MONASH University

Submission to Australian Human Rights Commission
Human Rights and Technology Project

by Dr Normann Witzleb, Associate Professor, Monash University, Faculty of Law

The right to privacy of young people in an interconnected world

Preliminary observations

1 Based on my particular expertise and current academic work, my submission focuses on the effect that new technologies have on the human rights of children and young people, in particular their right to privacy. The following submission is therefore directed at consultation questions 1 to 3, which identify the following issues:

(1) What types of technology raise particular human rights concerns? Which human rights are particularly implicated?

(2) Noting that particular groups within the Australian community can experience new technology differently, what are the key issues regarding new technologies for these groups of people (such as children and young people; older people; women and girls; LGBTI people; people of culturally and linguistically diverse backgrounds; Aboriginal and Torres Strait Islander peoples)?

(3) How should Australian law protect human rights in the development, use and application of new technologies? In particular: (a) What gaps, if any, are there in this area of Australian law? (b) What can we learn about the need for regulating new technologies, and the options for doing so, from international human rights law and the experiences of other countries? (c) What principles should guide regulation in this area?

2 The views expressed in this submission are mine and do not necessarily reflect the policies or opinions of Monash University.

Types of technology that raise particular human rights concerns and their effect on children and young people

3 New technologies are adopted at an unprecedented rate and increasingly permeate most aspects of social, home and personal life. Today's **children and young people** grow up in an **increasingly interconnected world**. Many technological developments do not focus

primarily on children and young people, yet minors are often no less affected by these innovations than adults. Social media platforms, such as Instagram, YouTube and WhatsApp, are open to adults and teenagers alike – but it is no secret that, due to lax enforcement of age limits, also a significant number of pre-teens (children below 13 years of age) use these platforms.[1] There are also a range of new services and technologies that are specifically marketed to, or predominantly used by, children and young people. Apart from social media services which have a disproportionately young audience (eg., Snapchat or Tiktok/musical-ly), this includes many applications in the fields of education, entertainment and child care. Such services or technologies, in particular where they are smart and connected, generate huge amounts of personal information about their users' characteristics or social interactions, including – depending on their functionality and use – their educational progress, consumer behaviour, and health and well-being.

4 While **social media platforms and the Internet of Things** (IoT) can offer major benefits, the social and legal norms around these technological advances are still in development. Connected devices can educate, entertain and protect children, but the ill-considered exposure to constant monitoring and analysis may also have detrimental effects on a young person's social and personal development.[2] Notwithstanding that today's youth are in many ways more intuitive and adept in mastering the digital environment than previous generations, they remain exposed to the risks and challenges of the online world. Where technologies are still developing, as is the case with the IoT, Big Data analytics and Artificial Intelligence (AI), the risks and opportunities associated with them take time to be fully understood. Regulation needs to tread a careful line that neither stifles innovation and progress nor exposes users to undue risk of harm.[3] This requires policy-makers, parents and children themselves to be particular vigilant so that both the possible benefits arising from these technologies and their associated dangers are appropriately weighted and balanced against each other.

5 As indicated, areas in which the human rights of children deserve particular attention include the field of online services and – as areas of emerging concern – **education, entertainment and smart homes**. In the last few years, there has already been substantial engagement with the risks and opportunities arising from children accessing social media or other online services.[4] Australia has responded to some of the concerns arising by

[1] Anthony D Miyazaki , Andrea JS Stanaland and May O Lwin, 'Self-Regulatory Safeguards and the Online Privacy of Preteen Children' (2009) 38 *Journal of Advertising* 79-91, DOI: 10.2753/JOA0091-3367380406.
[2] Kathryn C Montgomery, 'Youth and surveillance in the Facebook era: Policy interventions and social implications' (2015) 39 *Telecommunications Policy* 771, DOI: 10.1016/j.telpol.2014.12.006.
[3] See, for example, the discussion in Productivity Commission, *Data Availability and Use,* Report No. 82, 2017 Canberra; Bart van der Sloot, Dennis Broeders and Erik Schrijvers (eds), *Exploring the Boundaries of Big Data*, 2016, Amsterdam: Amsterdam University Press.
[4] For example, Australian Parliament, Joint Select Committee on Cyber-Safety, High-wire act: Cyber-safety and the young, Interim report, 2011, Canberra, ACT: Commonwealth of Australia, available at <http://www.aph.gov.au/parliamentarybusiness/committees/houseofrepresentativescommittees?url=jscc/report.htm>.

improving its regulatory frameworks and educational approaches towards harmful digital communications, including cyber-bullying and sexting.[5] However, the digital rights of children in the context of IoT, Big Data analytics and AI require further attention.

6 Discussion and policy development of privacy protection of students in educational settings is still in its early stages, and often focuses on overseas experiences.[6] Digital monitoring of students via **classroom management software and education apps**, combined with sophisticated 'learning analytics', track students' educational progress and learning outcomes.[7] These technologies are increasingly in use in many schools and universities, as are surveillance systems that monitor the attendance, movements and social media engagement of students in school and in class.[8] While the adoption of these innovative technologies promises enhanced safety, improved efficiencies and better educational outcomes, these benefits are countered by concerns about inappropriate commercialisation, commodification and habitualisation of surveillance that undermine young people's privacy, freedom of speech and other digital rights.[9] As a result, there are is still little consensus – internationally or domestically – about their appropriate usages, and the regulatory responses governing their implementation still require further research and attention.[10]

7 Similarly, there is an emerging discussion of the risks posed by **smart and connected toys**.[11] Many of these are mainly marketed at the parents of younger children and include stuffed animals, dolls and other characters equipped with microphone, speaker, video recording facilities which connect to a cloud service, usually via a companion app on a

[5] This includes the establishment of the Office of the eSafety Commissioner and other initiatives.
[6] For example, Valerie Steeves, Priscilla Regan and Leslie Regan Shade, 'Digital Surveillance in the Networked Classroom', in J Deakin et al. (eds), The Palgrave International Handbook of School Discipline, Surveillance, and Social Control, doi:10.1007/978-3-319-71559-9_23.
[7] Jason M Lodge and Linda Corrin, 'What data and analytics can and do say about effective learning' (2017) 2 *Science of Learning*, doi:10.1038/s41539-017-0006-5.
[8] Ben Williamson, 'Calculating children in the dataveillance school: Personal and learning analytics', in: E. Taylor and T. Rooney (eds), *Surveillance futures: Social and ethical implications of new technologies for children and young people*, 2017, London and New York: Routledge, 50–66; Alexis M Peddy, 'Dangerous Classroom "App"-titude: Protecting Student Privacy from Third-Party Educational Service Providers' (2017) *BYU Educationa and Law Journal* 125; available at <http://digitalcommons.law.byu.edu/elj/vol2017/iss1/5>.
[9] Leslie Regan Shade and Rianka Singh, '"Honestly, We're Not Spying on Kids": School Surveillance of Young People's Social Media' (2016) Social Media and Society, doi.org/10.1177/2056305116680005.
[10] David Rosen and Aaron Santesso, 'School Surveillance and Privacy' in J Deakin et al. (eds), in *The Palgrave International Handbook of School Discipline, Surveillance, and Social Control* (2018), doi.org/10.1007/978-3-319-71559-9_25; Amanda O'Keefe, 'Why we need a broader conversation about ed-tech privacy', *IAPP News* (28 September 2018), available at <https://iapp.org/news/a/why-a-broader-conversation-about-ed-tech-privacy-is-needed/>.
[11] For example, Donell Holloway and Lelia Green, 'The Internet of toys' (2016) 2 *Communication Research and Practice* 506–519, doi: 10.1080/22041451.2016.1266124; Giovanna Mascheroni and Donell Holloway (eds), *The Internet of Toys: A report on media and social discourses around young children and IoToys*, 2017, DigiLitEY.

mobile phone.[12] Products for older children include programmable devices, robotic sets and location trackers. Some smart toys developed in recent years were subject to well-publicised hacks (Barbie in 2015; VTech 2015; Cayla dolls in late 2016),[13] exposing security flaws in the protection of personal information of parents and children.

8 Another emerging field in which the right to respect for one's privacy and family life is at issue are **wearable devices and the automated home**. The utilization of smart technologies, including IoT and AI, has the potential the radically transform our home life, consumer behaviour and social interaction.[14] The major technology companies (Apple, Amazon, Alphabet/Google and Samsung) consider these technologies to hold enormous promise, and all of them seek to establish themselves and their products in this potentially enormous market as early leaders. These devices collect detailed profiles of personal information (including sensitive health-related information) about their users, yet it remains in many ways unclear how such data is stored, utilised and commercialised by the technology providers and the creators of particular applications.[15]

9 In all these fields, there is a developing international discussion of the benefits and risks of new technologies. Informed debate in Australia should take account of the international developments, yet give due recognition to the specifics of the **Australian context**, which includes our particular regulatory approaches, cultural sensibilities and societal aspirations.

Which human rights are particularly implicated?

10 The human right that is most immediately affected by the increasing datafication of many aspects of our lives, including the lives of children and young people, is the **right to privacy and data protection**.[16] All the above-mentioned technologies build on, or lead to, the accumulation of vast amounts of user data. Where such data is about an identified or potentially identifiable individual, it is 'personal information' that is subject to privacy laws.[17] In Australia, there continue to exist significant uncertainties around the definition

[12] Stéphane Chaudron et al., *Kaleidoscope on the Internet of Toys - Safety, security, privacy and societal insights*, 2017, Luxembourg: Publications Office of the European Union, EUR 28397 EN, doi:10.2788/05383.
[13] Eg. The internet of toys – the impact on children of a connected environment, Interview with John Carr, (2017) 2 *Journal of Cyber Policy* 227–231, doi.org/10.1080/23738871.2017.1355401.
[14] Carsten Maple, Security and privacy in the internet of things, (2017) 2 *Journal of Cyber Policy* 155–184, doi.org/10.1080/23738871.2017.1366536
[15] Tony Anscombe, *IoT and Privacy by Design in the Smart Home*, available at <https://www.welivesecurity.com/wp-content/uploads/2018/02/ESET_MWC2018_IoT_SmartHome.pdf>.
[16] Deborah Lupton and Ben Williamson, The datafied child: The dataveillance of children and implications for their rights (2017) 19 *New Media & Society* 780–794.
[17] *Privacy Act 1998* (Cth), s 6(1).

of personal information, in particular where information is supposedly de-identified.[18] As a result, the scope of application of privacy laws remains surprisingly unclear.

11 **Privacy rights** are concerned with controlling the flow of information about oneself. They are **protective and facilitative**, which means that an individual must be free to give up aspects of their privacy if they so choose, in particular if they perceive to gain benefits from doing so. As such, users of social networking sites may choose to give up privacy to obtain the benefits of the services provided by these sites. Similarly, users of IoT devices may give up privacy to obtain the benefits of convenience, entertainment, safety and individualised interaction that IoT applications provide. However, the rise of Big Data analytics and its potential to use data in new and unexpected make it increasingly doubtful whether users can really assess the uses to which their data might be put, and hence whether their **consent** is **fully informed and freely given**.[19]

12 Privacy is, of course, not an absolute right. It is a social construct and a contested concept. In practical terms, privacy will only be legally protected if it outweighs **countervailing interests and conflicting rights** held by others. Countervailing rights include freedom of expression and the commercial interests of those who seek to develop and market new technologies. In the case of rights, conflicting human rights positions need to be resolved by reference to considerations of **proportionality**, i.e. that each human right is only limited as far as is necessary for the protection of the conflicting human rights. In jurisdictions that lack a human rights framework in their domestic law, like Australia, this balancing exercise needs to be undertaken in the context of existing statutory and common law regulation, but requires that such laws are sufficiently open-textured to allow for conflicting human rights positions to be considered.

Relevant gaps in Australian law

The lack of a statutory privacy tort

13 As indicated above, this submission focuses on the protection of **privacy as one several key human rights** that are affected by modern technology.

14 Australia is signatory to a number of international instruments which enshrine the right to respect for one's private life, including the *International Covenant on Civil and Political*

[18] Normann Witzleb and Julian Wagner, 'When is Personal Data "About" or "Relating to" an Individual? A Comparison of Australian, Canadian, and EU Data Protection and Privacy Law' (2018) 4 *Canadian Journal of Comparative and Contemporary Law* 293–329.

[19] Solon Barocas and Helen Nissenbaum, 'Big Data's End Run around Anonymity and Consent', in: J Lane, V Stodden, S Bender, H Nissenbaum (eds), Privacy, Big Data, and the Public Good Frameworks for Engagement 44–75.

Rights.[20] Yet, the legal **protection of privacy** and personal information in Australian domestic law remains **piece-meal and incomplete**. Information privacy is protected mainly through statute law, in particular the federal *Privacy Act 1988* (Cth) and equivalents in the majority of Australian states and territories. The *Privacy Act 1988*, which applies to most Commonwealth government agencies and private sector organisations, adopts a principles-based, rather than a prescriptive, approach to data protection. It contains 13 Australian Privacy Principles (the APPs), which govern the collection, use, disclosure and store personal and sensitive information, and how individuals may access and correct records containing such information.

15 Unlike most other legal systems, including Canada, New Zealand and the UK, the right to privacy is not in itself protected in Australian domestic law. In the **absence of a common law right to privacy**, the law of torts, copyright legislation and the equitable doctrine of breach of confidence can provide a remedy in certain circumstances. Civil claims for breach of privacy are available only if, and as far as, other civil causes of action coincidentally cover conduct that affects privacy.[21] But the cost and delay involved with potential litigation mean that civil redress will in practice be sought only in exceptional circumstances. The complaints mechanisms available under the *Privacy Act 1988* (Cth), and its equivalents in most states and Territories, are more accessible to individual complainants but have significant gaps in their coverage.

16 To address this deficiency, the Australian Law Reform Commission (ALRC) has repeatedly called for a statutory cause of action for serious invasion of privacy in federal legislation.[22] A **statutory privacy tort** would provide victims of privacy invasion with a direct civil action for redress. The tort proposed by the ALRC would focus on 'intrusion into seclusion', i.e. the interference into physical sphere of privacy, and 'misuse of private information', the wrongful obtaining or publication of private information.[23] The ALRC recommended that the tort should be confined to intentional or reckless invasions of privacy, so that negligent invasions of privacy would not be actionable, and be subject to a requirement that the invasion must be serious.[24] Importantly, the proposed cause of action would only be satisfied if the public interest in privacy outweighed any countervailing public interests.[25] This requirement for a balancing exercise would ensure that freedom of

[20] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171, entered into force 23 March 1976.
[21] *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63, (2001) 208 CLR 199.
[22] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report 123, 2014, Canberra: ALRC; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108, 2008, Canberra: ALRC, Rec 74-1.
[23] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report 123, 2014, Canberra: ALRC, Rec 5-1.
[24] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report 123, 2014, Canberra: ALRC, Recs 7-1, 8-1.
[25] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report 123, 2014, Canberra: ALRC, Rec 9-1.

speech, freedom of the media, public health and safety, national security and other such public interests would not be disproportionately curtailed.

17 It has been the **consistent view** of all Australian law reform agencies and parliamentary enquiries that investigated the matter over the last decade that a **statutory privacy tort is needed**. Apart from the ALRC, a privacy tort was also recommended by the NSW Law Reform Commission,[26] the Victorian Law Reform Commission[27] and the South Australian Law Reform Institute.[28] Recently, the Law and Justice Committee of the NSW Legislative Council also supported the adoption of the ALRC privacy tort.[29]

18 I submit that these recommendations should now be implemented. A distinct privacy tort, introduced by legislation, would give visible recognition to the importance of privacy rights, and in doing so not only have an important **educative function**, but also give victims of privacy invasion an avenue of **individual redress**. The ALRC recommended a wide range of remedies, including damages, account of profits, injunctions, orders for delivery up, removal, correction or apology.[30] I also support the finding of the ALRC that access to justice would be enhanced if the Privacy Commissioner were given the power to investigate complaints about serious invasions of privacy.[31]

19 Australia has adopted a principles-based and technologically neutral approach to its privacy regulation. While this approach has the advantage of being adaptable over time, both in response to changing societal expectations and technological advancements, it has the drawback of creating uncertainty. Much depends on the interpretation of open-ended concepts by regulators, such as the Office of the Australian Information Commissioner, and the courts. In addition, there must be sufficiently **accessible procedures and adequate resourcing** to allow matters to be considered and resolved by the Commissioner in a timely and satisfactory way. While the powers of the Privacy Commissioner have recently been reviewed and expanded,[32] it continues to be the case that the data protection authorities in many comparable jurisdictions have greater

[26] New South Wales Law Reform Commission, *Invasion of Privacy*, Report 120, 2009, Sydney: NSW Law Reform Commission.
[27] Victorian Law Reform Commission, *Surveillance in Public Places*, Final Report 18, 2010, Melbourne: Victorian Law Reform Commission.
[28] South Australian Law Reform Institute, *Too much information - A statutory cause of action for invasion of privacy*, Final Report 4, 2014, Adelaide: South Australian Law Reform Institute.
[29] New South Wales (NSW), Legislative Council, Standing Committee for Law and Justice, *Remedies for the serious invasion of privacy*, Report 57, 2015, Sydney: Standing Committee for Law and Justice. See also Parliament of Victoria, Law Reform Committee, *Inquiry into Sexting: Report of the Law Reform Committee for the Inquiry into Sexting*, Parliamentary Paper No. 230, Session 2010-2013, 2013, Melbourne: Victorian Government Printer, Rec 12.
[30] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report 123, 2014, Canberra: ALRC, Recs 12-1–12-12.
[31] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report 123, 2014, Canberra: ALRC, Rec 16-1.
[32] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).

resources and stronger powers at their disposal to investigate and act decisively on matters of concern.

Learnings from the experiences of other countries

20 There have been a number of international developments in data privacy law that Australia would benefit from engaging in.

21 The **EU General Data Protection Regulation** (GDPR),[33] which entered into force in May 2018, contains a number of innovative approaches that should be considered by Australian policy makers. In the GDPR, the EU has abandoned its previous approach of setting the same data protection rules for adults and children. It is now explicitly recognised that children require particular protection. Recital 38 of the GDPR explains that **children merit specific protection** as they 'may be less aware of risks, consequences, safeguards […] and their rights in relation to the processing of personal data'. As a result, there are now a number of areas in which children enjoy stricter protection than adults. These include a requirement to provide clear and age-appropriate information in the privacy notice if data is collected from a child,[34] and enhanced protections against marketing and automated decision-making based on profiling. Under Art. 17 GDPR, data subjects have a right to erasure of information where information was collected from them while they were a child.[35] The particular position of children also needs to be considered in the development of industry codes of conduct (Art. 40 GDPR). Although children are not specifically identified, it is implicit also in the provisions on data protection by design (Art. 25) and privacy impact assessments (Art. 35) that the particular vulnerability of children needs to be given due weight in both contexts. Based on this increased emphasis on empowering and protecting children in the online environments, the UK Information Commissioner's Office is currently developing an *Age Appropriate Design Code*.[36] Introduced by the Data Protection Act 2018 (UK), the Code will provide guidance on the privacy standards that organisations are expected to adopt when they offer online services and apps that children are likely to access and process their data.

22 Another significant provision in the GDPR relating to children is contained in Art. 8 which sets out the requirements applying to **consent**. Where data processing relates to the offer of information society services directly to a child and its lawfulness is based on consent,[37] the GDPR requires that the consent is provided **from a person with parental**

[33] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ, L 119/1 (GDPR).
[34] Art. 12 GDPR.
[35] Art. 17(1)f GDPR.
[36] Information Commissioner's Office, *Call for Evidence: Age Appropriate Design Code*, available at <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-evidence-age-appropriate-design-code/>.
[37] Art. 6(1)(a) GDPR.

responsibility if the child is younger than 16 years of age.[38] However, the GDPR gives Member States discretion to set a lower age provided that such lower age is not below thirteen years.[39] These new provisions are widely seen as strengthening the privacy rights of young persons, although their operation in practice is yet to become fully apparent.[40]

23 Apart from consent, the other legitimation grounds for data processing in Art. 6(1) continue to apply to both children and adults. Where data processing is justified on the basis of the legitimate interests of the data controller or a third party, Article 6(1)(f) GDPR imposes a balancing test stating that –

> 'processing is lawful when it is necessary for the purposes of the legitimate interests of the data controller, except where such interests are overridden by the interests or fundamental rights of the data subject, in particular where the data subject is a child.'

24 The operation of this ground will require further elaboration in practice, yet it clearly establishes how **human rights standards are directly drawn** upon in the balancing of competing interests between data processors and data subjects. While this approach is commendable, it is difficult to adopt in a jurisdiction such as Australia, which lacks a domestic human rights act or charter. This provision also implies that, under the GDPR, the requirements on the legitimacy of data processing will be stricter in the case of children, as and when their rights are more affected than those of adults.

25 In adopting a new approach that provides additional specific protections for children, the EU was influenced by the regulatory approach adopted in the US,[41] which – in the absence of general data protection rules – has opted to introduce specific privacy protection regime in discrete contexts. In 1998, the US Congress enacted the **Children's Online Privacy Protection Act (COPPA)** to regulate the collection of personal information from children under the age of 13 years. Under the rule-making powers provided by COPPA, the Federal Trade Commission enacted rules that apply to operators of commercial websites, online services, and mobile apps that are directed at children under this age and to operators of general-audience commercial websites that have 'actual knowledge' that they are collecting personal information from children under thirteen. Intended to give parents more control over when information is collected from their children online, COPPA requires that parents be given 'direct notice' and that 'verifiable parental consent' be obtained before any personal information on children under the age of 13 is collected.

---

[38] Art. 8(1)1 GDPR.

[39] Art. 8(2)2 GDPR.

[40] See, for example, Karen Mc Cullagh, 'The general data protection regulation: a partial success for children on social network sites?' in: T. Bräutigam and S. Miettinen (eds), *Data Protection, Privacy and European Regulation in the Digital Age*, 2016, Helsinki: Unigrafia, 110, 127–129.

[41] Milda Macenaite and Eleni Kosta, 'Consent for processing children's personal data in the EU: following in US footsteps?' (2017) 26 *Information & Communications Technology Law* 146, doi: 10.1080/13600834.2017.1321096.

Companies subject to the COPPA Rule must have a 'clear and comprehensive' privacy policy and not use children's data for marketing-related purpose.

26 The lack of a federal human rights framework in Australia makes it difficult to ask decision makers to draw directly on human rights entitlements in balancing competing rights and interests. I submit that renewed consideration be given to the **enactment a federal Human Rights Act**. Especially in areas of rapid development, such as modern technology, an over-arching rights framework can assist in guiding decisions where simple legislation has yet to catch up. It can also assist in providing individuals with direct, effective redress where their human rights have been interfered with us.

27 Australia has so far not seen fit to introduce specific data protection rules for children and young persons. For example, the *Privacy Act 1988* (Cth) does not specify an age from which a young person can make their own privacy decisions. Instead, where consent is required for the handling of the personal information of a person under the age of 18, the organisation or agency will need to determine that person's capacity to consent on a case-by-case basis. Nonetheless, the Australian Privacy Principles Guidelines by the Office of the Australian Information Commissioner (OAIC) state that individuals aged 15 years or over can be presumed to have the capacity to consent, unless something suggests otherwise.[42] This approach has been adopted for reasons of practicality, but does not have a statutory underpinning. It is also at best implicit in the Australian legislation that data handling practices that disproportionately affect the young must be specifically designed to achieve a suitable standard of protection. Given that both the EU and US, recognised internationally as the most important drivers of international debates on privacy, now adopt an approach that gives explicit statutory recognition to the specific need for protecting the privacy of young people, I submit that the **data rights of young people should be given renewed consideration** in an Australian context.

28 Other innovations contained in the GDPR that respond to new threats to privacy as a result of technological developments, in particular Big Data and AI, include new provisions which address the appropriate limits of **profiling**. Profiling abuses can arise when decisions are made on the basis of unjustifiable profiling, including decisions made on an automated basis.[43] Article 22 GDPR now contains a general prohibition of automated decision-making on the basis of profiling. However, this prohibition is subject to three wide exceptions. These exceptions include that automated decision-making is necessary for entering into, or performance of, a contract or that a data subject has explicitly consented.[44] When one of these exceptions applies, the data controller must establish

[42] Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, B.58.

[43] Lyria Bennett Moses and Janet Chan, 'Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools' (2014) 37 *University of New South Wales Law Journal* 643.

[44] While the Regulation itself does not define the scope of 'necessary', recital 72 expresses the expectation that the European Data Protection Board will issue guidance on profiling. The use of special categories of data

suitable measures to safeguard the data subject's rights, freedoms and interests, including 'the right to obtain human intervention on the part of the controller, to express her or his point of view and to contest the decision' (Art. 22(3) GDPR). Article 22(2)(b) GDPR also contains an opening clause under which the Member States can create further exceptions subject to suitable protections.[45] Other than in the case of children,[46] this provision does not restrict the use of profiling as such but protects against automated decision-making based on profiling. It therefore allows individuals to object to the phenomenon of 'algorithmic governmentality'.[47]

29 There is currently **no specific regulation in Australia** of automated decision-making, although automated or computer-assisted decision-making is becoming increasingly widespread.[48] Anti-discrimination legislation may provide redress in cases in which decisions are based on non-permissible grounds such as race, sex or disability.

Children's particular needs for protection

30 There has already been much international debate on the implication of **children's rights in the digital world**.[49] While children and young people enjoy particular protection under the law, which generally requires that decisions are guided by what is in their best interests, they are not always afforded the opportunity to express their views on how new technology should be deployed. The particular statutory protections that children enjoy recognise the fact that children are **more susceptible to harm** from inappropriate use of, or exposure to, technology or technology-mediated content.[50] Their vulnerability is the result of yet incomplete appreciation of the risks and consequences of certain conduct, and their still developing awareness of the rights and safeguards available to them.[51]

(ie sensitive data) is subject to further restrictions. Recital 71 also notes that profiling should not concern children.

[45] Recital 71 GDPR envisages authorisations by Member States for the purposes of fraud and tax-evasion monitoring and prevention.

[46] See also Recital 38 of the GDPR; Article 29 Working Party, *Opinion 2/2010 on online behavioural advertising*, 2010, Brussels: Article 29 Working Party.

[47] Antoinette Rouvroy and Bernard Stiegler, 'The Digital Regime of Truth: From the Algorithmic Governmentality to a New Rule of Law' (2016) 3 *La Deleuziana – Online Journal of Philosophy* 16–29.

[48] The Hon Justice Melissa Perry and Alexander Smith, '*iDecide: the Legal Implications of Automated Decision-making*', Speech at the University of Cambridge, Cambridge Centre for Public Law Conference 2014: Process and Substance in Public Law, 15–17 September 2014.

[49] Urs Gasser and Sandra Cortesi, Children's Rights and Digital Technologies: Introduction to the Discourse and Some Metaobservations, in: Martin D Ruck et al., *Handbook of Children's Rights: Global and Multidisciplinary Perspectives*, 2016, London and New York: Routledge, ch 25.

[50] Sonia Livingstone and Brian O'Neill, 'Children's Rights Online: Challenges, Dilemmas and Emerging Directions', in: S. van der Hof et al. (eds), *Minding Minors Wandering the Web: Regulating Online Child Safety*, 2018, The Hague/Netherlands: T.M.C. Asser Press, DOI: 10.1007/978-94-6265-005-3_2.

[51] Gerison Lansdown, *The Evolving Capacities of the Child*, 2005, Florence: UNICEF Innocenti Research Centre.

31 The guiding regulatory framework for the protection of children's rights at an international level is the **UN Convention on the Rights of the Child** (UNCRC).[52] This Convention sets out the minimum protections, standards and entitlements that governments have committed to securing and implementing for all children without discrimination. Re-casting traditional notions about childhood and moving from 'protection to autonomy; from nurturance to self-determination; and from welfare to justice',[53] the UNCRC recognises children specifically as rights addressees and rights holders. This provides a suitable framework also for considering the protection of young people's privacy as an issue of human rights, in particular children's rights.

32 It is important that a consideration of young people's privacy listens to what young people regard as their privacy needs and be aware of the weight they attach to their privacy compared with other interests.[54] The **lived experience of many young people** is that many of their social interactions occur via social media and that status attaches to social media interactions. For most young people, social network sites are an important gathering place and forum for communication with their friends. The amount of information shared, and the attitudes towards sharing, will be greatly influenced by peer practice. Peer experience will also affect a young person's evaluation of risk and benefit when it comes to the disclosure of personal information.

33 A working paper by the Global Cyber Security Capacity Centre suggests that:

> The new privacy paradox, therefore, is not about young people over-sharing online with little understanding of the risks, but that social life is now conducted online and that SNSs [Social Networking Sites] do not provide users with the tools that would adequately enable them to manage their privacy in a way that is appropriate for them.[55]

34 To add complexity, it is often **adults who decide on children's access to technology**. Where there are generational conflicts, legal systems need to provide rules that determine at what point decision-making authority transfers from the parent or guardian

---

[52] *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1577 UNTS 3, entered into force 2 September 1990.

[53] Michael DA Freeman, 'Introduction: Rights, ideology and children', in: Michael DA Freeman and Philip E Veerman (eds), *The ideologies of children's rights*, 1992, Dordrecht: Martinus Nijhoff, p. 3.

[54] On the importance of giving voice to the views of children: Gerison Lansdown, *Every Child's Right to be Heard: Resource Guide on the UN Committee on the Rights of the Child General Comment No. 12*, 2011, Save the Children UK: London; Amanda Third et al., *Children's Rights in the Digital Age: A Download from Children Around the World*, 2014, Young and Well Cooperative Research Centre: Melbourne.

[55] Grant Blank, Gillian Bolsover and Elizabeth Dubois, *A New Privacy Paradox: Young people and privacy on social network sites*, Global Cyber Security Capacity Centre: Draft Working Paper, 2014, p 25, available at <https://www.oxfordmartin.ox.ac.uk/downloads/A New Privacy Paradox April 2014.pdf>.

to the child – and how to respond to the potential conflict between the rights of a child and the rights of adults.[56]

35 While the current regulatory response to these issues remains fragmented, it must be remembered that **education and self-regulation play a key role** in helping young people to minimise the risk of potentially harmful digital communication. Preventative and management strategies in school and other social settings assist young people with developing sound protocols and safe practices relating to the sharing of intimate images and other online communications. Such non-legal means will often be more accessible to young people, provide them with more effective protections and allow legal responses to be reserved for the most harmful and insidious consequences of inappropriate online behaviour. It is widely acknowledged that a multi-faceted approach is most effective in preparing children of Australia's contemporary society to take advantage of digital opportunities and in mitigating the associated risks.[57] There has been significant recent debate about many of the issues surrounding safe use of the Internet and of mobile devices.[58] Educational and social measures that encourage children, and their carers, to adopt safe practices and guard against harm, are of paramount importance. Legal regulation operates alongside these preventative approaches and should come into focus particularly when other measures have failed or are felt to be inadequate.

[56] See also Stacey B. Steinberg, 'Sharenting: Children's Privacy in the Age of Social Media' (2016) 66 *Emory Law Journal* 839.

[57] Ilan Katz et al, *Research on youth exposure to, and management of, cyberbullying incidents in Australia: Synthesis report*, SPRC Report 16/2014, 2014, Sydney: Social Policy Research Centre, UNSW Australia, p 14; Office of the Australian Information Commissioner, *The adequacy of protections for the privacy of Australians online*, Submission to Senate Standing Committee on Environment, Communications and the Arts, August 2010, Rec 1, available at <https://www.oaic.gov.au/engage-with-us/submissions/the-adequacy-of-protections-for-the-privacy-of-australians-online-submission-to-senate-standing-committee-on-environment-communications-and-the-arts-august-2010>.

[58] See, for example, Australian Parliament, Joint Select Committee on Cyber-Safety, *High-wire act: Cyber-safety and the young, Interim report*, 2011, Canberra, ACT: Commonwealth of Australia; Parliament of Victoria, Law Reform Committee, *Inquiry into Sexting: Report of the Law Reform Committee for the Inquiry into Sexting*, Parliamentary Paper No. 230, Session 2010-2013, 2013, Melbourne: Victorian Government Printer.