it enables affected individuals to actively challenge decisions and access an effective remedy, as opposed to just improving the transparency of ADM. The Commission noted in its Final Report that a human rights approach to the regulation of ADM requires access to an effective remedy where an individual's human rights have been breached.[183]

194. Information provided about an ADM decision must be conveyed in a clear, understandable format in order to allow individuals to properly respond. In the Commission's Final Report, stakeholders warned that simply providing the technical basis for AI informed decisions may do little to assist individuals to understand or challenge those decisions.[184]

195. While the Commission considers that the requirement for a right to reasons is currently more pressing than it was at the time of our Final Report, the Commission also acknowledges the difficulties surrounding the introduction of such a requirement.

196. It is technically difficult for some ADM systems to generate reasons. The use of AI may obscure the rationale or reasons for a decision –referred to as the problem of 'black box' or 'opaque' AI.[185] This, in turn, can make it difficult or even impossible to challenge the merits or lawfulness of a decision.[186] While some leading software companies are exploring building an explanation function into ADM systems, this process can be technically challenging and expensive.[187]

197. The ability of small and medium-sized entities to generate meaningful information may be hindered by the financial cost of extracting a useful explanation (particularly in complex ADM systems) and the time it would take for an organisation to generate an explanation.[188] It may be possible to overcome this difficulty if further research is conducted by centres of expertise on explainable AI and expert guidance is provided by government on how to provide reasons for AI-informed decisions, as recommendation by the Commission in its Final Report.[189]

198. Furthermore, there may not necessarily exist a legal entitlement to the provision of reasons in the current legislative environment. For instance, the Commission noted in in its Final Report that decisions by non-government bodies do not carry a legal entitlement to reasons.[190]

199. The Commission considers that in light of recent technological developments, a right to request reasons is a pressing requirement. This is particularly so in relation to use of ADM systems by government, as government should always be able to explain how they arrive at decisions, in

accordance with the principle of open government. As noted in the Final Report, the Commission opposes the use by government of ADM systems that cannot generate reasons, or a technical explanation, for the final decisions.[191] This is because government decisions will often inherently possess human rights impacts, and the principles of open government provide an important foundation in Australia's democratic system. The use by government of complex ADM systems, that cannot generate reasons, may leave individuals with no right to remedy.

200. This is illustrated by the Government's 'Robodebt' scheme in 2015, whereby an automated debt recovery system used an algorithm to identify any discrepancies between an individual's declared income to the Australian Taxation Office, and the individual's income reported to Centrelink. A discrepancy was considered undeclared income, and as a result, a debt notice was automatically generated and sent to the individual.[192]

201. The Commission has previously made a submission to the Senate Community Affairs References Committee regarding its inquiry into 'Centrelink's compliance program'.[193] In that submission the Commission noted its concerns and highlighted the risk posed to the right to social security which is protected by art 9 of the International Covenant on Economic, Social and Cultural Rights – the impediment of which can impede the realisations of other human rights.[194]

202. A parliamentary inquiry has since revealed that this process resulted in various inaccurate debt notices. As the scheme involved social security payments, such errors disproportionately affected people with pre-existing socioeconomic disadvantage and vulnerability.[195] The Commonwealth Ombudsman, in its review of the scheme, urged the Department of Human Services to 'improve the clarity' of the letters sent to individuals, and to provide people 'better information so they understand the information and can properly respond to it'.[196]

203. As demonstrated in the subsequent Royal Commission into the Robodebt Scheme (Royal Commission), countless individuals suffered because of the scheme's algorithm. In just one example of the serious harms caused by the scheme, Kathleen Madgwick told the Royal Commission of her son, Jarrad Madgwick, who had taken his own life just hours after he learned of a $2,000 Centrelink Robodebt.[197] The scheme demonstrates the dangers of the of ADM systems which lack human scrutiny and where clear, understandable reasons cannot be provided for decisions that inherently impact a person's human rights.

204. The use of black box AI may infringe upon human rights in whatever sector it arises, whether that be in government, the private or the non-government sector.[198]

16.2 Further work in regulating AI and ADM

205. The Commission strongly supports further work in regulating AI and ADM. The regulation of AI in ADM was subject to extensive reporting and work in our Final Report. The Commission recommended, for example, the appointment of an AI Safety Commissioner as an independent statutory office. This body would function as a source of expertise on AI, by providing guidance to government and the private sector on how to comply with laws surrounding the development and use of AI.[199]

206. For instance, as recommended in the Final Report, the proposed AI Safety Commissioner could develop guidance for government and non-government entities on how to generate reasons for AI-informed decisions.[200] This body would further function to provide independent advice to policy makers and parliament by monitoring trends in the use of AI in Australia and internationally to address risks associated with AI.[201] Lastly, it would also function to build the capacity of other regulators and the broader regulatory scheme surrounding AI and ADM, to adapt and respond to the rise of AI technologies.[202] The appointment of an AI Safety Commissioner is a fundamental first step in better regulating AI and ADM.

Recommendation 33: The Australian Government should establish an AI Safety Commissioner as an independent statutory office, focused on promoting safety and protecting human rights in the development and use of AI in Australia. The AI Safety Commissioner should:

- **work with regulators to build their technical capacity regarding the development and use of AI in areas for which those regulators have responsibility**
- **monitor and investigate developments and trends in the use of AI, especially in areas of particular human rights risk**
- **provide independent expertise relating to AI and human rights for Australian policy makers**
- **issue guidance to government and the private sector on how to comply with laws and ethical requirements in the use of AI.**

16.3 Algorithmic bias

207. While AI allows large amounts of relevant information to be considered in decision-making processes and may encourage efficient, data-driven decision making, its regulation is becoming increasingly important, due

to its potential to produce 'algorithmic bias'. Algorithmic bias arises where an ADM tool produces outputs that result in unfairness.[203] Algorithmic bias can entrench unfairness, or even result in unlawful discrimination.[204]

208. For instance, ADM systems may unintentionally produce discrimination in the employee vetting process. For instance, Amazon used an AI software that was designed to review resumes and determine which applicants Amazon should hire.[205] The algorithm systemically discriminated against women applying for technical jobs, such as software engineer positions. This is because the existing pool of Amazon software engineers were by majority male, and as such, the new software was fed data about those engineers' resumes.[206] The practice of directing software to discover resumes similar to resumes in a training data set will inevitably reproduce the demographics of the existing workforce.[207]

209. Another example of algorithmic bias was when, in 2019, a study discovered that a clinical algorithm used by many hospitals in the US to determine which patients required extra medical care produced racial bias.[208] The algorithm was trained on past data on healthcare spending, which reflects a trend whereby black patients have less income to spend on their healthcare as compared with white patients - a result of systemic wealth and income disparities.[209] As such, the algorithm's outputs reflected a discriminatory result whereby white patients required more medical care than black patients.[210]

210. Such examples highlight why AI and ADM require greater regulation, in the interests of increasing transparency, preventing unfairness and unlawful discrimination in algorithmic decision-making. This is especially the case given the difficulty of applying anti-discrimination law to complex ADM systems.[211] The Commission emphasises its 2020 technical paper '[Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias]' which considers algorithmic bias in greater detail. Australia must do more to regulate the use of AI and ADM as a matter of priority. In the two years since the Final Report was released there has been disappointingly little movement in this space. However, the Commission is pleased that broader work is now being done to engage with how to regulate AI and ADM.

Recommendation 34: Proposal 19.3 should be implemented as part of broader work to regulate AI and ADM. Such regulatory work should ensure human-rights-centred design and deployment of AI and ADM and would benefit from consultation with human-rights focused bodies, such as the Commission.

17 Proposal 27.1

Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123.

Consult with the states and territories on implementation to ensure a consistent national approach.

17.1 Freedom of expression

211. The Commission acknowledges the submissions by media organisations about the possible 'chilling effect' that the proposed tort for the serious invasion of privacy in the form recommended by the Australian Law Reform Commission's report, *Serious Invasions of Privacy in the Digital Era* (Report 123), may have on the freedom of expression.

212. The submissions from media organisations raising concerns about the proposed tort do raise important issues about the interaction between competing human rights, most notably the tension between the right to privacy and the right to freedom of expression. Most human rights are not absolute, and circumstances may require that different rights be balanced against important public interests, and against intersecting rights. Balancing rights is often a difficult task and is not exclusive to these two rights – for example, the right to access information and the right to national security interests will also often need to be balanced against one another.[212] Where such tensions exist a necessary balancing exercise is required.

213. As noted by the Discussion Paper, a common law tort of privacy has often been used in other jurisdictions by high profile individuals to take legal action against media outlets.[213] As noted by other submitters, if the statutory tort were introduced, wealthy and well-resourced individuals could commence proceedings under the proposed tort of privacy.[214] It has further been submitted by some media organisations that a tort of privacy would offer no benefit to the vast majority of Australians due to the cost of commencing litigation.[215]

214. It is relevant to consider issues in respect of a lack of access to justice in the Australian jurisdiction – where wealthy individuals and organisations can protect their legal rights, while those with less cannot. However, citing a lack of access to justice is by no means a reason to oppose legislative reform. The Commission is aware of numerous areas of the law effected by a lack of access to justice across Australia. Rather than using this as a reason to avoid necessary law reform, a better response would be to look for ways to improve access to justice for all individuals.

215. Submissions by media organisations noted that wealthy individuals may utilise the proposed statutory tort to avoid accountability to the detriment of Australian democracy.[216] Laws should never be used to frustrate accountability and transparency where there is no legal standing to do so. However, as noted in the Review Report, the public interest tests incorporated in Report 123's model does much to mitigate this concern – and functions as a weighing mechanism between the right to privacy and the right to freedom of expression.[217]

216. Although the tort may be used to frustrate attempts by media organisations to ensure accountability and transparency – this is not always the case. There are also circumstances where it could be argued that the media goes too far in exposing the private lives of individuals.

217. For example, take the scandal surrounding the attempt by Andrew Hornery of the Sydney Morning Herald to 'out' Australian actor Rebel Wilson as being in a same-sex relationship.[218] Hornery effectively informed Wilson that he would be publishing an article (which informed the public of a private same-sex relationship) about her relationship. In response to this communication, Wilson was arguably compelled to announce the relationship before Hornery could ever publish his article. This is an illustrative example of when the media may breach the right to privacy purposes other than ensuring transparency and accountability. It also demonstrates the importance of introducing a statutory tort.

17.2 Fault element

218. In its Final Report the Commission supported the OAIC in its claim that a statutory cause of action should be comprehensive and non-restrictive, and cover all intentional, reckless and negligent acts of privacy invasion by public and private entities.[219]

219. The Commission also agrees with the issue raised by the Castan Centre, that Report 123 sets the bar too high by limiting the fault elements to only intentional or reckless acts.[220]

220. The Commission does not support Report 123's model being confined to only intentional or reckless invasions of privacy. Negligent acts of privacy invasion should also be included in the statutory tort to avoid an unnecessarily limited application of the tort in different circumstances. To ensure this is achieved the tort should not specify a fault element.

Recommendation 35: Ensure that any statutory tort which is introduced differs from the model proposed in Report 123, in that it should cover

intentional, reckless and negligent acts by not specifying a fault element.

17.3 A non-restrictive tort

221. The Commission has previously supported a non-restrictive tort.[221] In contrast, Report 123's model confines the application to serious invasions of privacy either by intrusion upon seclusion or by misuse of private information. The tort should not be limited to only the two proposed categories on the basis that some serious invasions of privacy may fall outside of these categories.

222. A non-restrictive statutory tort could be more flexible and responsive to privacy concerns – allowing for art 17 of the ICCPR, art 12 UNDHR and the right to privacy and reputation under the proposed Australian Human Rights Act to be fully appreciated. In a world of rapid technological advancement (which often adopts Mark Zuckerberg's ethos of 'move fast and break things'),[222] such a tort must also be technology neutral to ensure it continues to be relevant as new and emerging technologies are developed and deployed.

223. The more restrictive tort proposed by Report 123 is too inflexible and may fail to keep up with technological advancements – advancements which may threaten the right to privacy in new and invasive ways. Accordingly, a non-restrictive and flexible tort must be introduced which diverges from the model proposed by Report 123.

224. Consistent with Recommendation 21 of the Commission's Final Report, the introduction of a statutory tort for serious invasions of privacy is supported. However, this should be a non-restrictive and flexible tort that differs from the more restrictive model proposed in Report 123.

Recommendation 36: Ensure that any statutory tort which is introduced differs from the model proposed in Report 123, in that it should be a non-restrictive and flexible tort which does not confine the tort to intrusions upon seclusion and misuse of private information.

18 Recommendations

225. The Commission makes the following recommendations.

Recommendation 1

Amend the objects of the Act to clarify that the Act is about the protection of personal information.

Recommendation 2

The human right to privacy must be included as the paramount object in s 2A of the Act.

Recommendation 3

'Geolocation tracking data' should be defined as sensitive information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time.

Recommendation 4

Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable. Appropriate accessibility measures should also be in place.

Recommendation 5

The OAIC provides guidance on the meaning to 'up-to-date' in respect of Proposal 10.1.

Recommendation 6

The definition of consent be amended to provide that it must be voluntary, informed, current, specific, and unambiguous.

Recommendation 7

OAIC guidance should be strengthened to fully incorporate the ALRC Report 124 national decision-making principles.

Recommendation 8

A parliamentary inquiry into the risks of facial recognition technologies be commenced with terms of reference which, among other things, specifically considers the human rights risks of the technologies.

Recommendation 9

Federal, State and Territory governments should introduce legislation which specifically regulates the use of facial recognition and other biometric technologies. Such legislation should:

- expressly protect human rights
- apply to the use of this technology in decision making that has a legal, or similarly significant, effect for individuals, or where

there is a high risk to human rights, such as in policing and law enforcement

- be developed through in-depth consultation with the community, industry and expert bodies such as the Australian Human Rights Commission and the Office of the Australian Information Commissioner.

Recommendation 10

The Model Law be implemented by government, with in-depth consultations with the community, industry and expert bodies such as the Australian Human Rights Commission and the Office of the Australian Information Commissioner being held to assist before any legislation is finalised.

Recommendation 11

Until the legislation recommended in Recommendation 9 comes into effect, Australia's federal, state and territory governments should introduce a moratorium on the use of facial recognition and other biometric technology in decision making that has a legal, or similarly significant, effect for individuals, or where there is a high risk to human rights, such as in policing and law enforcement.

Recommendation 12

A child be defined as an individual who has not reached 18 years of age.

Recommendation 13

The Act be amended to require that collection notices and privacy policies are clear and understandable, in particular for any information likely to be accessed by children. This should be done in with children, parents and carers, child development experts, child-welfare advocates, industry, OAIC, the eSafety Commissioner and the Australian Human Rights Commission.

Recommendation 14

The amendments referred to in Recommendation 14 should utilise broader language (as determined through consultations) to capture the true range of circumstances in which children may need to understand collection notices or privacy policies.

Recommendation 15

The requirements contained within Proposal 16.3 should be further specified in a Children's Online Privacy Code, which should provide

guidance on the format, timing and readability of collection notices and privacy policies.

Recommendation 16

Greater investment be provided to schools enabling them to teach children from the start of their primary education about how privacy and data may affect them online. Children must be taught how to read/understand collection notices and privacy policies in the prescribed format as determined by the Act and/or the Children's Online Privacy Code.

Recommendation 17

The principle of the 'best interests of the child' should be the primary test used across all instruments affecting children online, including the Children's Online Privacy Code, with a positive duty on relevant actors to demonstrate that the principle is applied.

Recommendation 18

A Children's Online Privacy Code should adopt a broad definition of services that are 'likely to be accessed by children'.

Recommendation 19

A Children's Online Privacy Code should be developed following consultations with children and young people, parents and carers, schools, child development/welfare experts and both the eSafety Commissioner and the Australian Human Rights Commission.

Recommendation 20

The definition of 'at-risk adult', provided in ALRC Report 131, be included in any OAIC guidance, and the Act where appropriate.

Recommendation 21

OAIC guidance must set out a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information.

Recommendation 22

The term 'people experiencing vulnerability' is adopted in OAIC guidance, and the Act where appropriate.

Recommendation 23

OAIC guidance should be clear to not discourage proactive and preventative safeguarding measures to be activated if there is a perceived risk that a person is experiencing vulnerability.

Recommendation 24

OAIC guidance concerning disability should be developed and co-designed with people with disability.

Recommendation 25

OAIC guidance on capacity and consent should be updated to reflect ALRC Report 124 and the Diversity, dignity, equity and best practice: a framework for supported decision-making report.

Recommendation 26

Further consultations should be undertaken in respect of Proposal 17.3. Such consultations should have regard for ALRC Report 131 and the National Plan to Respond to the Abuse of Older Australians 2019-2023..

Recommendation 27

A nation-wide education campaign should be enacted by the Federal government around the rights and responsibilities of principals and their substitute decision makers.

Recommendation 28

The Federal government should facilitate the training of financial institutions and other entities required to act on enduring powers of attorney to prevent financial abuse.

Recommendation 29

Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights.

Recommendation 30

OAIC guidance should be developed on the types of decisions with a legal or similarly significant effect on an individual's rights.

Recommendation 31

Any OAIC guidance which attempts to define 'substantially automated' decisions must give proper consideration to the role automation bias may play in how deeply individuals scrutinise an ADM's decision.

Recommendation 32

The OAIC should develop guidance which defines 'substantially automated' decisions. This guidance must include a non-exhaustive list of decisions considered as 'substantially automated'.

Recommendation 33

The Australian Government should establish an AI Safety Commissioner as an independent statutory office, focused on promoting safety and protecting human rights in the development and use of AI in Australia. The AI Safety Commissioner should:

- work with regulators to build their technical capacity regarding the development and use of AI in areas for which those regulators have responsibility
- monitor and investigate developments and trends in the use of AI, especially in areas of particular human rights risk
- provide independent expertise relating to AI and human rights for Australian policy makers
- issue guidance to government and the private sector on how to comply with laws and ethical requirements in the use of AI.

Recommendation 34

Proposal 19.3 should be implemented as part of broader work to regulate AI and ADM. Such regulatory work should ensure human-rights-centred design and deployment of AI and ADM and would benefit from consultation with human-rights focused bodies, such as the Commission.

Recommendation 35

Ensure that any statutory tort which is introduced differs from the model proposed in Report 123, in that it should cover intentional, reckless and negligent acts by not specifying a fault element.

Recommendation 36

Ensure that any statutory tort which is introduced differs from the model proposed in Report 123, in that it should be a non-restrictive and flexible tort which does not confine the tort to intrusions upon seclusion and misuse of private information.

Endnotes

[1] Attorney-General's Department, '*Privacy Act Review*' ('Discussion Paper') (Commonwealth of Australia, Discussion Paper, October 2021) 18-19.

[2] Attorney-General's Department, '*Privacy Act Review Report 2022*' ('Review Report') (Commonwealth of Australia, Report, February 2023) 21-22 [3.4].

[3] Attorney-General's Department, Review Report (Commonwealth of Australia, Report, February 2023) 21-22 [3.4].

[4] Attorney-General's Department, Review Report (Commonwealth of Australia, Report, February 2023) 21-22 [3.4].
[5] Attorney-General's Department, Discussion Paper (Commonwealth of Australia, Discussion Paper, October) 20.
[6] Attorney-General's Department, Review Report (Commonwealth of Australia, Report, February 2023) 21-22 [3.4].
[7] See e.g. Submission to the Discussion Paper: Digital Rights Watch 2 & 5; Australian Privacy Foundation 2-3; Lived Experience Australia 3; NSW Council for Civil Liberties 4.
[8] See *Universal Declaration of Human Rights,* article 12; *Convention on the Rights of the Child,* article 16.
[9] 'Derogations during a state emergency' Article 4(2) in *International Covenant on Civil and Political Rights* (United Nations, Treaty Series vol. 999, 16 December 1966).
[10] Australian Human Rights Commission ('AHRC'), '*Free & Equal Position Paper: A Human Rights Act for Australia*' ('Position Paper') (Position Paper, March 2023) 46.
[11] Office of the Australian Information Commissioner ('OAIC'), *'What is Privacy?'* *https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-privacy*.
[12] See generally Zuboff, Shoshana, '*The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier*' (New York: Public Affairs, 2019); see also Toby Walsh, '*Machines Behaving Badly: The Morality of AI*' (Black Inc, Melbourne, 2022).
[13] Jacob Kastrenakes, 'Google's chief internet evangelist says 'privacy may actually be an anomaly'' The Verge (online, 21 November 2013) https://www.theverge.com/2013/11/20/5125922/vint-cerf-google-internet-evangelist-says-privacy-may-be-anomaly.
[14] Attorney-General's Department, Review Report (Commonwealth of Australia, Report, February 2023) 22.
[15] AHRC, Position Paper (Position Paper, March 2023) 111 & 347.
[16] AHRC, Position Paper (Position Paper, March 2023) 139.
[17] AHRC, Position Paper (Position Paper, March 2023).
[18] AHRC, Position Paper (Position Paper, March 2023) 20.
[19] AHRC, Position Paper (Position Paper, March 2023) 23.
[20] *Momcilovic v The Queen* (2011) 245 CLR 1, [43] (French CJ).
[21] AHRC, Position Paper (Position Paper, March 2023) 111 & 347.
[22] AHRC, Position Paper (Position Paper, March 2023) 347.
[23] AHRC, Position Paper (Position Paper, March 2023).
[24] AHRC, Position Paper (Position Paper, March 2023) 308; Parliament Joint Committee on Human Rights, '*Annual Report 2020*' (Commonwealth of Australia, Report, 13 May 2021) 16 Figure 3.1.
[25] Parliament Joint Committee on Human Rights, '*Annual Report 2021*' (Commonwealth of Australia, Report, 28 September 2022) 15.
[26] AHRC, Position Paper (Position Paper, March 2023) 309.
[27] AHRC, Position Paper (Position Paper, March 2023) 56 citing Elise Scott, 'Senate passes controversial metadata laws' *Sydney Morning Herald* (Online, 27 March 2015) https://www.smh.com.au/politics/federal/senate-passes-controversial-metadata-laws-20150326-1m8q3v.html.; see also See e.g. discussion in Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report: Twentieth report of the 44th Parliament* (March 2015) 39–75; Australian Human Rights Commission submission to the Parliamentary Joint Committee on Human Rights, *Review of the mandatory data retention regime* (July 2019) https://humanrights.gov.au/our-work/legal/submission/review-mandatory-data-retention-regime-2019.

[28] AHRC, Position Paper (Position Paper, March 2023) 56 citing see e.g. *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth); *Telecommunications Legislation Amendment (International Production Orders) Act 2020* (Cth); *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth).
[29] AHRC, Position Paper (Position Paper, March 2023) 56 citing see e.g. Parliamentary Joint Committee on Intelligence and Security, '*Review of the mandatory data retention regime*' (October 2020) xi; see e.g. Independent National Security Legislation Monitor, '*Trust but verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*' (9th Report, June 2020) 42 (Recommendation 3).
[30] Deloitte, '*Smart everything, everywhere Mobile Consumer Survey*' (Survey, 2017) 6.
[31] Australian Competition and Consumer Commission ('ACCC'), *Consumer Views and Behaviours on Digital Platforms* (November 2018) 21.
[32] *Privacy Act 1988* (Cth) sch 1.
[33] *Privacy Act 1988* (Cth) s 6 'sensitive information'.
[34] Zak Doffman, 'Black Lives Matter: US Protesters Tracked by Secretive Phone Location Technology', *Forbes* (online, 26 June 2020) https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/?sh=6eeb5fa84a1e.
[35] Zak Doffman, 'Black Lives Matter: US Protesters Tracked by Secretive Phone Location Technology', *Forbes* (online, 26 June 2020) https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/?sh=6eeb5fa84a1e.
[36] Lorenzo Franceschi-Bicchierai, 'Firm That Tracked Protesters Targeted Evangelicals During 2016 Election', *Vice* (online, 27 June 2020) https://www.vice.com/en/article/9353qv/mobilewalla-tracked-protesters-targeted-evangelicals-during-2016-election.
[37] Lorenzo Franceschi-Bicchierai, 'Firm That Tracked Protesters Targeted Evangelicals During 2016 Election', *Vice* (online, 27 June 2020) https://www.vice.com/en/article/9353qv/mobilewalla-tracked-protesters-targeted-evangelicals-during-2016-election.
[38] *Privacy Act 1988* (Cth) s 6 'sensitive information'.
[39] ACCC, '*Digital Platforms Inquiry – Final Report*' (Commonwealth of Australia, Final Report, July 2019) 401–428.
[40] Deloitte, 'The Symbiotic Relationship: Getting the Balance Right', in *Australia Privacy Index 2018* (Deloitte, Report) 8.
[41] Deloitte, 'The Symbiotic Relationship: Getting the Balance Right', in *Australia Privacy Index 2018* (Deloitte, Report) 16.
[42] Consumer Policy Research Centre, '*Duped by Design – Manipulative online design: Dark patterns in Australia*' (Paper, June 2022) 6.
[43] Consumer Policy Research Centre, '*In whose interest? Why businesses need to keep consumers safe and treat their data with care*' (Working Paper, March 2023) 4.
[44] Li Li, et al., 'I will only know after using it: The repeat purchasers of smart home appliances and the privacy paradox problem' 128 *Computers & Security* (2023) 1.
[45] Consumer Policy Research Centre, '*2020 Data and Technology Consumer Survey*' (Survey, December 2020) 33.
[46] Consumer Policy Research Centre, '*2020 Data and Technology Consumer Survey*' (Survey, December 2020) 26.
[47] Lik-Hang Lee, et al., 'All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda' 2021 *arXIV* 37.

[48] Lik-Hang Lee, et al., 'All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda' 2021 *arXIV* 37.
[49] Lik-Hang Lee, et al., 'All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda' 2021 *arXIV* 37.
[50] Li Li, et al., 'I will only know after using it: The repeat purchasers of smart home appliances and the privacy paradox problem' 128 Computers & Security (2023) 1.
[51] ACCC, '*Digital Platform Services Inquiry – September 2023 Report on the expanding ecosystems of digital platform service providers*' (Commonwealth of Australia, Issues Paper, March 2023) 7 citing ACCC, *Digital Platform Services Inquiry Fifth Interim Report* (Commonwealth of Australia, Firth Interim Report, 11 November 2022) 44.
[52] ACCC, '*Digital Platform Services Inquiry – September 2023 Report on the expanding ecosystems of digital platform service providers*' (Commonwealth of Australia, Issues Paper, March 2023) 7-8.
[53] Consumer Policy Research Centre, '*In whose interest? Why businesses need to keep consumers safe and treat their data with care*' (Working Paper, March 2023) 4 citing Anthony Nadler & Lee McGuigan, 'An impulse to exploit: the behavioral turn in data-driven marketing' 35(2) *Critical Studies in Media Communication* (2018) 151-165.
[54] Consumer Policy Research Centre, '*In whose interest? Why businesses need to keep consumers safe and treat their data with care*' (Working Paper, March 2023) 4.
[55] Consumer Policy Research Centre, '*In whose interest? Why businesses need to keep consumers safe and treat their data with care*' (Working Paper, March 2023) 10 citing Jack Balkin, 'The fiduciary model of privacy' 134(11) *Harvard Law Review Forum* (2020) 12.
[56] OAIC, '*APP Guidelines*' (website, July 2019) [B.37]-[B.58].
[57] Australian Law Reform Commission (2014) '*Equality, Capacity and Disability in Commonwealth Laws*' (ALRC Report 124), p.24
[58] AHRC, '*Human Rights and Technology Final Report 2021*' ('Final Report') (Commonwealth of Australia, Final Report, 2021) see e.g. recommendations 2, 9 & 15.
[59] AHRC, Final Report (Final Report, 2021) 111; see e.g. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN doc A/HRC/41/35 (28 May 2019); Office of the Australian Information Commissioner, *'Australian Community Attitudes to Privacy Survey 2020*' (Commonwealth of Australia, Survey, 2020) 81.
[60] Roundtree, '*Facial Recognition Technology Codes of Ethics: Content Analysis and Review*' 211-220.
[61] AHRC, Final Report (Final Report, 2021) 113 citing Josh Bavas, 'Facial Recognition Quietly Switched on at Queensland Stadiums, Sparking Privacy Concerns,' *ABC News* (online, 6 June 2019); Josh Bavas, 'The Facial Recognition Security Issue Police Tried to Keep Secret', *ABC News* (online, 6 May 2019); Lisa Neville MP, 'New Police Eye in the Sky to Keep Victorians Safe' (Media Release, 10 July 2019); see, for example, Samantha Dick, 'Perth's Facial Recognition Cameras Prompt Scowls - And a Campaign to Stop 'Invasive' Surveillance', *The New Daily* (online, 1 February 2020); Sarah Basford, 'Australian Schools Have Been Trialling Facial Recognition Technology Despite Serious Concerns About Children's Data', *Gizmodo* (online, 10 March 2020).
[62] See e.g. Jarni Blakkarly, 'Kmart, Bunnings and The Good Guys using facial recognition technology in stores' *CHOICE* (online, last updated 12 July 2022); There is a growing amount of literature on the use of facial recognition in a range of settings including sports stadiums, schools and retail outlets in Australia. See Brett Hutchins and Mark Andrejevcic, 'Olympian Surveillance: Sports Stadiums and the Normalization of Biometric Monitoring' (2021) 15 *International Journal of Communication*, 363; See Josh Bavas, 'Facial Recognition Quietly Switched on at Queensland Stadiums, Sparking Privacy Concerns,' *ABC News* (online, 6 June 2019); Mark Andrejevic and Neil Selwyn, 'Facial Recognition Technology in Schools: Critical Questions and Concerns' (2020) 45(2) *Learning, Media and Technology*, 115; Sarah Basford,

'Australian Schools Have Been Trialling Facial Recognition Technology Despite Serious Concerns About Children's Data', *Gizmodo* (online, 10 March 2020); Rick Sarre, 'Facial Recognition Technology is Expanding Rapidly Across Australia. Are Our Laws Keeping Pace?' The Conversation (online, 10 July 2020) ; Eden Gillespie, 'Are You Being Scanned? How Facial Recognition Technology Follows You, Even as You Shop', *The Guardian* (online, 24 February 2019).

[63] K.W Miller, 'Facial Recognition Technology: Navigating the Ethical Challenges' (2023) 56(1) *Computer* 76.

[64] Roundtree, '*Facial Recognition Technology Codes of Ethics: Content Analysis and Review*' 211-220.

[65] Roundtree, '*Facial Recognition Technology Codes of Ethics: Content Analysis and Review*'218.

[66] See generally Genia Kostka, Lea Steubacker & Miriam Meckel 'Under big brothers watchful eye: Cross-country attitudes towards facial recognition technology' (2023) 40(1) *Government Information Quarterly*.

[67] Genia Kostka, Lea Steubacker & Miriam Meckel 'Under big brothers watchful eye: Cross-country attitudes towards facial recognition technology' (2023) 40(1) *Government Information Quarterly* 1 citing Feldstien, S, 'The Global Expansion of AI Surveillance' *Carnegie Endowment for International Peace* (September 2019).

[68] K.W Miller, 'Facial Recognition Technology: Navigating the Ethical Challenges' (2023) 56(1) *Computer* 76.

[69] Sanjeev Kumar, 'Delhi: Facial recognition system helps trace 3,000 missing children in 4 days' *The New India Express*, (online, 22 April 2018) https://www.newindianexpress.com/nation/2018/apr/22/3000-missing-children-traced-in-four-days-by-delhi-police-with-facial-recognition-system-software-1804955.html.

[70] Julie Zaugg, 'India is trying to build the world's biggest facial recognition system' *CNN Business* (online, 18 Oct 2019) https://edition.cnn.com/2019/10/17/tech/india-facial-recognition-intl-hnk/index.html.

[71] See e.g. the right to respect for the family as provided for under art 23.1 ICCPR; see also art 10 International Covenant on Economic, Social and Cultural Rights.

[72] Alexandra Ulmer & Zeba Siddiqui, 'India's use of facial recognition tech during protests causes stir' *Reuters* (online, 17 February 2020) https://www.reuters.com/article/us-india-citizenship-protests-technology-idUSKBN20B0ZQ.

[73] Genia Kostka, Lea Steubacker & Miriam Meckel 'Under big brothers watchful eye: Cross-country attitudes towards facial recognition technology' (2023) 40(1) *Government Information Quarterly* 1 citing Feldstien, S, 'The Global Expansion of AI Surveillance' *Carnegie Endowment for International Peace* (September 2019).

[74] James Leibold, 'Surveillance in China's Xinjiang region: Ethnic sorting, coercion, and inducement' *Journal of Contemporary China* (2020) 29(121) 46-60.

[75] Office of the United Nations High Commissioner for Human Rights, *OHCHR Assessment of human rights concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China* (31 August 2022), [96]. <https://www.ohchr.org/en/documents/country-reports/ohchr-assessment-human-rights-concerns-xinjiang-uyghur-autonomous-region>.

[76] Genia Kostka, Lea Steubacker & Miriam Meckel 'Under big brothers watchful eye: Cross-country attitudes towards facial recognition technology' (2023) 40(1) *Government Information Quarterly* 13.

[77] Genia Kostka, Lea Steubacker & Miriam Meckel 'Under big brothers watchful eye: Cross-country attitudes towards facial recognition technology' (2023) 40(1) *Government Information Quarterly* 13.

[78] Genia Kostka, Lea Steubacker & Miriam Meckel 'Under big brothers watchful eye: Cross-country attitudes towards facial recognition technology' (2023) 40(1) *Government Information Quarterly* 13.
[79] Jarni Blakkarly, 'Kmart, Bunnings and The Good Guys using facial recognition technology in stores' *CHOICE* (online, last updated 12 July 2022).
[80] Office of the Australian Information Commissioner, *'OAIC Opens Investigations into Bunnings and Kmart*' (Media Statement, 12 July 2022).
[81] Jarni Blakkarly, 'Kmart, Bunnings and The Good Guys using facial recognition technology in stores' *CHOICE* (online, last updated 12 July 2022); see also Amy Periera, '*Complaint OAIC on Use of Facial Recognition*' (CHOICE, Submission, June 2022).
[82] See generally Human Technology Institute, '*Facial Recognition Technology Towards a Model Law*' ('Model Law') (University of Technology Sydney, Report, September 2022) https://www.uts.edu.au/human-technology-institute/projects/facial-recognition-technology-towards-model-law.
[83] AHRC, Final Report (Final Report, 2021) 119.
[84] Human Technology Institute, Model Law (University of Technology Sydney, Report, September 2022) https://www.uts.edu.au/human-technology-institute/projects/facial-recognition-technology-towards-model-law.
[85] See generally Yilun Wang & Michal Kosinski, 'Deep Neural Networks are more Accurate than Humans at Detecting Sexual Oreintation from Facial Images' (2018) 114(2) *Journal of Personality and Social Psychology* 246-257.
[86] See generally Michal Kosinski, ' Facial Recognition Technology can Expose Political Oreintation from Naturalistic Facial Images' (2021) 11(100) *Nature Scientific Reports*.
[87] ILGA World: Lucas Ramon Mendos, Kellyn Botha, Rafael Carrano Lelis, Enrique López de la Peña, Ilia Savelev and Daron Tan, '*State-Sponsored Homophobia 2020: Global Legislation Overview Update*' (Geneva: ILGA, December 2020) 25.
[88] Yilun Wang & Michal Kosinski, 'Deep Neural Networks are more Accurate than Humans at Detecting Sexual Oreintation from Facial Images' (2018) 114(2) *Journal of Personality and Social Psychology* 246.
[89] Toby Walsh, '*Machines Behaving Badly: The Morality of AI*' (Black Inc, Melbourne, 2022) 200-201.
[90] Yilun Wang & Michal Kosinski, 'Deep Neural Networks are more Accurate than Humans at Detecting Sexual Oreintation from Facial Images' (2018) 114(2) *Journal of Personality and Social Psychology* 1.
[91] AHRC, Final Report (Final Report, 2021) 114.
[92] AHRC, Final Report (Final Report, 2021) 114.
[93] AHRC, Final Report (Final Report, 2021) 114; Pete Fussey and Daragh Murray, '*Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*' (Human Rights, Big Data and Technology Project, July 2019) 36.
[94] AHRC, Final Report (Final Report, 2021) 114.
[95] AHRC, Final Report (Final Report, 2021) 115; See David Pozen, 'The Mosaic Theory, National Security, and the Freedom of Information Act' (2005) 115 *Yale Law Journal* 628.
[96] AHRC, Final Report (Final Report, 2021) 115; *Report of the Special Rapporteur on the Right to Privacy*, UN Doc A/HRC/40/63 (27 February 2019) 3.
[97] AHRC, Final Report (Final Report, 2021) 115; See e.g. Human Rights Watch, '*China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*' (Report, 1 May 2019).
[98] Bobby Allyn, 'The Computer Got It Wrong': How Facial Recognition Led To False Arrest Of Black Man' *NPR* (online, 24 June 2020) https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig#:~:text=Bobby%20Allyn-

,'The%20Computer%20Got%20It%20Wrong'%3A%20How%20Facial%20Recognition%20Led,False%20Arrest%20Of%20Black%20Man&text=Police%20in%20Detroit%20were%20trying,estimated%20%243%2C800%20worth%20of%20merchandise.

[99] See e.g. Joy Buolamwini and Timinit Guru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 *Proceedings of Machine Learning Research* 1; KS Krishnapriya, Kushal Vangara, Michael C King, Vitor Albiero and Kevin Bowyer, 'Characterizing the Variability in Face Recognition Accuracy Relative to Race' (Conference Paper, IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 2019); Inioluwa Deborah Raji and Joy Buolamwini, 'Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products' (Conference on Artificial Intelligence, Ethics, and Society, 2019).

[100] Larry Magid, 'IBM, Microsoft And Amazon Not Letting Police Use Their Facial Recognition Technology' *Forbes* (online, 12 June 2020) https://www.forbes.com/sites/larrymagid/2020/06/12/ibm-microsoft-and-amazon-not-letting-police-use-their-facial-recognition-technology/?sh=15a148191887.

[101] Toby Walsh, '*Machines Behaving Badly: The Morality of AI*' (Black Inc, Melbourne, 2022) 195.

[102] Ryan Mac, et al., 'Surveillance Nation' *Buzzfeed News* (online, April 6 2021) https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition.

[103] OAIC, '*Clearview AI breached Australians' privacy*' (Media Release, 03 November 2021).

[104] OAIC, '*OAIC and ICO conclude joint investigation into Clearview AI*' (Media Release, 03 November 2021).

[105] OAIC, '*Clearview AI breached Australians' privacy*' (Media Release, 03 November 2021).

[106] Ryan Mac, et al., 'Surveillance Nation' *Buzzfeed News* (online, April 6 2021) https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition; Ed Markey, '*Senators Markey, Merkley lead colleagues on legislation to ban government use of facial recognition, other biometric technology*' (Press Release, 15 June 2021).

[107] John Tobin (ed), *The UN Convention on the Rights of the Child* (OUP, 2019), 570.

[108] Committee on the Rights of the Child, General Comment No. 25 (2021) UN Doc CRC/C/GC/25 ('CRC General Comment 25') 68.

[109] CRC General Comment 25 68.

[110] Committee on the Rights of the Child, General Comment No. 16 (2013) CRC/C/GC/16 12.

[111] Human Rights Council, *Report of the Special Rapporteur on the Right to Privacy*, Joseph Cannataci, on Artificial Intelligence and Privacy, and Children's Privacy (2021) UN Doc A/HRC/46/37 [72].

[112] ACCC, '*Digital Platforms Inquiry – Final Report*' (Commonwealth of Australia, Report, 2019) 447-448.

[113] OAIC, '*Privacy Tips for Parents and Carers*' OAIC website.

[114] CRC General Comment 25 14-15.

[115] Antonia Quadara, Alissar El-Murr and Joe Latham, '*The effects of pornography on children and young people*' (Australian Institute of Family Studies, December 2017).

[116] Our Watch, '*Pornography, young people and preventing violence against women*' (Background Paper, 2020) 14.

[117] Our Watch, '*Pornography, young people and preventing violence against women*' (Background Paper, 2020) 14.

[118] CRC General Comment 25 9-11.

[119] CRC General Comment 25 9-11.

[120] Human Rights Council, *Report of the Special Rapporteur on the Right to Privacy*, Joseph Cannataci, on Artificial Intelligence and Privacy, and Children's Privacy (2021) UN Doc A/HRC/46/37 91.
[121] OAIC Submission to the Discussion Paper 120.
[122] OAIC Submission to the Discussion Paper 120.
[123] OAIC Submission to the Discussion Paper 120.
[124] Human Rights Watch, *'How Dare They Peep into My Private Life? Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic*' (Report, 25 May 2022).
[125] Human Rights Watch, *'How Dare They Peep into My Private Life? Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic*' (Report, 25 May 2022).
[126] Human Rights Watch, *'How Dare They Peep into My Private Life? Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic*' (Report, 25 May 2022).
[127] Human Rights Watch, *'How Dare They Peep into My Private Life? Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic*' (Report, 25 May 2022).
[128] See e.g. Ben Williamson, 'Decoding Class Dojo: psycho-policy, social-emotional learning and persuasive educational technologies' (2017) 42(4) *Learning, Media and Technology* 440-453; see generally Jamie Manolev, Anna Sullivan & Roger Slee 'The datafication of discipline: ClassDojo, surveillance and a performative classroom culture' (2019) 44(1) *Learning, Media and Technology*; Ben Robinson, 'The ClassDojo app: training in the art of dividuation' (2021) 34(7) *International Journal of Qualitative Studies in Education;* Agata Soroko, 'No child left alone' (2016) 25(3) *Our Schools/Our Selves*; Daniela Kruel DiGiacomo, Spencer Greenhalgh & Sarah Barriage, 'How Students and Principals Understand ClassDojo: Emerging Insights' (2022) 66(2) *TechTrends* 172-184.
[129] H. Cook, 'It's all about controlling students': researchers slam popular app' *The Sydney Morning Herald* (online, 18 January 2019) https://www.smh.com.au/education/it-s-all-about-controlling-students-researchers-slam-popular-app-20190118-p50s8l.html
[130] Human Rights Watch, *'How Dare They Peep into My Private Life? Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic*' (Report, 25 May 2022).
[131] See e.g. Digital Futures Commission, '*Problems with data governance in UK schools – the cases of Google Classroom and ClassDojo*' (Report, 2022) 8.
[132] Human Rights Watch, *'How Dare They Peep into My Private Life? Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic*' (Report, 25 May 2022) observed 145 EdTech products directly sending or granting access to children's personal data to 196 third-party companies, overwhelmingly AdTech.
[133] Human Rights Watch, *'How Dare They Peep into My Private Life? Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic*' (Report, 25 May 2022).
[134] See generally Human Rights Watch, *'How Dare They Peep into My Private Life? Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic*' (Report, 25 May 2022).
[135] Digital Futures Commission, '*Problems with data governance in UK schools – the cases of Google Classroom and ClassDojo*' (Report, 2022) 8.
[136] UK Information Commission Office, *'Age appropriate design: a code of practice for online services*' (September 2020) 39-41, 61-62, 74-75, 81-82, 96-100.
[137] Human Rights Council, *Report of the Special Rapporteur on the Right to Privacy*, Joseph Cannataci, on Artificial Intelligence and Privacy, and Children's Privacy (2021) UN Doc A/HRC/46/37 127.
[138] John Tobin (ed), '*The UN Convention on the Rights of the Child*' (OUP, 2019), 55; see also CRC General Comment 25 17-18.

[139] CRC General Comment 25 17.
[140] CRC General Comment 25 12-13.
[141] CRC General Comment 2513.
[142] Human Rights Council, *Report of the Special Rapporteur on the Right to Privacy*, Joseph Cannataci, on Artificial Intelligence and Privacy, and Children's Privacy (2021) UN Doc A/HRC/46/37 116.
[143] CRC General Comment 25 75.
[144] Human Rights Council, *Report of the Special Rapporteur on the Right to Privacy*, Joseph Cannataci, on Artificial Intelligence and Privacy, and Children's Privacy (2021) UN Doc A/HRC/46/37 127.
[145] Human Rights Council, *Report of the Special Rapporteur on the Right to Privacy*, Joseph Cannataci, on Artificial Intelligence and Privacy, and Children's Privacy (2021) UN Doc A/HRC/46/37 127.
[146] CRC General Comment 25 42.
[147] Human Rights Council, *Report of the Special Rapporteur on the Right to Privacy*, Joseph Cannataci, on Artificial Intelligence and Privacy, and Children's Privacy (2021) UN Doc A/HRC/46/37 90.
[148] CRC General Comment 25 16-18.
[149] Human Rights Council, *Report of the Special Rapporteur on the Right to Privacy*, Joseph Cannataci, on Artificial Intelligence and Privacy, and Children's Privacy (2021) UN Doc A/HRC/46/37 80.
[150] Human Rights Council, *Report of the Special Rapporteur on the Right to Privacy*, Joseph Cannataci, on Artificial Intelligence and Privacy, and Children's Privacy (2021) UN Doc A/HRC/46/37 118.
[151] Position Paper 195-205
[152] Elena Martellozzo et al., '*I Wasn't Sure it Was Normal to Watch it: the Impact of Online Pornography on the Values, Attitudes, Beliefs and Behaviours of Children*' (NSPCC, Report, May 2017).
[153] Australian Law Reform Commission, '*Elder Abuse—A National Legal Response*' (ALRC Report 131, 2017) 15.
[154] Office of the Public Advocate, '*Line of sight: Refocussing Victoria's adult safeguarding laws and practices*' (State of Victoria, 2022) 7.
[155] The Public Advocate, '*Adult Safeguarding in Queensland: Volume 2*' Reform Recommendations (Queensland, 2022) 8.
[156] Submission to the Attorney-General's Department, Discussion Paper (Commonwealth of Australia, Discussion Paper, October): Energy and Water Ombudsman NSW 2 which submitted that it was critical that the significant vulnerability experienced due to family violence be included.
[157] Submission to the Attorney-General's Department, Discussion Paper (Commonwealth of Australia, Discussion Paper, October): Social Services Portfolio 26; OAIC 126 and Castan Centre 24 - both citing Normann Witzleb et al, '*Privacy risks and harms for children and other vulnerable groups in the online environment*' (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020).
[158] Attorney-General's Department, Review Report (Commonwealth of Australia, Report, February 2023) 160.
[159] Department of Social Services, '*NDIS Quality and Safeguarding Framework*' (2016) 31.
[160] Australian Law Reform Commission, '*Equality, Capacity and Disability in Commonwealth Laws*' (2014, ALRC Report 124).

[161] Royal Commission into Violence Abuse Neglect and Exploitation of People with Disability '*Diversity, dignity, equity and best practice: a framework for supported decision-making*' (2023).
[162] Attorney-General's Department, Review Report (Commonwealth of Australia, Report, February 2023) 200.
[163] See e.g. submissions to the Attorney-General's Department, Discussion Paper (Commonwealth of Australia, Discussion Paper, October): Calabash Solutions 19; Office of the Victorian Information Commissioner 8.
[164] See e.g. submissions to the Attorney-General's Department, Discussion Paper (Commonwealth of Australia, Discussion Paper, October): Calabash Solutions 19.
[165] Consumer Policy Research Centre, '*In whose interest? Why businesses need to keep consumers safe and treat their data with care*' (Working Paper, March 2023) 4 citing Consumer Policy Research Centre, '*Duped by Design – Manipulative online design: Dark patterns in Australia*' (Paper, June 2022) 6.
[166] Consumer Policy Research Centre, '*In whose interest? Why businesses need to keep consumers safe and treat their data with care*' (Working Paper, March 2023) 10 citing Jack Balkin, 'The fiduciary model of privacy' 134(11) *Harvard Law Review Forum* (2020) 12.
[167] *International Covenant on Civil and Political Rights* art 17 requires states to protect, in law, against the interference or attack on the 'arbitrary or unlawful interference' with an individual's 'privacy, family, home or correspondence'; *Universal Declaration of Human Rights* art 12 states that 'no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation'; AHRC, Position Paper (Position Paper, March 2023) sets out a right to privacy and reputation.
[168] AHRC, Final Report (Final Report, 2021) 120.
[169] AHRC, Final Report (Final Report, 2021) 47.
[170] *General Data Protection Regulation* (EU) art 22 provides for a right for a data subject not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
[171] AHRC, Final Report (Final Report, 2021) 12 & 39.
[172] AHRC, Final Report (Final Report, 2021) 41.
[173] AHRC, Final Report (Final Report, 2021) 43.
[174] AHRC, Final Report (Final Report, 2021) 43.
[175] UK Information Commissioner's Office, *What Does the UK GDPR Say About Automated Decision-making and Profiling* (website).
[176] UK Information Commissioner's Office, *What Does the UK GDPR Say About Automated Decision-making and Profiling* (website).
[177] Submissions to Attorney-General's Department, Discussion Paper (Commonwealth of Australia, Discussion Paper, October): Experian Australia 21; Woolworths Group 13; Ai Group 11; Business Council of Australia 11; The Australian Communications and Media Authority 4.
[178] Submissions to Attorney-General's Department, Discussion Paper (Commonwealth of Australia, Discussion Paper, October): Ai Group 11; Business Council of Australia 11.
[179] Max Schemmer, et al., '*On the Influence of Explainable AI on Automation Bias*' (Working Paper, 2022) 1 quoting Kathleen Mosier & Linda Skitka, 'Automation Use and Automation Bias' in Proceedings of the Human Factors and Ergonomics Society Annual Meeting 43(3) *SAGE Publications* (1999) 344–348.
[180] See e.g. Hilary Hanson, 'GPS Leads Japanese Tourists To Drive Into Australian Bay' Huffpost (Online, 19 March 2012) https://www.huffingtonpost.co.uk/entry/gps-tourists-australia_n_1363823.

[181] Schemmer 1 citing Eugenio Alberdi, et al., 'Effects of Incorrect Computer-Aided Detection (CAD) Output on Human Decision-Making in Mammography' 11(8) *Academic Radiology* (2004) 909–918.
[182] UK Information Commissioner's Office, *What Does the UK GDPR Say About Automated Decision-making and Profiling* (website).
[183] AHRC, Final Report (Final Report, 2021) 82.
[184] AHRC, Final Report (Final Report, 2021) 65.
[185] AHRC, Final Report (Final Report, 2021) 80.
[186] AHRC, Final Report (Final Report, 2021) 80.
[187] AHRC, Final Report (Final Report, 2021) 83.
[188] AHRC, Final Report (Final Report, 2021) 81.
[189] AHRC, Final Report (Final Report, 2021) 81.
[190] AHRC, Final Report (Final Report, 2021) 81.
[191] AHRC, Final Report (Final Report, 2021) 66.
[192] Commonwealth Ombudsman, *Centrelink's Automated Debt Raising and Recovery System: A report About the Department of Human Services' Online Compliance Intervention System for Debt Raising and Recovery* (April 2017).
[193] AHRC, '*Centrelink's compliance program*' submission to Senate Community Affairs References Committee regarding its inquiry into 'Centrelink's compliance program'.
[194] AHRC, '*Centrelink's compliance program*' submission to Senate Community Affairs References Committee regarding its inquiry into 'Centrelink's compliance program' 5.
[195] AHRC, Final Report (Final Report, 2021) 42.
[196] Commonwealth Ombudsman, *Centrelink's Automated Debt Raising and Recovery System: A report About the Department of Human Services' Online Compliance Intervention System for Debt Raising and Recovery* (April 2017).
[197] Alexandria Utting, 'Kathleen Madgwick tells Robodebt royal commission about her son Jarrad and the damage the scheme caused' ABC News (online, 10 March 2023) https://www.abc.net.au/news/2023-03-10/qld-robodebt-scheme-government-royal-commission-fraud/102027838.
[198] AHRC, Final Report (Final Report, 2021) 80.
[199] AHRC, Final Report (Final Report, 2021) 13.
[200] AHRC, Final Report (Final Report, 2021) 62.
[201] AHRC, Final Report (Final Report, 2021) 13.
[202] AHRC, Final Report (Final Report, 2021) 13.
[203] AHRC, Final Report (Final Report, 2021) 13.
[204] AHRC, Final Report (Final Report, 2021) 13.
[205] Rachel Goodman, 'Why Amazon's Automated Hiring Tool Discriminated Against Women', *American Civil Liberties Union* (online, 12 October 2018) https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against.
[206] Rachel Goodman, 'Why Amazon's Automated Hiring Tool Discriminated Against Women', *American Civil Liberties Union* (online, 12 October 2018) https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against.
[207] Rachel Goodman, 'Why Amazon's Automated Hiring Tool Discriminated Against Women', *American Civil Liberties Union* (online, 12 October 2018) https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against.
[208] Crystal Grant, 'Algorithms are Making Decisions About Health Care, Which May Only Worsen Medical Racism' *American Civil Liberties Union* (online, 3 October 2022) https://www.aclu.org/news/privacy-technology/algorithms-in-health-care-may-worsen-medical-racism.

[209] Crystal Grant, 'Algorithms are Making Decisions About Health Care, Which May Only Worsen Medical Racism' *American Civil Liberties Union* (online, 3 October 2022) https://www.aclu.org/news/privacy-technology/algorithms-in-health-care-may-worsen-medical-racism.

[210] Crystal Grant, 'Algorithms are Making Decisions About Health Care, Which May Only Worsen Medical Racism' *American Civil Liberties Union* (online, 3 October 2022) https://www.aclu.org/news/privacy-technology/algorithms-in-health-care-may-worsen-medical-racism.

[211] AHRC, Final Report (Final Report, 2021) 108.

[212] AHRC, Position Paper (Position Paper, March 2023) 24.

[213] See e.g. Attorney-General's Department, Discussion Paper (Commonwealth of Australia, Discussion Paper, October) 193.

[214] Submissions to the Attorney-General's Department, Discussion Paper (Commonwealth of Australia, Discussion Paper, October): Australia's Right to Know 1; Guardian Australia 21; SBS 12-13; Commercial Radio Australia 3.

[215] Submission to the Attorney-General's Department, Discussion Paper (Commonwealth of Australia, Discussion Paper, October): Guardian Australia 21.

[216] See e.g. Submission to the Attorney-General's Department, Discussion Paper (Commonwealth of Australia, Discussion Paper, October): Guardian Australia 21.

[217] Attorney-General's Department, Review Report (Commonwealth of Australia, Report, February 2023) 286.

[218] Sammy Gecsoyer, 'Rebel Wilson speaks about threat to be outed: "It was grubby behaviour"' *The Guardian* (online, 21 October 2022) https://www.theguardian.com/film/2022/oct/20/rebel-wilson-speaks-out-about-being-outed.

[219] AHRC, Final Report (Final Report, 2021) 123.

[220] Submission to the Attorney-General's Department, Discussion Paper (Commonwealth of Australia, Discussion Paper, October): Castan Centre 56-57.

[221] AHRC, Final Report (Final Report, 2021) 123.

[222] Hemant Taneja, 'The Era of "Move Fast and Break Things" Is Over' *Harvard Business Review* (online, 22 January 2019) https://hbr.org/2019/01/the-era-of-move-fast-and-break-things-is-over