EDUCATIONAL TECHNOLOGY (EDTECH) IN AUSTRALIAN SCHOOLS: A CASE FOR BETTER PRACTICE

ANNA BUNN*

Schools increasingly rely on Educational Technology ('EdTech') products for administrative functions and teaching. While offering significant benefits, EdTech raises concerns about providers' information-handling practices and extensive student data collection, often involving third parties. This article examines one EdTech website used in Australian schools as illustrative of broader information practices. Focusing on Australia, it outlines legal and policy frameworks governing children's information collection, use and disclosure by EdTech providers, and discusses the national Safer Technology for Schools initiative. Adopting a child rights lens, this article argues that schools and education authorities have an important role in protecting students' personal information, as well as promoting their agency and developing the digital and data literacy of students and teachers. Ultimately, however, EdTech providers must do the 'heavy lifting'. This article explores proposed reforms to Australia's privacy laws and considers their likely future impact on the Australian EdTech sector.

I INTRODUCTION

Educational Technology ('EdTech') refers to the wide range of technology used for educational functions or in educational institutions. This includes 'software, hardware and other solutions that support the education value chain'.[1] Examples of EdTech used in schools include the devices students use; platforms used for school management, including learning management and school operations; web-based learning tools; and applications ('apps').[2] The EdTech sector was already

* Associate Professor, Curtin Law School, Curtin University. Associate Investigator with the ARC Centre of Excellence for the Digital Child. The author thanks the anonymous reviewers for their constructive feedback, as well as Meika Atkins for her research and editorial assistance.

1 Deloitte Australia and EduGrowth, *The Australian EdTech Market Census 2020: COVID-19 Update* (Report, July 2021) 4 <https://www.deloitte.com/au/en/Industries/government-public/analysis/australian-edtech-market-census.html> ('*EdTech Market Census 2020*').

2 A more detailed consideration of data infrastructures used in schools can be found in Luci Pangrazio, Neil Selwyn and Bronwyn Cumbo, 'A Patchwork of Platforms: Mapping Data Infrastructures in Schools' (2023) 48(1) *Learning, Media and Technology* 65 <https://doi.org/10.1080/17439884.2022.2035395>.

in a growth phase pre-COVID-19,[3] but unsurprisingly, the pandemic has further accelerated that growth.[4] It is predicted that by 2026 the sector will be worth USD342 billion globally.[5] In Australia, the EdTech sector is one of the biggest employers of technology workers,[6] and (as at June 2023) accounted for AUD3.6 billion in revenue.[7] In terms of the market focus for the EdTech sector in Australia, in mid-2023, 47% of companies targeted schools and early education providers.[8]

The growth of the EdTech sector brings enormous potential benefits but also raises 'thorny quality and ethical questions'.[9] It also raises questions of governance, not least relating to the data practices of EdTech providers. With a focus on those data practices, and taking a child rights perspective, this article considers whether Australian schools (K–12) and education authorities are demonstrating best practice in terms of the EdTech processes and procedures they adopt. It is argued that to demonstrate best practice (or at least 'better practice'), schools and authorities need to move beyond a focus on mere legal compliance: they must take a more active role in weighing the risks associated with EdTech, along with the benefits, and they must do more to afford children and young people appropriate opportunities to have a say in whether and how their data is used and on what terms. They should also facilitate this process through appropriate digital and data literacy education, both for students and teachers. Although this article focuses on the Australian context, the concerns about EdTech data practices apply beyond Australia. Some of the paths to bringing about change in the Australian space (such as through the introduction of a Children's Privacy Code) build on international developments. And in terms of responses to EdTech data practices, the Australian experience, it is suggested, also has something to offer here: in particular, through processes implemented by way of the Safer Technologies 4 Schools ('ST4S') model, which is discussed later in this article.

Taking a child rights lens to the practices of schools and education authorities in relation to EdTech requires a focus on the benefits and potential benefits of the

3 In Australia, EduGrowth notes that the sector 'has undergone rapid growth, doubling in size between 2015 and 2023': 'Australian EdTech', *EduGrowth* (Web Page) <https://edugrowth.org.au/australian-edtech>.

4 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, May 2022) <https://www.hrw.org/sites/default/files/media_2022/10/HRW_20220711_Students%20Not%20Products%20Report%20Final-IV-%20Inside%20Pages%20and%20Cover.pdf> ('*How Dare They Peep*'); Ben Williamson, Felicitas Macgilchrist and John Potter, 'Covid-19 Controversies and Critical Research in Digital Education' (2021) 46(2) *Learning, Media and Technology* 117, 117 <https://doi.org/10.1080/17439884.2021.1922437>.

5 *EdTech Market Census 2020* (n 1) 5.

6 Ibid 6.

7 Australian Trade and Investment Commission and EduGrowth, 'Sector Overview and Statistics as of June 2023' (Web Page) <https://australianedtech.com.au/sector-overview-and-statistics/> ('Australian EdTech Sector Overview').

8 Ibid.

9 Leslie Loble and Aurora Hawcroft, *Shaping AI and EdTech to Tackle Australia's Learning Divide* (Report, December 2022) 6 <https://doi.org/10.57956/kxye-qd93>.

technology[10] – insofar as these can support the right to participation and to education – as well as on some of the risks (including to privacy). For that reason, Part II of this article provides background on EdTech and offers an overview of some of its many benefits, as well as its risks. It also considers why the adoption of a child rights perspective requires schools to move beyond legal compliance. Part III explains some of the information practices of EdTech providers and the education policy environment associated with the selection and use of EdTech in Australian schools. Part IV explains why schools need to become better gatekeepers and model best (or better) practice. Part V explores what better practice might look like. It also considers Australian privacy law reforms – and proposed future reforms – and the extent to which they will assist in guarding against some of the data practices explained in this article. Part VI offers some conclusions and reflections.

II BACKGROUND

The burgeoning of EdTech brings with it, as with most things, the promise of good and the potential for harm. Some of the benefits are directly due to the affordances of the technology itself, insofar as they enable continuity of education in times of crisis[11] and improve access to education for those unable to attend in-person lessons or consultations[12] or who require support.[13] EdTech products offer a range of rich and engaging learning resources[14] and opportunities for students

10 See, eg, Committee on the Rights of the Child, *General Comment No 25 (2021) on Children's Rights in Relation to the Digital Environment*, UN Doc CRC/C/GC/25 (2 March 2021) 1 [3] ('*General Comment No 25*').

11 See, eg, *How Dare They Peep* (n 4) 18; Raluca David et al, 'Education during the COVID-19 Crisis: Opportunities and Constraints of Using EdTech in Low-Income Countries' (Policy Brief, April 2020) <https://doi.org/10.5281/zenodo.3750975>.

12 See, eg, Daniel Rodriguez-Segura, 'EdTech in Developing Countries: A Review of the Evidence' (2022) 37(2) *World Bank Research Observer* 171, 178 <https://doi.org/10.1093/wbro/lkab011>; Sheila Jagannathan, 'The Digital Learning Opportunity' in Sheila Jagannathan (ed), *Reimagining Digital Learning for Sustainable Development: How Upskilling, Data Analytics, and Educational Technologies Close the Skills Gap* (Routledge, 2021) 17, 19 <https://doi.org/10.4324/9781003089698-3>; Legislative Assembly Education and Health Standing Committee, Parliament of Western Australia, *A Better Connected Future: Opportunities for Digital Innovation in Secondary Education* (Report No 8, November 2019) vii ('*Better Connected Future Report*').

13 See Paul Lynch, Nidhi Singal and Gill A Francis, 'EdTech for Learners with Disabilities in Primary School Settings in LMICs: A Systematic Literature Review' (Literature Review, March 2021) <https://doi.org/10.5281/zenodo.4348994>; Emma Lindeblad et al, 'Assistive Technology as Reading Interventions for Children with Reading Impairments with a One-Year Follow-Up' (2017) 12(7) *Disability and Rehabilitation: Assistive Technology* 713 <https://doi.org/10.1080/17483107.2016.1253116>.

14 Office of Educational Technology, United States Department of Education, *Reimagining the Role of Technology in Education: 2017 National Education Technology Plan Update* (Report, January 2017) 12–16; Centre for Educational Research and Innovation, OECD, *Innovating Education and Educating for Innovation: The Power of Digital Technologies and Skills* (Report, 2016) 91–7 <http://dx.doi.org/10.1787/9789264265097-en> ('*Innovating Education Report*').

to grow their networks,[15] among other things.[16] Other benefits arise from the data that is captured by or generated through the use of EdTech, and how it is then used. This includes data mining to understand how students learn, leading to the development of adaptive learning environments;[17] the use of data to assess the impact of educational initiatives and to hold educators accountable;[18] and the use of tracking or analytics to target interventions towards at-risk students and adapt courses to students' needs.[19] Some schools even employ data analysts to leverage the power of student data to improve performance.[20]

These benefits are not realised by all. The fact that EdTech is increasingly embedded into learning environments means that for individuals and schools with limited resources or access to digital technology and infrastructure, the digital divide becomes wider still. As the United Nations ('UN') has noted, 'if digital inclusion is not achieved, existing inequalities are likely to increase, and new ones may arise'.[21] This issue has a gendered dimension,[22] as well as a geopolitical one.[23]

---

15 See, eg, Catholic Education Office of Western Australia, Submission No 2 to Legislative Assembly Education and Health Standing Committee, Parliament of Western Australia, *Inquiry into Digital Innovation in Secondary Education* (15 August 2019) 4, explaining how students in Catholic schools in Western Australia ('WA') have used technology to participate in classes with students in various other countries both synchronously and asynchronously. See also *Innovating Education Report* (n 14) 95.

16 For example, Joanna Zimmerle and Anne Wall discuss how some researchers have demonstrated a connection between use of educational apps and improved academic performance, including upon special education students: Joanna C Zimmerle and Anne S Wall, 'What's in a Policy? Evaluating the Privacy Policies of Children's Apps and Websites' (2019) 36(1) *Computers in the Schools* 38, 41 <https://doi.org/10.1080/07380569.2019.1565628>. The *Better Connected Future Report* (n 12) xi refers to other benefits of EdTech, including enabling students to stay with their families and therefore 'ensuring the sustainability of small regional communities', and notes that some digital tools can 'help disadvantaged Aboriginal students to learn and create in a way that is more suited to their culture'.

17 Sarah Turner, Kruakae Pothong and Sonia Livingstone, Digital Futures Commission, *Education Data Reality: The Challenges for Schools in Managing Children's Education Data* (Report, June 2022) 5 <https://eprints.lse.ac.uk/119731/1/Livingstone_education_data_reality_published.pdf>; Min Liu et al, 'The Use of Analytics for Educational Purposes: A Review of the Literature from 2015 to Present' in Myint Swe Khine (ed), *Emerging Trends in Learning Analytics: Leveraging the Power of Education Data* (Brill Sense, 2019) 26, 35–41 <https://doi.org/10.1163/9789004399273_003>; Ryan S Baker and Kenneth R Koedinger, 'Towards Demonstrating the Value of Learning Analytics for K–12 Education' in David Niemi et al (eds), *Learning Analytics in Education* (Information Age Publishing, 2018) 49; Marie Bienkowski, Mingyu Feng and Barbara Means, United States Department of Education, *Enhancing Teaching and Learning through Educational Data Mining and Learning Analytics: An Issue Brief* (Report, October 2012) <https://files.eric.ed.gov/fulltext/ED611199.pdf>.

18 Frida Alim et al, Electronic Frontier Foundation, *Spying on Students: School-Issued Devices and Student Privacy* (Report, 13 April 2017) 7.

19 See, eg, Loble and Hawcroft (n 9); Jasmina Bryne, Emma Day and Linda Raftree, United Nations Children's Fund, *The Case for Better Governance of Children's Data: A Manifesto* (Report, May 2021) 16 <https://www.unicef.org/innocenti/media/1031/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf>.

20 Pangrazio, Selwyn and Cumbo (n 2) 75.

21 *General Comment No 25* (n 10) 1 [4].

22 Ibid 2 [11].

23 The United Nations' *The Sustainable Development Goals Report 2024* notes that:

> Between 2021 and 2022, the growth rate in schools' Internet access for pedagogical purposes doubled globally and even tripled in some regions. At the upper secondary level, 91 per cent of schools had access to electricity, 81 per cent had computers and 69 per cent were connected to the Internet. Significant

Digital divides are not only apparent across country borders, but within countries,[24] regions[25] and individual schools.[26]

Despite the undeniable benefits associated with EdTech, numerous concerns have been raised about the technology. As Joel Reidenberg and Florian Schaub have remarked:

> [L]earning analytics may assist with self-assessment but could also amplify performance-related stress for students; and algorithmic assessment and decision making can personalize learning experience but may also alter or suppress learning opportunities for certain students, for instance, when data and algorithms provide an incomplete or inaccurate representation of learning progress …[27]

There is also, of course, the ever-present risk of technology failures which, when they occur at scale, are often well-publicised,[28] and broader concerns that the

---

> disparities remained, particularly in sub-Saharan Africa, where less than a third of primary schools and about half of secondary schools had access to electricity, hindering the use of technology.

United Nations, *The Sustainable Development Goals Report 2024* (Report, 2024) 17 <https://unstats.un.org/sdgs/report/2024/The-Sustainable-Development-Goals-Report-2024.pdf>.

24 See, eg, Casey Temple, 'The Digital Divide: Lessons COVID-19 Taught Us about the Digital Exclusion of Students from Low Socio-Economic Backgrounds', *United Nations Association of Australia* (Blog Post, 15 November 2020) <https://www.unaa.org.au/2020/11/15/the-digital-divide-lessons-covid-19-taught-us-about-the-digital-exclusion-of-students-from-low-socio-economic-backgrounds/>; Barbara Preston, *Digital Inclusion for All Public School Students* (Report, June 2020) <https://www.aeufederal.org.au/application/files/5315/9372/9335/DigitalInclusion_BPreston.pdf>; Erin Parke, 'Australia's Digital Divide Means 2.8 Million People Remain "Highly Excluded" from Internet Access', *ABC News* (online, 16 October 2022) <https://www.abc.net.au/news/2022-10-16/australia-digital-divide-millions-cannot-access-internet/101498042>. The 2023 Australian Digital Inclusion Index notes the 'considerable digital gap between First Nations and non-First Nations people in Australia' and the 'persistent' (although narrowing) 'divide between capital cities and other parts of the country': Julian Thomas et al, *Measuring Australia's Digital Divide: Australian Digital Inclusion Index 2023* (Report, 2023) 5 <https://doi.org/10.25916/528s-ny91>. In 2019, the Legislative Assembly Education and Health Standing Committee of the Parliament of WA reported on its finding that the states of New South Wales ('NSW'), South Australia and Victoria all had higher bandwidth targets than WA and that the provision of devices varies between states: *Better Connected Future Report* (n 12) 41, 47.

25 See findings 14–16 of the *Better Connected Future Report* (n 12): at xiii. As observed by Catholic Education Western Australia, '[t]he conundrum of equity in education is that the schools who are often most in need of [information and communications technology] and other technologies are usually the schools which are least well resourced to acquire and maintain them': at 46. See also Pangrazio, Selwyn and Cumbo (n 2) 77.

26 For example, between students in the same school from different socio-economic backgrounds. Michael Dezuanni et al refer to the fact that

> [t]he digital experiences of low-income families are as varied and complex as the families themselves, however low-income families with limited access to data, appropriate devices, and the ability and support to use them face additional challenges to full economic, social and cultural participation.

Michael Dezuanni et al, *Advancing Digital Inclusion in Low Income Australian Families: Interim Findings Report* (Report, October 2022) 5.

27 Joel R Reidenberg and Florian Schaub, 'Achieving Big Data Privacy in Education' (2018) 16(3) *Theory and Research in Education* 263, 268 <https://doi.org/10.1177/1477878518805308>.

28 See, eg, Michael McGowan, 'Naplan Online Failures Bring More Calls from States for Reform', *The Guardian* (online, 16 May 2019) <https://www.theguardian.com/australia-news/2019/may/16/naplan-online-failures-bring-more-calls-from-states-for-reform>; Colin Lecher, 'Remote Exam Software Is Crashing when the Stakes Are the Highest' *The Markup* (online, 13 October 2020) <https://themarkup.org/coronavirus/2020/10/13/remote-exam-software-failures-privacy>; Jason Kelley, 'Bar Applicants Deserve

pedagogical benefits of EdTech have (at best) not always been rigorously assessed[29] or fully realised.[30] As Leslie Loble and Aurora Hawcroft have noted, EdTech tools 'penetrate classrooms largely through marketing campaigns and without rigorous evaluation or understanding of how best to use them'.[31] Attention has also been drawn to discrimination or bias that may be built into algorithms[32] or occur as a result of their use, the effects of which may be more or less visible.[33] Concerns have also been expressed that students' intellectual property is sometimes inappropriately assigned to EdTech providers,[34] as well as that some uses of EdTech involve an intrusion into students' private spaces, such as homes and bedrooms.[35]

Many concerns raised about EdTech centre on the vast amount and variety of ways in which data is captured and generated. Velislava Hillman has commented: 'Data in education increasingly influence decision making and change not only *how* the curriculum is designed (through data) but also *who* designs it (the agents that extract the data and their algorithms).'[36]

These concerns are part of a broader debate about the political economy of education and how the business interests of EdTech companies are able to influence curriculum, infrastructure, assessment and school organisation, among other things.[37] Concerns about the data practices of EdTech providers themselves,

---

Better than a Remotely Proctored "Barpocalypse"' *Electronic Frontier Foundation* (Blog Post, 9 October 2020) <https://www.eff.org/deeplinks/2020/10/bar-applicants-deserve-better-proctored-barpocalypse>.

29 Eleanor Stringer, Cathy Lewin and Robbie Coleman, *Using Digital Technology to Improve Learning* (Guidance Report, 2019) 7; Marisa Meyer et al, 'How Educational are "Educational" Apps for Young Children? App Store Content Analysis Using the Four Pillars of Learning Framework' (2021) 15(4) *Journal of Children and Media* 526 <https://doi.org/10.1080/17482798.2021.1882516>.

30 Stringer, Lewin and Coleman (n 29) 7; Laura A Outhwaite et al, 'Can Maths Apps Add Value to Learning? A Systematic Review' (Working Paper No 23-02, Centre for Education Policy and Equalising Opportunities, University College London, 2023) <https://repec-cepeo.ucl.ac.uk/cepeow/cepeowp23-02.pdf>.

31 Loble and Hawcroft (n 9) 13.

32 See, eg, Nabeel Gillani et al, 'Unpacking the "Black Box" of AI in Education' (2023) 26(1) *Educational Technology and Society* 99, 106–7 <https://doi.org/10.30191/ETS.202301_26(1).0008>. The United Nations Children's Fund ('UNICEF') notes that '[a]lgorithms tend to reproduce patterns of bias and historical discrimination found in the data used to train them': Byrne, Day and Raftree (n 19) 29.

33 A visible example, in the education context, comes from 2020 when the use of an algorithm to calculate student 'A-Level' grades in England and Wales was found to work in such a way that it entrenched socio-economic advantage, leading to its eventual abandonment: see Daan Kolkman, 'F**k the Algorithm? What the World Can Learn from the UK's A-Level Grading Fiasco', *LSE* (Blog Post, 26 August 2020) <https://blogs.lse.ac.uk/impactofsocialsciences/2020/08/26/fk-the-algorithm-what-the-world-can-learn-from-the-uks-a-level-grading-fiasco/>. Although not without ongoing consequences, such as the impact on university placements: see Anthony Kelly, 'A Tale of Two Algorithms: The Appeal and Repeal of Calculated Grades Systems in England and Ireland in 2020' (2021) 47(3) *British Educational Research Journal* 725, 729 <https://doi.org/10.1002/berj.3705>.

34 Elana Zeide and Helen Nissenbaum, 'Learner Privacy in MOOCs and Virtual Education' (2018) 16(3) *Theory and Research in Education* 280, 294 <https://doi.org/10.1177/1477878518815340>.

35 Lisa Archbold et al, 'Children's Privacy in Lockdown: Intersections between Privacy, Participation and Protection Rights in a Pandemic' (2021) 3(1) *Law, Technology and Humans* 18, 22 <https://doi.org/10.5204/lthj.1803> ('Children's Privacy in Lockdown').

36 Velislava Hillman, 'EdTech in Schools: A Threat to Data Privacy?', *LSE* (Blog Post, 27 May 2021) <https://blogs.lse.ac.uk/medialse/2021/05/27/edtech-in-schools-a-threat-to-data-privacy/> (emphasis in original).

37 Julian Sefton-Green, Michael Dezuanni and Luci Pangrazio, 'A Research Agenda to Examine the Political Economy of Digital Childhood' (Digital Child Working Paper No 2022-06, ARC Centre of Excellence for the Digital Child, 2022) 19 <https://doi.org/10.26187/ae09-g889>; Sonia Livingstone et al, 'The

or the data practices they facilitate, are not only about whether these practices are lawful. Rather, the concern is with data governance more generally and with the potential consequences that stem from the collection and use of vast amounts of user information – what some have termed 'datafication'[38] or 'dataveillance'.[39] These consequences include (but are not limited to) commercialisation of schools and the increased 'privatisation' of education;[40] impact on pedagogy and resulting shifts in power (as alluded to above); problems (such as data theft) that materialise when things go wrong; and the difficulty of validating the claims made about students based on data captured about them.[41] There is also concern that childhood is becoming 'commodified' and that profiling of children allows them to be targeted for commercial purposes. Illustrative of this last point, a report by Human Rights Watch on EdTech products endorsed by governments during the COVID-19 pandemic found that:

> Most online learning platforms sent or granted access to children's data to third-party companies, usually advertising technology ('AdTech') companies. In doing so, they appear to have permitted the sophisticated algorithms of AdTech companies the opportunity to stitch together and analyse these data to guess at a child's personal characteristics and interests, and to predict what a child might do next and how they might be influenced.[42]

It has been said that 'the use of Big Data analytics to inform marketing activities has the potential to result in manipulation and to impair children's decisional autonomy'.[43] But profiling children enables more than marketing and targeted advertising. As the UN Children's Fund has observed, targeting (or 'microtargeting')[44] can be used 'to shape children's beliefs on issues such as gender or political participation'[45] and 'manipulate children's consumption patterns and behaviours, thus infringing on their freedom of choice and expression'.[46] In its

---

Googlization of the Classroom: Is the UK Effective in Protecting Children's Data and Rights?' (2024) 7 *Computers and Education Open*, 100195:1–8 <https://doi.org/10.1016/j.caeo.2024.100195>.

38 Deborah Lupton, 'Thinking with Care about Personal Data Profiling: A More-than-Human Approach' (2020) 14 *International Journal of Communication* 3165, 3165, citing José van Dijck, 'Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology' (2014) 12(2) *Surveillance and Society* 197.

39 Lupton (n 38) 3165, citing Roger Clarke and Graham Greenleaf, 'Dataveillance Regulation: A Research Framework' (2017) 25(1) *Journal of Law, Information and Science* 104.

40 See, generally, Ben Williamson and Anna Hogan, *Commercialisation and Privatisation in/of Education in the Context of COVID-19* (Report, July 2020).

41 Chris Zomer, 'The Datafication of Student Engagement and Children's Digital Rights' (2024) 6 *Computers and Education Open* 100189:1–8, 6 <https://doi.org/10.1016/j.caeo.2024.100189>.

42 *How Dare They Peep* (n 4) 2. For a detailed consideration of the AdTech industry and the Australian context, see Lisa Archbold et al, 'Adtech and Children's Data Rights' (2021) 44(3) *University of New South Wales Law Journal* 857 <https://doi.org/10.53637/PJPS3138> ('AdTech').

43 Normann Witzleb et al, 'Privacy Risks and Harms for Children and Other Vulnerable Groups in the Online Environment' (Research Paper, Office of the Australian Information Commissioner, 18 December 2020) 33.

44 See Byrne, Day and Raftree (n 19) 30, citing Michaela Smiley, 'What is Microtargeting and What Is It Doing in Our Politics?' *Mozilla Blog* (Blog Post, 4 October 2018) <https://blog.mozilla.org/en/firefox/microtargeting-dipayan-ghosh/>.

45 Byrne, Day and Raftree (n 19) 5.

46 Ibid 23–4.

recent review of the Australian *Privacy Act 1988* (Cth) ('*Privacy Act*') the Attorney-General's *Privacy Act Review Report 2022* ('*Privacy Review Report*') remarks that:

> Targeting has the potential to cause significant harm when individuals have limited awareness of why and how they are being targeted and no control over it, and where targeted content and advertising may be used to manipulate, discriminate, exclude and exploit individuals based on their vulnerabilities.[47]

The UN Committee on the Rights of the Child ('Committee') has commented that digital practices including profiling and behavioural targeting 'may lead to arbitrary or unlawful interference with children's right to privacy; they may have adverse consequences on children, which can continue to affect them at later stages of their lives'.[48] And children and young people themselves have expressed concerns about the sharing of their data and lack of transparency regarding what happens to it,[49] as well as about the use of their data to sell them things.[50] Yet, as things stand, not only are these practices prevalent in Australia, they are also generally legal.[51]

Recent privacy law reforms and proposed future reforms in Australia herald some changes. These reforms respond to the recognised need to 'better align Australia's laws with global standards of information privacy protection and properly protect Australians' privacy'.[52] Some of the recommended reforms are targeted specifically towards children (under 18 years old) and reflect a child rights approach to information privacy by explicitly noting that the UN *Convention on the Rights of the Child* ('*CRC*')[53] 'recognises the need to extend particular care to children',[54] and that this necessitates striking a balance between adequate protection of children's (right to) privacy and their other rights, including the right to participate online. This idea of striking a balance between protection and participation rights has been neatly captured by the former United Kingdom ('UK') Information Commissioner's emphasis on protecting children *within* the

47 Attorney-General's Department (Cth), *Privacy Act Review Report 2022* (Report, 16 February 2023) 210 ('*Privacy Review Report*').

48 *General Comment No 25* (n 10) 11–12 [68].

49 Ibid 1 [3].

50 See, eg, Reset.Tech Australia, Submission No 31 to Senate Standing Committee on Economics, Parliament of Australia, *Influence of International Digital Platforms* (February 2023) 3. The most recent Office of the Australian Information Commissioner ('OAIC') *Australian Community Attitudes to Privacy Survey* report found that '[n]ine in ten (92%) parents believe children should have the right to grow up without being profiled and targeted' and that 91% of parents believe that 'technology used in schools and for education purposes should only collect the minimum amount of personal information necessary for the service': Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey* (Report, August 2023) 90–1 ('*Attitudes to Privacy Survey*').

51 This is discussed further in Part II(B).

52 *Privacy Review Report* (n 47) 1.

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

54 *Privacy Review Report* (n 47) 146.

digital environment – highlighting that protection within the digital environment should not come at the cost of exclusion from it.[55]

Some of the detail of the privacy law reforms is discussed later in Part V of this article. However, even when (and if) these reforms are implemented, this article argues that schools themselves – and the broader ecosystems of which they are part, such as education authorities or umbrella organisations – have an important 'gatekeeping' role to play. In order to protect children *within* the digital environment schools and education authorities should be mindful of the limits of a parental consent model. They should also recognise that even strengthened information privacy laws do not guarantee that children will be appropriately protected within the digital environment – not least because it is not assured that EdTech providers will comply with their legal obligations. On the other hand, schools and education authorities occupy a special position: they arguably 'confer legitimacy on any product or worldview promoted there',[56] and they are crucial markets for EdTech products. Because of this, they have both the capacity and the opportunity to adopt practices and policies that promote children's best interests and to exert a 'mediating' influence on the power wielded by EdTech, particularly as it plays out through data practices. Moreover, schools are uniquely placed to create opportunities for meaningful choice and consent by parents and students where appropriate. These arguments are developed further in Part IV, following an overview of some of the information practices of EdTech providers and the legal and policy framework applicable in Australia.

III EDTECH IN AUSTRALIAN SCHOOLS

Identifying all the different EdTech platforms and apps used in Australian schools would be a near impossible task. However, insights can be drawn from various sources. An investigation conducted by the Office of the Victorian Information Commissioner ('OVIC') in 2020 ('OVIC Examination') found that public schools in Victoria used a range of apps and web-based learning tools. Some were selected by the schools themselves, while others were provided under a central licence by the Victorian Department of Education and Training. OVIC noted that many of the apps used to meet specific curriculum needs were free – a matter of concern, given that '[g]enerally, free apps and web-based learning tools are related to lower levels of privacy protections and increased use of information to be on-sold or used for targeted marketing'.[57] OVIC grouped the majority of products

55 Information Commissioner's Office (UK), *Age Appropriate Design: A Code of Practice for Online Services* (17 October 2022) 2 <https://ico.org.uk/media2/0oppn5fg/age-appropriate-design-a-code-of-practice-for-online-services-all-2-1-87.pdf> ('*UK Children's Code*').

56 Faith Boninger, Alex Molnar and Kevin Murray, National Education Policy Center, *Asleep at the Switch: Schoolhouse Commercialism, Student Privacy, and the Failure of Policymaking* (Report, August 2017) 5 <http://nepc.colorado.edu/publication/schoolhouse-commercialism-2017>.

57 Office of the Victorian Information Commissioner, *Examination into the Use of Apps and Web-Based Learning Tools in Victorian Government Primary Schools* (Examination Report, 18 August 2020) 16 [58] ('*OVIC Examination Report*').

into four categories: educational, administrative, productivity and assessment.[58] However, the report also noted that some apps were game-based.[59]

Luci Pangrazio, Neil Selwyn and Bronwyn Cumbo provide a useful snapshot of the digital infrastructure used in three specific Victorian secondary schools, outlining their functionality, interoperability, and some of the reasons schools select particular platforms.[60] The researchers found eight main purposes for the schools' data infrastructure,[61] that are likely to be reflected in other schools across Australia, although the actual products may differ:

- *School management* – often a platform that manages attendance and timetabling data, as well as basic learning tasks and subject forums (ie, Compass, Moodle);
- *School operations* – often a platform that manages business and administration data related to student enrolments, teacher employment and the general running of the school (ie, Synergetic, EMS360);
- *Interacting with parents* – often an app that manages a specific task, such as organising excursions, presenting student learning or gathering medical histories of students (ie, CareMonkey, Parent Teacher Online);
- *Learning content* – a subject-specific learning platform (ie, Maths Pathways, Pearson);
- *Doing work* – generic programmes and platforms for teachers and students to create documents and presentations (ie, Microsoft Office, Kahoot);
- *Converging data* – a hidden part of the infrastructure used to aggregate and streamline multiple sources of information (ie, Hapara Dashboard, Casync);
- *Monitoring devices and Wi-Fi* – use by the technology staff to keep track of devices and manage Wi-Fi across the school (ie, Active Directory, ClearPass);
- *Mirroring platforms* – an interface to a larger platform that is easier for teachers to use (ie, Syn-Web part of Synergetic).[62]

In the government school sector, it is usual practice to seek parental consent before schools provide student information to a third-party online service provider, or – depending on the provider – at least to notify parents that a particular service is being used. These school-issued requests to parents provide some insight into the third-party services being used. As the parent of a secondary school student at a government school in Western Australia ('WA'), the author received a request from the school to provide consent to a total of 34 third-party apps and services, and notification of the use of 12 others. Third-party services for which consent was requested included subject-specific apps, classroom tools, creativity and design tools, and websites and apps to guide students through after-school and career choices, or to offer information on health and wellbeing.

58 Ibid 13 [49].

59 Ibid 16 [58], 29–31. This report appears to be confined to an assessment of apps and digital resources used in the classroom and available to students, rather than software used for administrative or safeguarding purposes.

60 Pangrazio, Selwyn and Cumbo (n 2).

61 The term 'data infrastructures' is used to refer not only to technologies used in schools, but also to 'roles, practices and standards related to various aspects of school organisation': ibid 69.

62 Ibid.

A EdTech Providers: Information Practices

The use of EdTech in schools invariably requires the collection, use and disclosure of information about individual students (and often also about teachers and even parents and guardians). An extract of a report for the UK Digital Futures Commission about a particular software product – Times Tables Rock Stars from Maths Circle – is illustrative:

> Schools are able to contract directly with Maths Circle to gain access to Times Tables Rock Stars for their students, and using limited data about the student (name, email address, class or year information) to create a profile for them. Times Tables Rock Stars is accessed either through an app, or directly through a web browser. Its use generates further data associated with the student profile – information about usage of the platform, as well as details about the child's performance when using it … But less clearly, data about the platform use will be collected by cookies embedded in the platform. Data can also be shared – anonymised – with third parties for research, and, in extreme circumstances, shared with other parties.[63]

The information practices outlined in this example are representative of those that occur in Australian schools,[64] although the nature and extent of the information collected from or about students varies between providers. Some request relatively minimal information, such as student name and email address, whereas others (typically products used for school management) request detailed personal information, including photographs, health information and even biometric information.[65] As noted in a case study on G Suite for Education ('G Suite') undertaken as part of the OVIC Examination, schools also sometimes provide information beyond that actually required by the provider, and users sometimes choose to provide extra (ie, non-mandatory) information, such as profile photos and phone numbers.[66]

In addition to information requested as part of a 'sign-up' or registration process, many EdTech providers also collect information when users interact with the product. For example, one web-based tool used to support career education in secondary schools, Year13, gives users the option to complete career quizzes and other activities, which then enable Year13 to collect other information about the user, including personal information.[67] Providers may also collect information about

63 Turner, Pothong and Livingstone (n 17) 18–19.

64 See, eg, the EdTech providers listed in third-party services catalogues issued by Australind Senior High School in WA based on risk assessments by the DoE (WA): Australind Senior High School, 'Third Party Online Services: Notification' (Catalogue) <https://australind.wa.edu.au/wp-content/uploads/2025/04/Website-Third-Party-Catalogue-Notification.pdf> ('Third Party Consent Catalogue: Notification'); Australind Senior High School, 'Third Party Online Services: Bundled' (Catalogue) <https://australind.wa.edu.au/wp-content/uploads/2025/04/Website-Third-Party-Catalogue-Consent.pdf> ('Third Party Consent Catalogue: Bundled').

65 For example, Compass Education uses biometrics which enables fingerprint access for certain functions: 'Biometric Data', *Compass Education* (Web Page) <https://policies.compass.education/biometric-data>.

66 *OVIC Examination Report* (n 57) 17.

67 *Year13* (Website) <https://year13.com.au/>.

users passively.[68] In the context of the G Suite case study, for example, OVIC notes that the provider 'collects device information such as hardware model, operating system version, IP address, location information using GPS and IP address and browser information'.[69]

Many of the products used in Australian schools also enable information to be collected about users by third parties. An example of this can be seen from the use of the Blacklight privacy tool to inspect Year13's website. Although Year13 is presented here as a single case study, its practices are illustrative of broader industry practices across the EdTech sector.[70] Year13 is one of the EdTech products listed on the consent request made to the author and referred to above. The Blacklight inspection identified that Year13's website contained a higher-than-average number of ad trackers and third-party cookies (see Figure 1).[71] The purpose of these cookies is to collect various information about the user, such as user behaviour on the site and the user's browser type and IP address, which can then be used to build user profiles and target individuals for advertising purposes.[72] When running the Year13 website link through Blacklight, it 'detected trackers on this page sending data to companies involved in online advertising', including Reddit, Facebook, Twitter, Microsoft and Salesforce.[73] The Blacklight inspection of Year13 also revealed a higher-than-average number of third-party cookies (see Figure 1); these can also be used to build user profiles and target individuals for advertising (or other) purposes.[74]

68 Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019) 378 <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf> ('*Digital Platforms Report*').

69 *OVIC Examination Report* (n 57) 17.

70 *How Dare they Peep* (n 4) 64–5.

71 'Blacklight', *The Markup* (Web Page) <https://themarkup.org/blacklight>. The results were generated by using the Blacklight privacy inspector to conduct a scan of the Year13 website: see above n 67. Noting that results are dynamic and may change over time, references to 'Blacklight' (n 71) refer to the Blacklight inspection results for the Year13 website at the time of writing. For the tool's methodology, see Surya Mattu and Aaron Sankin, 'How We Built a Real-Time Privacy Inspector', *The Markup* (online, 31 May 2023) <https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector>.

72 Mattu and Sankin (n 71). For consideration of children's rights in the context of AdTech, see Archbold et al, 'AdTech' (n 42). The Australian Competition and Consumer Commission's *Digital Platforms Report* (n 68) contains an in-depth discussion of online tracking for targeted advertising purposes, including types of technologies used: see *Digital Platforms Report* (n 68) 387–90.

73 The listed sites were found by expanding the '[a]d trackers found on this site' section: 'Blacklight' (n 71).

74 These consist of a 'bit of text – usually a unique number or a string of characters' that can identify users when they 'visit other websites that contain tracking code from the same company': Mattu and Sankin (n 71).

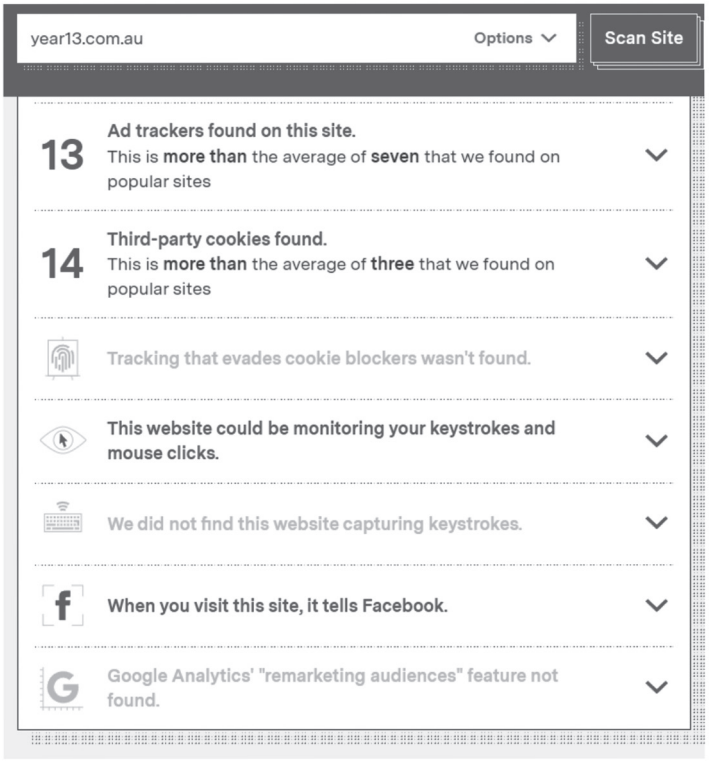

Figure 1: Results of Blacklight review of the Year13 website, as at 13 August 2024

As also indicated in Figure 1, the Year13 website informs Facebook, via a pixel, whenever a user visits it. According to the organisation behind Blacklight:

> The Facebook pixel is a piece of code Facebook created that allows other websites to target their visitors later with ads on Facebook. Common actions that can be tracked by pixel include viewing a page or specific content, adding payment information, or making a purchase … 30 percent of [popular] sites used the Facebook pixel.[75]

The Blacklight tool also found that the Year13 website 'could be monitoring your keystrokes and mouse clicks', although it was not possible to determine how data collected in this way is used.[76] Nevertheless, Blacklight notes that such practices can be 'insecure and make sensitive user data such as passwords and credit card information more vulnerable to leaks'.[77]

Information about a user, for example about their age, interests or even their location, can also sometimes be inferred from other sources. Inferred information is that which is generated by 'analysing and making inferences based on either data actively provided by a consumer, other passively-collected user data, or data

75 Ibid.
76 See Figure 1 above.
77 'Blacklight' (n 71).

from de-identified datasets'.[78] For example, location information can be inferred from various sources including (but not limited to) GPS, IP addresses, time zone, connection speed and even other devices in the vicinity of the user's device or connected to the user's network.[79]

Determining how student information is used by EdTech providers themselves (as opposed to third parties, such as AdTech players) can to some extent be gleaned by considering the terms of a given provider's privacy policy. For example, Year13 makes clear in its privacy policy that it uses information for various purposes, including:

- sharing information with school and career advisers;
- conducting its business;
- communicating information to advertisers, sponsors and supporters;
- communicating information about its products and services; and
- undertaking 'internal administrative, research, planning, marketing and product development'.[80]

Year13's 'For Business' section states that: 'Our first-party data and extensive Gen Z insights portfolio enables us to provide our partners with data informed recommendations.'[81] The business pages assure potential partners that their brand will be 'top of mind with young people as they make foundational decisions'.[82] Among Year13's partners are tertiary education providers and the Armed Forces, but also a bank, a fast-food company, a clothing brand and a travel organisation.

Even when privacy policies (alongside publicly available information) do explain what personal information is collected and what it is used for, they can only reveal so much about an organisation's information practices. Privacy policies are typically written in a way that permits a wide range of information to be collected and used. They often use vague language,[83] and 'do not clearly set out to each user what is occurring with their user data specifically'.[84] Moreover, there is no requirement on the part of entities bound by the *Privacy Act* to disclose whether personal information is collected directly by third parties, such as through the use of cookies and pixels embedded into those entities' web pages.

B Legal and Policy Framework

This section overviews the legal and policy framework applicable to the information practices of Australian schools, as well as of the EdTech providers themselves. It is not intended as a comprehensive analysis of all laws and policies that apply to EdTech providers and schools, but rather to highlight some commonalities and differences that apply between jurisdictions (meaning, as between government and non-government schools, as well as between different

78 *Digital Platforms Report* (n 68) 378.
79 Ibid 385.
80 'Privacy Policy', *Year13* (Web Page) <https://year13.com.au/privacy-policy>.
81 'For Business', *Year13* (Web Page) <https://year13.com.au/business>.
82 Ibid.
83 *Digital Platforms Report* (n 68) 405, 601.
84 Ibid 397.

states) and some of the issues or gaps that are apparent in terms of regulating the information practices of EdTech providers themselves.

1 Information Privacy Laws

Some of the information practices described in the previous section *may* be subject to state or federal privacy laws, which are described below.

The *Privacy Act* is the primary national legislation governing information privacy in Australia. The Act contains a set of Australian Privacy Principles ('APPs') which regulate the collection, use and disclosure of personal information.[85] The APPs also impose other obligations on entities required to comply with them,[86] and provide individuals with other rights vis-à-vis those entities[87]. The APPs apply to federal government agencies, as well as to organisations, other than those classed as a 'small business operator'.[88]

At the state and territory level, all jurisdictions – except South Australia ('SA') – have enacted privacy legislation that includes a set of legislated privacy principles governing the information handling practices of state public sector agencies.[89] The various state-based privacy principles are broadly equivalent to the APPs, regulating the collection, use and disclosure of personal information, although the collection, use and disclosure of health information may be subject to separate rules.[90] In SA, public sector agencies are subject to a set of information privacy principles contained in an instruction issued by a Premier and Cabinet

85 *Privacy Act 1988* (Cth) sch 1 ('*APPs*').

86 Such as the requirement to maintain an up-to-date privacy policy containing certain information: ibid sub-cls 1.3–1.4.

87 Such as rights to access and correct their personal information: ibid cls 12–13.

88 *Privacy Act 1988* (Cth) s 6C(1) ('*Privacy Act*'). A 'small business operator' is an 'individual, body corporate, partnership, unincorporated association or trust' which 'carries on one or more small businesses' and also 'does not carry on a business that is not a small business': at s 6D(3). A 'small business' is one which, at any given time, had an annual turnover of $3 million or less for the previous financial year: at s 6D(1). However, this definition must be considered alongside the other provisions of section 6D: at ss 6D(2)–(9). Importantly, a business that provides a health service and holds health information is not considered a small business: at s 6D(4)(b).

89 See *Information Privacy Act 2014* (ACT) sch 1 ('*ACT Privacy Principles*'); *Privacy and Personal Information Act 1998* (NSW) pt 2 ('*NSW Information Protection Principles*'); *Information Act 2002* (NT) sch 2; *Information Privacy Act 2009* (Qld) schs 3 (these apply to agencies other than health agencies), 4; *Personal Information and Protection Act 2004* (Tas) sch 1; *Privacy and Data Protection Act 2014* (Vic) sch 1 ('*Vic Information Privacy Principles*'); *Privacy and Responsible Information Sharing Act 2024* (WA) sch 1 ('*WA Privacy Act*') (as passed, although note that the in-force version does not, at the time of writing, contain schedule 1).

90 The *ACT Privacy Principles* (n 89) applies to 'personal information', which is defined in section 8 to exclude 'personal health information' within the meaning of the *Health Records (Privacy and Access) Act 1997* (ACT), the latter Act setting out principles for the collection, use and disclosure of personal health information. The *NSW Information Protection Principles* (n 89) applies to 'personal information' defined in section 4, but excludes, by virtue of section 4A, 'health information' within the meaning of the *Health Records and Information Privacy Act 2002* (NSW) – the latter establishes a set of Health Privacy Principles. The *Vic Information Privacy Principles* (n 89) applies to 'personal information' defined in section 3 to exclude information of a kind to which the *Health Records Act 2001* (Vic) applies, the latter setting out a set of Health Privacy Principles.

circular.[91] WA has recently passed legislation to enact its first comprehensive set of Information Privacy Principles for the state public sector,[92] although the Principles themselves will only come into effect on a day yet to be fixed by proclamation[93] – likely in 2026.[94]

The following sections consider the application of current Australian privacy laws to EdTech providers and third parties receiving information via EdTech products, before considering their application in the Australian school context.

2 EdTech Providers and Third Parties: Application of Privacy Laws

Two threshold considerations determine whether an EdTech provider or third-party organisation must comply with the APPs. First, where an organisation's turnover in the previous financial year is $3 million or less, that organisation is classed as a 'small business' and not bound to comply with the APPs (unless it provides a health service or is otherwise unable to rely on the small business exemption).[95] Second, an organisation established outside of Australia is only bound by the *Privacy Act* if it has an 'Australian link', as defined in the *Privacy Act*.[96]

In terms of the first consideration, while many EdTech providers exceed the annual turnover threshold, others do not. Taking only EdTech companies founded in Australia or by an Australian, for example, statistics for mid-2023 found that 78% were early- or late-stage start-ups with annual revenue under $2 million. Only 14% were established companies with over $2 million in annual revenue.[97] This suggests that, at least in terms of the Australian EdTech sector, most providers may qualify for the small business exemption.[98] Nevertheless, many may choose to treat themselves as bound by the *Privacy Act*; indeed, from a reputational point

91 Department of the Premier and Cabinet (SA), *Information Privacy Principles (IPPS) Instruction* (PC 012, 4 May 2020).

92 The *WA Privacy Act* (n 89) and its associated Information Privacy Principles ('IPPs') (which appear in the version as passed, but not – at the time of writing – the Act 'in force') reflect some of the changes that have been recommended at the federal level in the course of the *Privacy Review Report* (n 47). For example, IPP 1 provides that: 'An IPP entity must not collect personal information that relates to an individual unless the collection is fair and reasonable in the circumstances', taking into account various matters including, where the information relates to a child, whether 'the collection … is in the best interests of the child': *WA Privacy Act* (n 89) sch 1 sub-cl 1.4(g). A similar provision applies to IPP 2, about the disclosure and use of personal information: at sch 1 sub-cl 2.2.

93 *WA Privacy Act* (n 89) s 2(c).

94 Department of the Premier and Cabinet, 'Interim Privacy Position', *Government of Western Australia* (Web Page, 9 December 2024) <https://www.wa.gov.au/government/announcements/interim-privacy-position-0>.

95 *Privacy Act* (n 88) s 7(1)(ee). The definition of small business and small business operator is set out at section 6D.

96 *Privacy Act* (n 88) ss 5B(1A)–(3).

97 'Australian EdTech Sector Overview' (n 7).

98 That said, any small business that trades in personal information is not exempt from the *Privacy Act* (n 88): at s 6D(4)(c)–(d). Essentially, this involves asking whether the business (regardless of turnover) collects or discloses personal information for 'a benefit, service or advantage'. Even if this is the case, the business does not 'trade' in personal information if the information is collected or disclosed for a benefit, service or advantage with the *consent* of all individuals concerned, or is authorised or required by law to collect or disclose the information for a benefit, service or advantage: 'Trading in Personal Information', *Office of the*

of view, or where there is the possibility of a swift growth trajectory, many would be well advised to comply with the *Privacy Act* even before being legally required to do so.[99]

As to whether EdTech companies established outside of Australia have an Australian link, the *Privacy Act* requires that an organisation either meets certain criteria listed in the *Privacy Act*,[100] or carries on business in Australia or an external Territory.[101] The meaning of 'carries on business in Australia or an external Territory', as the term is used in the *Privacy Act*, was litigated in *Facebook Inc v Australian Information Commissioner*.[102] Although that decision dispenses only with the question of whether there was a prima facie case that Facebook carried on business in Australia, it suggests that the absence of a physical presence and of any 'indicia' of carrying on business in Australia will not preclude a finding that an organisation carries on business here.[103] Accordingly, even EdTech providers without a physical presence in Australia may be bound by the *Privacy Act*. The Information Commissioner has noted that '[a]n increasing number of the matters being considered by the Commissioner present factual situations that enliven s 5B(3) of the *Privacy Act*'[104] (ie, the 'Australian link' provisions) and that establishing jurisdiction under this section can be 'resource intensive'.[105]

Given the notice and consent model on which current privacy laws are based, even those EdTech providers bound by the *Privacy Act* are able to collect and use a wide range of personal information for a broad array of purposes, subject to taking reasonable steps to notify individuals of what is collected and why, and in

---

Australian Information Commissioner (Web Page) <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/trading-in-personal-information>.

99 Small businesses and non-profit organisations may choose to signal a public commitment to upholding the APPs and being bound by the *Privacy Act* (n 88) by 'officially' opting in to it and registering with the OAIC. The OAIC maintains a register of small business and not-for-profit organisations that have opted in: 'Privacy Opt-In Register' *Office of the Australian Information Commissioner* (Web Page) <https://www.oaic.gov.au/privacy/privacy-registers/privacy-opt-in-register> which, as of August 2025, listed 794 organisations that had opted in. How many (if any) of those would be considered a business within the EdTech sector has not been investigated for purposes of this research.

100 *Privacy Act* (n 88) s 5B(2).

101 Ibid s 5B(3)(b). Previously an organisation was also required by section 5B(3)(c) to 'collect or hold personal information in Australia', which caused interpretive issues: see *Facebook Inc v Australian Information Commissioner* (2022) 289 FCR 217, 243 [108] (Perram J) ('*Facebook*'). That section was repealed by the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth) s 10.

102 *Facebook* (n 101). The Information Commissioner had sought leave of the Federal Court to serve documents on Facebook Inc in connection with the Cambridge Analytica scandal, the requirement for leave being enshrined in the then applicable *Federal Court Rules 2011* (Cth). This required the OAIC to demonstrate that there was a prima facie case that Facebook Inc was carrying on business in Australia, within the meaning of the Australian link provisions in the *Privacy Act* (n 88). Facebook submitted that it had no physical presence in Australia in that it 'entered into no contracts, employed no personnel, had no customers and derived no revenues': *Facebook* (n 101) 233 [67] (Perram J). The Full Court found that the absence of a physical presence in Australia did not preclude a finding that Facebook was carrying on business in Australia and that this was consistent with the objects and focus of the *Privacy Act* (n 88): *Facebook* (n 101) 234 [70] (Perram J, Allsop CJ agreeing at 218 [1], Yates J agreeing at 255 [166]).

103 *Facebook* (n 101) 235 [74] (Perram J).

104 Office of the Australian Information Commissioner, Submission to Attorney-General's Department (Cth), *Review of the Privacy Act 1988 Issues Paper* (11 December 2020) 113 [8.28].

105 Ibid 114 [8.31].

some cases to gain their consent to the collection or use of the information.[106] Any requirements to notify individuals about the collection of their personal information and the purpose or purposes for which it is collected, or to gain consent to the collection or use of information, are usually managed through broadly worded privacy policies and collection notices.[107]

The *Privacy Act* itself does not prevent the collection or use of children's personal information. Nor does it stipulate a fixed age at which a person should be considered capable of consenting to the collection of their personal information.[108] Despite this, some EdTech providers always require parental consent for the collection of information from students under 18,[109] or under a stipulated age.[110] In other cases, EdTech companies (theoretically) restrict their services to users over a certain age. These requirements may be put in place to allow the provider to comply with laws in some of the other jurisdictions in which they operate.[111] Recent reforms to the *Privacy Act* require the drafting of a Children's Online Privacy Code which will apply to online services likely to be accessed by children: some provisions of the (yet to be drafted) code may prevent certain activities in relation to children's information. The Children's Online Privacy Code is considered in more detail in Part V, below.

---

106 *APPs* (n 85) sub-cl 3.3 provides that an APP entity must not collect 'sensitive information' about an individual unless that individual consents, and the information is reasonably necessary for at least one of the entity's functions or activities (or in the case of agencies, directly related to one or more of those functions or activities). *APPs* (n 85) APP 6 requires that personal information should not be used for a secondary purpose unless the individual has consented to use for that purpose or where the organisation is able to rely on another ground listed in sub-clause 6.2 or 6.3.

107 The fact that privacy policies are broadly and often vaguely worded is discussed further in Part III.

108 Although the OAIC provides guidance on meeting consent requirements in relation to personal information of those under 18: Office of the Australian Information Commissioner, 'Australian Privacy Principles Guidelines: *Privacy Act 1988*' (Guidelines, July 2019) 13 [B.58] which provide:

> If it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.

109 See, eg, 'Privacy Policy', *Mathspace* (Web Page, 16 October 2023) <https://mathspace.co/au/privacy-policy>.

110 In practice, whenever EdTech companies require parental consent, and where information is provided to the company by schools, it is the schools that manage this consent process. See, eg, 'Third Party Consent Catalogue: Bundled'(n 64).

111 Such as, in the US, the *Children's Online Privacy Protection Act of 1998*, 15 USC §§ 6501–6 (1998) – a federal law requiring operators of websites or online services directed to children to (among other things) obtain 'verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children': at §6502(b)(1)(A)(ii). A child is defined for the purpose of the rule as a person under 13 years of age: at §6501(1). In the European Union ('EU'), the *GDPR* provides that children under 16 are not able to consent to the processing of their personal data, although member states are able to reduce this age, but not to below 13: *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, arts 6(1), 8(1) ('*GDPR*').

The APPs only apply to the collection, handling, use and disclosure of 'personal information', as defined in the *Privacy Act*.[112] As discussed above, while EdTech companies and third-party organisations often collect personal information about users (names, dates of birth and so on) they also collect information about users' devices, IP addresses, location information and browser information (so-called 'technical information'), and they also infer information about individual users. Technical and inferred information is nevertheless capable of 'individuati[ng]' users: that is, it enables users to be 'single[d] out', even if their identity is not known,[113] and can allow that person to be targeted or otherwise acted upon. As Salinger Privacy has explained in its response to the *Privacy Review Report*:

> It is our strong submission that rapid advances in technologies, including artificial intelligence and facial recognition, and business practices involving probabilistic and other forms of data linkage, mean that 'not identifiable by name' is no longer an effective proxy for 'will suffer no privacy harm'.[114]

Given the uncertainty about whether technical and inferred information can always be considered personal information within the meaning of the *Privacy Act*,[115] proposed Australian privacy law reforms recommend amending the definition of 'personal information' to clarify that it applies to technical, de-identified and inferred information relating to an individual.[116] Despite the Australian Government 'agree[ing] in-principle',[117] these recommendations have not found themselves into the first tranche of reforms passed by the *Privacy and Other Legislation Amendment Act 2024* (Cth) ('*Privacy Amendment Act*'). Until those reforms are progressed, there is a risk that some of the information gathering activities of EdTech organisations and third parties may be unregulated under the *Privacy Act*,[118] and even with this change, doubts have been expressed about whether it will resolve the existing state of confusion as to when an individual is 'reasonably identifiable'.[119]

---

112 *Privacy Act* (n 88) s 6(1) (definition of 'personal information') defines personal information as:

> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
> (a) whether the information or opinion is true or not; and
> (b) whether the information or opinion is in a recorded form or not.

113 Salinger Privacy, 'The Definition of Personal Information' (Research Paper, Office of the Australian Information Commissioner, 17 February 2020) 1 <https://www.oaic.gov.au/__data/assets/pdf_file/0012/1308/definition-of-pi.pdf.pdf>. Salinger Privacy also remark on an apparent mistake in how the concept of 'individuation' is understood in the *Privacy Review Report* (n 47): Salinger Privacy, Submission No 800054720 to Attorney-General's Department (Cth), *Government Response to the Privacy Act Review Report* (31 March 2023) 14–15 <https://www.salingerprivacy.com.au/wp-content/uploads/2023/03/23-03-31_Privacy-Act-Review_Salinger-Privacy-Submission.pdf> ('Salinger Response').

114 Salinger Response (n 113) 14.

115 *Digital Platforms Report* (n 68) 393.

116 *Privacy Review Report* (n 47) 23–37.

117 Australian Government, 'Government Response: Privacy Act Review Report' (Response, 2023) 5 <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF> ('Government Response').

118 Salinger Response (n 113) 12–22.

119 Ibid 12–16.

3 Australian Schools: Application of the Australian Privacy Laws

Whether a school needs to comply with the *Privacy Act* depends primarily on whether it is a government or non-government school. Government schools make up the majority (close to 70%) of schools in Australia,[120] accounting for 64% of all students enrolled in Australian schools in 2023.[121] Non-government schools usually have a religious affiliation,[122] with Catholic schools accounting for just over 18% of all schools in Australia and independent schools for the remainder.[123]

The majority of non-government schools are bound by the *Privacy Act* and will need to comply with the APPs;[124] government schools, on the other hand, as agencies within the state public sector, are usually not subject to the *Privacy Act* or the APPs.[125] As previously noted, however, all states and territories have privacy principles that apply to the state public sector and which, therefore, apply to government schools. In addition, some states have health records laws that operate in addition to (although with some overlap with) information privacy principles. In this article, the application of health records laws to schools or EdTech providers is not further considered.

As with EdTech providers, most schools manage legal requirements imposed by either the APPs or the principles applicable in their jurisdiction through privacy policies and standard collection notices. These policies and notices inform students, parents and others about the broad range of information collected by the school, the purposes for which it is (or may) be used, and the persons and entities to whom it is (or may) be disclosed. Some schools may choose to (or even be expected to)[126] undertake privacy impact assessments when selecting or using new EdTech products. However, when schools are merely recommending EdTech products for use in the classroom, or otherwise, and are not themselves entering personal information into the products, there are no requirements to comply with privacy laws or conduct privacy impact assessments. There may nevertheless be policy requirements that influence the processes schools adopt before recommending EdTech products: these are discussed briefly in the next section.

4 Policy Overlay

Both government and non-government schools need to comply with a range of policies set by state education departments, or by body corporates or other

120 Australian Curriculum, Assessment and Reporting Authority, *National Report on Schooling in Australia 2023* (Report, 26 June 2024) 4 <https://dataandreporting.blob.core.windows.net/anrdataportal/ANR-Documents/nationalreportonschoolinginaustralia_2023.pdf>.

121 Ibid.

122 Ibid.

123 Ibid 19.

124 'Children and Young People', *Office of the Australian Information Commissioner* (Web Page) <https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/children-and-young-people>.

125 The definition of 'agency' in the Act and for the purpose of considering whether an entity must comply with the *APPs* (n 85) is set out in *Privacy Act* (n 88) s 6(1) (definition of 'agency').

126 A report by the OVIC into the use of EdTech in Australian primary schools reports that '[s]ome of the schools we met with were not aware that they were expected to complete PIAs [privacy impact assessments]': *OVIC Examination Report* (n 57) 5.

governing bodies respectively, pertaining to their use or recommendation of EdTech products. Reviewing all these different frameworks is beyond the scope of this article. However, Pangrazio and Anna Bunn compared some key aspects of Department of Education ('DoE') policies on the selection of EdTech products in government schools in New South Wales ('NSW'), Victoria and WA.[127] They note that schools in WA have less autonomy than their NSW and Victorian counterparts to procure EdTech products as they are restricted to using only those products that are provided under licence by that state's DoE, or that have undergone a risk assessment by the Department.[128] They also note that the DoE in each of these states pre-assesses a range of different EdTech products but that 'none of the risk assessments, risk ratings and underpinning methodology is publicly available'.[129] Pangrazio and Bunn also note that schools in each state bear the responsibility for notifying parents of the use of third-party products and, in some cases, seeking parental consent to the collection of personal information by the EdTech providers. The authors remark on the fact that each school sector (government, Catholic and independent) and each state jurisdiction has its 'own processes of procurement and quality assurance shaped by different priorities and values'.[130]

IV SCHOOLS: GATEKEEPING AND MODELLING 'BEST PRACTICE'

UN General Comments are 'a means by which a UN human rights expert committee distils its considered views on an issue … and presents those views in the context of a formal statement of its understanding to which it attaches major importance'.[131] General Comments are regarded as 'central to understanding human rights treaty obligations'[132] and a necessary interpretative aid for the *CRC* given that its language is 'quite general', with intentionally 'built-in' elasticity.[133] *General Comment No 25 (2021) on Children's Rights in Relation to the Digital Environment* ('*General Comment No 25*') is designed to explain how the *CRC*

127 Luci Pangrazio and Anna Bunn, 'Assessing the Privacy of Digital Products in Australian Schools: Protecting the Digital Rights of Children and Young People' (2024) 6 *Computers and Education Open* 100817:1–8 <https://doi.org/10.1016/j.caeo.2024.100187>.

128 Ibid 4.

129 Ibid.

130 Ibid.

131 Philip Alston, 'The Historical Origins of the Concept of "General Comments"' in Laurence Boisson de Chazournes and Vera Gowland-Debbas (eds), *The International Legal System in Quest of Equity and Universality* (Martinus Nijhoff Publishers, 2001) 763, 764 <https://doi.org/10.1163/9789004479012_043>.

132 Helen Keller and Leena Grover, 'General Comments of the Human Rights Committee and Their Legitimacy' in Helen Keller and Geir Ulfstein (eds), *UN Human Rights Treaty Bodies: Law and Legitimacy* (Cambridge University Press, 2012) 116, 117–18 <https://doi.org/10.1017/CBO9781139047593.005>.

133 Cynthia Price Cohen and Susan Kilbourne, 'Jurisprudence of the Committee of the Rights of the Child: A Guide for Research and Analysis' (1998) 19(3) *Michigan Journal of International Law* 633, 642.

should be implemented in the digital environment.[134] In relation to the use of educational technologies, it provides as follows:

> Standards for digital educational technologies should ensure that the use of those technologies is ethical and appropriate for educational purposes and does not expose children to violence, discrimination, misuse of their personal data, commercial exploitation or other infringements of their rights, such as the use of digital technologies to document a child's activity and share it with parents or caregivers without the child's knowledge or consent.[135]

The obligation to develop such standards (as with other obligations arising from the *CRC*) falls upon States Parties and, as such, applies directly to government education authorities. However, all schools – even non-government schools – have an important role to play in affording children the full range of their *CRC* rights, not least because they are places where children spend a large portion of their time and because they occupy a position of considerable authority, as well as influence. As Emma Nottingham, Caroline Stockman and Maria Burke have remarked, COVID-19 provided opportunities for EdTech companies to gain 'increased influence over the education sector' and has 'helped to cement data-intrusive norms in the schooling environment'.[136] Therefore, to afford children their full range of rights and protect against the misuse of their personal information (as urged in *General Comment No 25*), this article argues that schools should exemplify – and demand – best (or, at least, better) practice in relation to this information. There are three reasons why better practice is needed, each of which is explored below.

A Parental Consent Model is Unsatisfactory

Schools are often required (by law or policy) to seek parental consent to the data practices of EdTech organisations. This is unsatisfactory for reasons related to privacy policy length, complexity and opacity; the information practices of EdTech providers; and the trust placed in schools by parents. These reasons mean that it is not possible to say that consent is 'informed'. Additionally, *meaningful* choice as to whether or not to consent is often absent, in which case consent is not 'freely given'. From the child rights perspective, this is unsatisfactory because consent needs to be informed and freely given by the child, or a parent/caregiver (where the child does not have the capacity to consent).[137]

The Office of the Australian Information Commissioner ('OAIC') *Community Attitudes to Privacy Survey* of 2023 found that 54% of parents lack the time to read privacy policies for the services used by their child.[138] This is unsurprising given the 'length, complexity and ambiguity' of online terms and conditions and privacy policies.[139] The Australian Competition and Consumer Commission ('ACCC')

134 *General Comment No 25* (n 10).
135 Ibid 17 [103].
136 Emma Nottingham, Caroline Stockman and Maria Burke, 'Education in a Datafied World: Balancing Children's Rights and School's Responsibilities in the Age of Covid 19' (2022) 45 *Computer Law and Security Review* 105664:1–16, 15 <https://doi.org/10.1016/j.clsr.2022.105664>.
137 *General Comment No 25* (n 10) 12 [71].
138 *Attitudes to Privacy Survey* (n 50) 89.
139 *Digital Platforms Report* (n 68) 23.

found that key characteristics of many privacy policies of large platforms were likely to 'impede consumers' ability to accurately and comprehensively understand' their data practices. These included excessive length, linked external content, vague language and the 'tendency to understate data collection, use and disclosure'.[140] This suggests that many parents will simply provide consent, when requested by the school, to the use of a particular platform or app without reading the relevant privacy policy. What has been termed 'consent fatigue',[141] or 'privacy fatigue',[142] may also contribute, as individuals overwhelmed by consent requests tend to disengage from making meaningful choices. The bundled consent nature of many of these requests in particular makes this a strong possibility.

Parents and guardians may also assume that consent is merely a formality, and that a substantive evaluation of the privacy and other risks has already been undertaken by the school (or the relevant authority). This is supported by the OVIC Examination, which concluded that: 'Parents and carers are likely to assume that the privacy implications of apps and web-based learning tools used by their students have been considered before the tools are rolled out.'[143] In fact, schools may explicitly convey to parents that products hold 'low' or 'minimal' risk.[144]

The volume of third-party apps requiring consent further complicates parental engagement. One WA high school requested bundled consent for 46 different third-party services, offering only all-or-nothing consent options.[145] While some schools provide summaries of personal information collection, these are typically superficial, omitting details about data sharing or student tracking.

Even engaged parents may struggle to comprehend data practices described in privacy policies. The ACCC noted that vague language prevents consumers from determining the exact scope of data collection and usage.[146] Common Sense Media's 2021 *State of Kids Privacy* report found many education apps lack transparency,

---

140 Ibid 402. See also Simon Elvery and Teresa Tan, 'You Read the Terms and Conditions, Right?' *ABC News* (online, 27 February 2025) < https://www.abc.net.au/news/2025-02-27/classroom-apps-technology-kids-data-terms-conditions/104966952>, who examined the length of the terms and conditions and privacy policies of third-party tools that parents were urged to read by schools seeking consent and found that this amounted to 'hundreds of pages of dense legalese'.

141 Bart W Schermer, Bart Custers and Simone van der Hof, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) 16(2) *Ethics and Information Technology* 171, 176 <https://doi.org/10.1007/s10676-014-9343-8>.

142 Hanbyul Choi, Jonghwa Park and Yoonhyuk Jung, 'The Role of Privacy Fatigue in Online Privacy Behavior' (2018) 81 *Computers in Human Behavior* 42 <https://doi.org/10.1016/j.chb.2017.12.001>.

143 *OVIC Examination Report* (n 57) 6 [16]. See also *How Dare They Peep* (n 4) 9, where an Australian school parent commented that she 'just trusted the school had looked into it' when asked about consenting to the use of EdTech in schools during COVID-19.

144 This author, for example, received an email from Lesmurdie Senior High School in WA referring to a number of products in respect of which consent was sought as 'low risk': Email from Lesmurdie Senior High School to Anna Bunn, 22 March 2022. Australind Senior High School in WA informs parents that EdTech products have been thoroughly evaluated by the DoE and are 'minimal risk': 'Third Party Consent Catalogue: Notification' (n 64).

145 'Third Party Consent Catalogue: Bundled' (n 64). Note that one of these services (Kahoot!) was classified as medium risk.

146 *Digital Platforms Report* (n 68) 405, discussing the frequent use of the word 'may', which is ambiguous and denotes various meanings.

typically withholding information about practices, including data monetisation.[147] And Sonia Livingstone et al observed that even expert lawyers were unable to ascertain Google Classroom's actual data collection practices, concluding that it is not surprising that 'schools struggle to grasp the nature, purposes or consequences of education data processing'.[148] If that is true for schools, it is certainly true for parents. Additionally, privacy policies themselves often only disclose the practices of the EdTech provider itself and will not necessarily disclose the practices of third parties who may collect information via cookies, pixels and so on. As Lisa Archbold et al have remarked: 'Given the complexity, opacity and power asymmetries of data processing, it is clear that the obtaining of consent, even augmented by other controls, may not be sufficient to legitimise a data practice.'[149]

Regardless of whether parents understand privacy policies, it is difficult to say that they always have a meaningful choice as to whether to provide consent to the collection and use of personal information by apps and platforms. They may fear educational disadvantages for their children if they withhold consent, and some of the language employed by schools when seeking consent may contribute to this. For example, in its enrolment form section about third-party services used in the school, Australind Senior High School (in WA) writes that these services provide 'a positive benefit to our student learning capabilities'[150] and that 'students who do not have parent consent for the different categories … will not be able to use the Third Party Online Service, in class, during the lesson and will be restrictive [sic] with some assessment tasks'.[151] Bundled consent requests further limit parents' ability to opt out selectively.

Parental consent is, of course, often legally required as a prerequisite to the disclosure by the school of certain student information.[152] However, given the issues referred to above, there is an argument that parents should not even be asked to consent unless the school itself has undertaken its own assessment of the provider's information practices and weighed the risks against the benefits that will accrue to a student from using the EdTech product in question.

Yet, while most schools have a level of autonomy in terms of the choice of EdTech products used within the school and are generally ultimately responsible

147 Girard Kelly et al, Common Sense Media, *State of Kids' Privacy* (Report, 2021) 3. Common Sense Media's most recent *State of Kids' Privacy* report analysed 'the practice of selling data for 200 of the most popular products used by kids and families' and found that 'the majority of companies whose privacy policies say they do not or share users' data to third parties actually have other forms of data monetization practices that would likely be *considered* selling or sharing data under new *California Privacy Rights Act* amendments': Girard Kelly, Jeff Graham and Steve Garton, Common Sense Media, *State of Kids' Privacy* (Report, 2023) 1 (emphasis in original).

148 Livingstone et al (n 37) 4.

149 Archbold et al, 'AdTech' (n 42) 870.

150 'Third Party Online Services Consent Form', *Australind Senior High School* (Web Page, 8 March 2021) <https://web.archive.org/web/20231107064418/https://australind.wa.edu.au/third-party-consent-online-services/>.

151 'Online Services Third Party Consent', *Australind Senior High School* (Web Page, 16 February 2022) <https://web.archive.org/web/20231110174510/https://australind.wa.edu.au/2022-third-party-consent/>.

152 For example, where the information is 'sensitive' personal information and where the child is not considered to have capacity to consent.

for assessing the associated risks, the OVIC Examination found that for some schools, 'considerations such as cost were a greater priority'.[153] The majority of teachers interviewed by Ellie Rennie et al said that cost was a factor in the apps they chose and they would mostly choose free apps.[154] As to whether teachers considered privacy when selecting apps, Rennie et al found that less than half said they did, approximately 16% said they did not, while the remainder

> gave answers that were unclear, indicating that either they did not understand the question or were unable to articulate clearly if they considered privacy when selecting apps. In some responses, teachers demonstrated that they think of privacy mostly in relation to cyber safety.[155]

More recently, research on the use of digital reading platforms found that teachers did not discuss privacy issues at all, thus 'drawing attention to the intangibility of data flows that are not directly situated in practice'.[156]

We can certainly be sympathetic as to why many teachers either do not consider or do not understand the information practices and associated policies of EdTech providers: those are, as noted, often complex and opaque. Yet, digital literacy is one of the general capabilities listed in the Australian Curriculum.[157] Among other things, this envisages students being able to effectively manage online privacy and safety, as well as their digital identities. By the time they reach Years 9 and 10, students are expected to 'manage proactively their personal data, exhibiting integrity across online behaviours and managing the data collection technology used to track their online navigation'.[158] If this is a capability expected of students by the time they reach Year 9 then, arguably, so should it be a capability expected of teachers, particularly as digital literacy is unlikely to be taught as a standalone subject within schools but, rather, integrated across the curriculum. Of course, teachers need to be adequately supported to develop their own capabilities in terms of understanding and managing data collection technologies, something recognised in *General Comment No 25*.[159]

The OVIC Examination even found that some schools were at risk of breaching the Victorian Information Privacy Principles:

> By focussing mainly on the financial aspect of an app or web-based learning tool it is possible for schools to overlook important privacy related issues such as how information is collected, stored and shared by app and web-based learning tool providers. In particular, if a school is choosing an app or web-based learning tool based on its cost, and not properly considering the privacy practices of the provider

153 *OVIC Examination Report* (n 57) 5 [7].

154 Ellie Rennie et al, 'Privacy and App Use in Australian Primary Schools: Insights into School-Based Internet Governance' (2019) 170(1) *Media International Australia* 78, 84 <https://doi.org/10.1177/1329878X19828368>.

155 Ibid.

156 Tiffani Apps, Karley Beckman and Sarah K Howard, 'Valuable Data? Using Walkthrough Methods to Understand the Impact of Digital Reading Platforms in Australian Privacy Schools' (2023) 48(2) *Learning, Media and Technology* 294, 304 <https://doi.org/10.1080/17439884.2022.2160458>.

157 Australian Curriculum, Assessment and Reporting Authority, *General Capabilities: Digital Literacy (Previously ICT)* (Review Report, 2021) 1.

158 Ibid 10.

159 *General Comment No 25* (n 10) 18 [105].

> of the tool it may not properly consider risks associated with information being collected to be on-sold or used for targeted marketing.[160]

In understanding the risks associated with EdTech – including those associated with the collection and use of information – it is unsurprising that schools will rely on resources and guidance provided by education departments (in the case of government schools) or wider organisational units (in the case of non-government schools).[161] Ultimately, however, the adequacy of this guidance and these resources is itself debatable. For example, in WA, the DoE conducts risk assessments for all third-party apps and tools used in schools, and the Victorian DoE provides pre-populated (or partially pre-populated) privacy impact assessments for some, but not all, EdTech products used in schools.[162] However, the methodology underpinning these assessments is unknown and difficult to access.[163]

In NSW, the DoE Online Tools Marketplace lists various products that have either been assessed through the ST4S initiative, or are required to undergo an ST4S assessment.[164] ST4S is described as a 'standardised approach to evaluating digital products and services used by schools across Australia and New Zealand against a nationally consistent security and privacy control framework',[165] and the ST4S initiative involves all Australian state and territory education departments as well as the National Catholic Education Commission and Independent Schools Australia. Yet, as noted by Pangrazio and Bunn, it is 'unclear to what extent (if at all) the education departments in Victoria and WA require ST4S assessment'[166] and 'anecdotal observations' suggest that 'the ST4S framework appears to be used more routinely in departments of education than the Catholic or Independent sector'.[167] There are also other challenges to ST4S assessment becoming a prerequisite to the approval of all EdTech products used in schools: these include resource limitations and issues around terminology.[168] There are also concerns that some of the Big Technology ('BigTech') players may be circumventing assessment under the ST4S framework altogether.[169]

B Compliance with Privacy Laws Does Not Equate to Best Practice

Although schools are naturally focused on compliance with law and policy, the shortcomings associated with the notice and consent model of privacy protection,

---

160 *OVIC Examination Report* (n 57) 20 [75].

161 Such as education commissions (such as the Catholic Education Commission of WA), associations (such as Independent Schools Associations in each state and territory and Independent Schools Australia), and bodies corporate responsible for governance across numerous schools (such as those established in each state and territory to oversee systemic Catholic schools).

162 *OVIC Examination Report* (n 57) 28.

163 The author has requested details of this methodology from the DoE in WA but has been told that the request needs to be considered through the Department's research approval process. Twelve months after submitting that approval request, there have been no developments. See also Pangrazio and Bunn (n 127) 7.

164 Ibid 4.

165 *Safer Technologies 4 Schools* (Website) <https://st4s.edu.au/> ('*ST4S*').

166 Pangrazio and Bunn (n 127) 4.

167 Ibid.

168 Ibid.

169 Ibid 5.

as discussed in the previous section, mean it is unfair and unrealistic to place the onus of managing children's privacy entirely upon parents (or students). Thus, even if EdTech organisations themselves are fully compliant with Australian law (which they may not always be),[170] as observed by the ACCC, 'the existing regulatory frameworks for the collection and use of data have not held up well to the challenges of digitalisation and the practical reality of targeted advertising that rely on the monetisation of consumer data and attention'.[171] In terms of children, specifically, it has been widely recognised in Australia and beyond that they are 'more vulnerable than adults and are less able to understand the long-term implications of consenting to their data collection'.[172] Yet, as Archbold et al have remarked, 'the reliance on technology places commercial service providers at the centre of students' schooling environment'.[173]

From a child rights perspective, this is problematic not least because *General Comment No 25* requires that digital educational technologies should not 'expose children to … misuse of their personal data, commercial exploitation or other infringements of their rights'.[174] Moreover, the call made in *General Comment No 25* for outright prohibition of 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'[175] suggests very clearly that such practices are not in a child's best interests. As such, it is suggested that schools have a role to play in moving beyond 'good practice' in relation to the protection of students' information – as demonstrated by compliance with legal 'minimum standards' – towards 'best practice' or at least (and perhaps more accurately given that there is no universally accepted best practice standards) better practice. What better practice might look like is explored further in Part V.

C Exerting Influence through Policy and Practice

At the time of writing, only some of the privacy law reforms recommended by the Attorney-General, and referred to earlier in this article, have been laid before Parliament. Aside from the requirement to develop a Children's Online Privacy Code, other recommendations relating to children and their data have been deferred. Regardless of when these reforms occur, or what form the legislation takes, individual schools – and their overarching authorities – are well-placed to drive at least some changes in the data practices of EdTech companies. Beyond this, there is a compelling argument that they have a responsibility to do so. As recognised in *General Comment No 1 (2001): Article 29(1)* on the aims of education: 'Every child has the right to receive an education of good quality which

170 *OVIC Examination Report* (n 57) 17–18.
171 *Digital Platforms Report* (n 68) 3.
172 Byrne, Day and Raftree (n 19) 4. See also *GDPR* (n 111) recital 38, which states that: 'Children merit specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned, and their rights in relation to the processing of personal data.'
173 Archbold et al, 'Children's Privacy in Lockdown' (n 35) 22.
174 *General Comment No 25* (n 10) 17 [103].
175 Ibid 7 [42].

in turn requires a focus on the quality of the learning environment, of teaching and learning processes and materials, and of learning outputs.'[176] As the use of EdTech is often an integral part of the learning environment, as well as part of the teaching and learning process and materials, schools and education authorities should be responsible for assessing the quality of the EdTech – from both a pedagogical and a rights-based perspective.

That schools will continue to have a role in this space is clear when considering that some EdTech providers may not even meet their legal obligations. For example, Livingstone et al refer to a fine levied on Google by the French data protection authority for violations of the *GDPR*, including its failure to conduct a Data Protection Impact Assessment and to identify areas of risk.[177] As Nottingham, Stockman and Burke observe in relation to the UK's *Age Appropriate Design Code* ('*UK Children's Code*'), enforcement may continue to present difficulties if technology companies see profit in data breaches, 'despite having to pay a hefty fine'.[178]

One way schools might insist on better data practices – or avoid particular practices –is by negotiating relevant contractual terms when procuring EdTech products or licences. The higher the contract value for the EdTech provider, the more bargaining power the school or authority will have in negotiating terms.[179] Extending this idea, it has been proposed (in the UK context) that schools may form data trusts that work to negotiate and promote the rights of the schools, parents and students in relation to personal data shared with EdTech providers.[180] However, given the need to establish bespoke governance mechanisms (including the appointment of a board and a data trustee), this would only be worthwhile where the particular EdTech product was significantly integrated into school administration or teaching and learning. In many cases, however, the EdTech product in question is provided 'free' and schools have little opportunity to individually negotiate terms that depart from the provider's standard conditions.

Another option is for schools or education authorities to adopt a policy of only using EdTech products and providers that meet privacy standards higher than those

176 Committee on the Rights of the Child, *General Comment No 1 (2001): Article 29(1)*, UN Doc CRC/GC/2001/1 (17 April 2001) 7 [22].

177 Livingstone et al (n 37) 6.

178 Nottingham, Stockman and Burke (n 136) 10.

179 One option could be to require the provider to attach a bespoke privacy policy to the contract that relates specifically to the product being used in the school. This is in contrast to the tendency for large organisations to develop one privacy policy that applies to several different products and services. For example, the privacy policy applicable to Minecraft Education has to be distilled from the Microsoft Privacy Statement. A privacy policy or statement, incorporated in a contract, could also clarify how data is combined (if it is combined) across different products or services: see, eg, Livingstone et al (n 37) 3, who note that the French data protection authority 'underscored the further confusion created by the plethora of services (eg, YouTube, Google Maps and Gmail) and the lack of information about how data were [sic] combined across them'. Contracts could also require providers to undertake that students using their educational products are not given access to additional services: see, eg, at 5.

180 AI Council (UK) and Ada Lovelace Institute, *Exploring Legal Mechanisms for Data Stewardship* (Final Report, March 2021) 47 <https://www.adalovelaceinstitute.org/wp-content/uploads/2021/03/Legal-mechanisms-for-data-stewardship_report_Ada_AI-Council-2.pdf>.

currently required by law. For example, schools (or education authorities) might refuse to use or recommend EdTech products that clearly monetise student data or enable student profiling. Alternatively – since this could exclude many free but potentially valuable EdTech products and disadvantage resource-limited schools – explicit requirements could be introduced requiring such products to be carefully evaluated to ensure that the pedagogical and other benefits to the students justify any associated data risks. In other words, a conclusion would need to be reached that despite the risks involved, it is (on balance – given the pedagogical or other value of the product to the student) in students' best interests for the particular product to be used. This is significant, as at least one study has noted variability in the evidence that the use of EdTech in the classroom results in positive gains for students.[181]

Conducting such assessments within individual schools would be challenging, however – not least because schools often lack the resources or the expertise to determine whether the benefits outweigh the risks, at least in terms of those associated with an entity's data practices.[182] And as Emma Day et al observe, 'any risk-benefit analysis of children's data processed by EdTech remains contested on pedagogic, economic, inclusion and/or data protection and privacy grounds'.[183] Yet even an imperfect analysis could serve as a counterpoint to the current practice, where the use of EdTech in the classroom and associated data surveillance practices are more or less normalised.[184] Indeed, Nottingham, Stockman and Burke recommend conducting a child rights impact assessment in the digital schooling context and comment that this assessment would 'need to appropriately balance the best interests of the child and ensure that the interests of the children in receiving an education are not used as a reason to allow third-party data processing to take place for unethical commercial purposes'.[185]

Analyses conducted at a higher level – for instance, by education departments or other school authorities – are more realistic and to some extent, as explained above, this already occurs in Australia. However, the methodologies behind these analyses are often unclear and it is likely they focus more on compliance than children's rights and best interests.

Greater consistency – and an arguably fairer[186] and more efficient evaluation process – could be achieved by adopting a national standard for assessing

---

181 Cathy Lewin et al, Education Endowment Foundation, *Using Digital Technologies to Improve Learning: Evidence Review* (Report, December 2019) <https://educationendowmentfoundation.org.uk/public/files/Using_Digital_Technology_to_Improve_learning_Evidence_Review.pdf>; Stringer, Lewin and Coleman (n 29) 6–7.

182 Day et al note that 'the operation of EdTech services can be obscure even for lawyers' and that, given issues with transparency in the operations of large EdTech companies, 'hard-pressed schools often face little choice in practice but to trust the assurances they receive from EdTech and agree on a contract': Emma Day et al, 'Who Controls Children's Education Data? A Socio-Legal Analysis of the UK Governance Regimes for Schools and EdTech' (2024) 49(3) *Learning, Media and Technology* 356, 363 <https://doi.org/10.1080/17439884.2022.2152838>.

183 Ibid 358 (citations omitted).

184 Apps, Beckman and Howard (n 156) 306; Sonia Livingstone and Julian Sefton-Green, *The Class: Living and Learning in the Digital Age* (New York University Press, 2016) 140.

185 Nottingham, Stockman and Burke (n 136) 12.

186 See Day et al (n 182) 364.

EdTech providers. Such a standard does, in fact, already exist in Australia: the ST4S assessment process, referred to above. The ST4S process is administered by Education Services Australia, a not-for-profit company that is owned by all Australian state and territory education ministers, as well as the Commonwealth Government Education Minister. The framework itself has been developed collaboratively with all Australian school jurisdictions and the New Zealand Ministry of Education.[187] Its aims are to provide 'an assessment approach with transparent requirements and standards' as well as 'summary reports aimed at reducing risks to schools when choosing digital products and services'.[188]

The ST4S assessment framework is updated twice a year and some of the questions reflect an approach to assessment that extends beyond measuring compliance with legal and other standards, including privacy principles. For example, one question asks whether the service's application development has the characteristic of 'privacy-by-design'.[189] In December 2023, the framework was amended to introduce a question about whether the organisation or service uses, shares, publishes or provides access to any user data (including where de-identified, aggregated etc) for 'advertising, market research or similar purposes'.[190] Another recent update incorporates a section on the use of artificial intelligence ('AI') in services.[191] ST4S also operates a badge program to allow schools to easily identify providers that have been through assessment. Among other criteria, those who participate in the badge program must have been through a recent assessment and must not display advertising, nor 'use or share information (including where de-identified) for advertising, marketing, promotional or similar purposes'.[192]

The ST4S process is a step in the right direction, but imperfect. Currently, participation in the ST4S process appears to be largely voluntary,[193] and as ST4S has no standing funding and relies on product funding, it is likely that the ST4S Assessment Team does not have the resources to assess all suppliers who wish to be considered.[194] Additionally, providers may still be considered compliant (albeit not entitled to an ST4S badge) even though they *do* use, share, publish or provide access to user data for advertising, market research or similar purposes.[195] In itself, this may be misleading. There is also an issue about how school authorities

187 *ST4S* (n 165).

188 Ibid.

189 Although what is meant by this is not further explained: Safer Technologies 4 Schools Team, 'Safer Technologies for Schools Assessment: Supplier Guide' (Guide, 17 July 2024) [6.2.8] <https://st4s.edu.au/wp-content/uploads/2024/07/Safer-Technologies-4-Schools-Supplier-Guide-2023.2-v1.1.pdf> ('ST4S Supplier Guide').

190 Ibid [6.3.2].

191 Ibid [6.9].

192 'ST4S Product Badge Program', *Safer Technologies 4 Schools* (Web Page, March 2025) <https://st4s.edu.au/badge-program/>.

193 Although in NSW it is a requirement that products listed in the Online Marketplace will have gone through ST4S assessment (or will undertake to do so): Pangrazio and Bunn (n 124) 4.

194 For example, the 'ST4S Supplier Guide' (n 189) advises suppliers that: 'Each assessment period a limited number of services can undergo a full ST4S Assessment' and that eligible suppliers will be prioritised based on 'members' needs and consultation with their schools.': at [1.5]–[2].

195 Pangrazio and Bunn (n 127) 4.

interpret ST4S results. As noted by Pangrazio and Bunn, for example, some states use the word 'passed' for EdTech services that are considered ST4S compliant, while others use the word 'endorsed', potentially undermining consistency across educational jurisdictions,[196] and even legitimising practices that are of concern (such as using user data for advertising, market research, or similar). Moreover, other than in the case of independent schools, results of an ST4S assessment are not directly communicated to schools by the ST4S team.[197]

More fundamentally, there remains a question about whether education authorities allow BigTech players, such as Google or Microsoft, to bypass the ST4S assessment process entirely.[198] Part of the problem here is the general difficulty of ascertaining what methodology education departments use to assess the privacy and security of digital products used in schools. While some jurisdictions are relatively open, others make it very difficult for researchers to determine how digital products are assessed.[199] In short, while the ST4S initiative is undoubtedly valuable, there are some limitations. To address concerns over the collection and use of children's data by EdTech products used in schools, the ST4S process would need to be consistently used and applied across all school jurisdictions. Education authorities would ideally mandate that any EdTech product used in schools had undergone an ST4S assessment and achieved a 'compliant' outcome, and may need to go even further and consider whether an ST4S badge (with its more stringent requirements) should be a prerequisite, at least in some circumstances. For this to occur, significant resourcing would need to be channelled into the ST4S initiative to increase its assessment capacity.

The resourcing issue could partially be resolved if schools were required or encouraged (eg, by education authorities) only to use EdTech products that have undergone a sufficiently recent ST4S *self-assessment* and achieved a satisfactory outcome.[200] Currently, self-assessment is the first step in the assessment process. It involves organisations completing a 'readiness check' to determine whether they are ready to undergo a full assessment. The readiness check is less detailed than the full assessment,[201] and to be of any real benefit to schools it would at least need to include questions that assess the extent to which the relevant product avoids 'risky' privacy practices (such as profiling and use of data for advertising and marketing). It would ideally also do more than indicate whether an organisation is ready to undergo full assessment but would, instead, seek to assign an initial risk

196 Ibid.
197 'ST4S Supplier Guide' (n 189) [3.1].
198 Pangrazio and Bunn (n 127) 5.
199 Ibid 7.
200 'ST4S Readiness Check', *Safer Technologies 4 Schools* (Web Page) <https://st4s.edu.au/readiness-check/>.
201 This survey itself is not accessible until an organisation registers with ST4S, but the questions that comprise the readiness check are set out in the Supplier Guide: 'ST4S Supplier Guide' (n 189) [2.1]. The question about whether the organisation uses or shares user data for the purpose of advertising or marketing etc is not included in the readiness check.

rating.[202] Even then, a 'satisfactory' self-assessment outcome cannot carry the same weight as an independent assessment, particularly if there are no pre-determined consequences for organisations who produce an inaccurate assessment.[203]

In summary, schools (and their overarching authorities) have greater capacity to understand the data practices of EdTech providers than do parents and students. Schools and education authorities also have greater capacity to insist on *better* practices: to move beyond legal compliance and focus on the best interests of the child. Yet clearly there are challenges for schools in terms of expertise and resourcing. Schools therefore need adequate support from education departments and other organisations and access to better assessment tools or more resourcing for existing tools.

Ultimately, however, ensuring that children's privacy and other rights implicated by data practices are adequately protected should not be a matter only for users (whether children, parents or the schools themselves). Greater responsibility needs to be borne by the EdTech providers themselves to adopt better practices and to build in privacy (and safety) by design. Partly towards achieving this end, privacy law reforms have been recommended by the Australian Attorney-General in the most recent privacy law review. The recommendations reflect a changing perspective on allocation of responsibility for information privacy, but it remains to be seen whether all recommendations will be enacted and, if they are, where they will lead.

V BETTER PRACTICE AND PRIVACY LAW REFORMS

Although there is no recognised 'gold standard' of protection for children and young people in terms of how their information is collected and used, the *GDPR*[204] has been described as a 'global benchmark in data protection'.[205] Its standards have been translated and applied to children's use of digital services, including through the statutory *UK Children's Code*[206] and the Irish Data Protection Commission's guidance on protecting children's data, included in 'Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing' ('Fundamentals').[207] The *UK Children's Code* is focused on designing in privacy

202 Although, as is noted in the 'ST4S Supplier Guide' (n 189), the fact that a product is 'high risk' does not necessarily mean it should not be used – sometimes this is an unavoidable outcome: at [2.2.3]–[2.2.4].

203 Although promoting an incorrect self-assessment outcome could potentially form the basis of an action under the *Australian Consumer Law* for misleading or deceptive conduct or representations: *Competition and Consumer Act 2010* (Cth) sch 2 ss 18, 29.

204 *GDPR* (n 111).

205 Archbold et al, 'AdTech' (n 42) 866.

206 *UK Children's Code* (n 55).

207 Data Protection Commission (Ireland), 'Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing' (Guidance, December 2021) <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> ('Fundamentals'). Other jurisdictions are considering similar codes. These include (but are not necessarily limited to) the European Commission, which is facilitating an EU code of conduct for age-appropriate design: 'Special Group on the EU Code of Conduct on Age-Appropriate

to all 'information society services which are likely to be accessed by children',[208] whereas the 'Fundamentals' are somewhat broader and intended to apply beyond the 'engineering and design of online products and services'.[209] Both are underpinned by the best interests of the child principle,[210] and both contain provisions related to profiling,[211] data minimisation,[212] and the use of location tracking[213] and nudge techniques.[214]

Taken together, these standards can be said to represent best (or better) practice in terms of children's privacy and data rights than is represented by Australian law in its current state. However, following the *Privacy Amendment Act*, the *Privacy Act* has now been amended to require that the Information Commissioner develop a Children's Online Privacy Code applicable to relevant services likely to be accessed by children.[215] The Code must be developed and registered within 24 months of the date that the *Privacy Amendment Act* received Royal Assent: therefore by 10 December 2026.[216] At the time of writing, the Code is still in development, with a draft set to be released for public consultation in 2026.[217] However, the *Privacy Review Report* recommended that it could 'to the extent possible' align with 'the scope of the UK Age Appropriate Design Code'.[218] If it is so aligned, the Children's

---

Design', *European Commission* (Web Page, 20 September 2023) <https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design>. 'Providers of very large online platforms' are already required to take into account the 'best interests of minors' when 'taking measures such as adapting the design of their service and their online interface, especially when their services are aimed at minors or predominantly used by them': *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)* [2022] OJ L 277/1, 24. Furthermore, a joint resolution of Canadian privacy commissioners and others has called for the introduction of an age-appropriate design code: Office of the Privacy Commissioner of Canada et al, 'Putting Best Interests of Young People at the Forefront of Privacy and Access to Personal Information' (Joint Resolution, 4–5 October 2023) <https://www.priv.gcage .ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_231005_01/>. In the US, the *California Age-Appropriate Design Code Act*, Cal Civ Code (West 2023) was also passed but then successfully challenged in the United States District Court of California on the grounds of unconstitutionality and subject to a preliminary injunction: *NetChoice LLC v Bonta*, 692 F Supp 3d 924 (ND Cal, 2023). That decision was appealed to the Ninth Circuit: *NetChoice LLC v Bonta*, 113 F 4d 1101 (9th Cir, 2024). The outcome was that the preliminary injunction applied by the District Court was affirmed in part but vacated in part. NetChoice then filed for a second preliminary injunction, upheld in full in *NetChoice LLC v Bonta*, 770 F Supp 3d 1164 (ND Cal, 2025), with that decision, as at June 2025, pending appeal to the Ninth Circuit.

208 *Data Protection Act 2018* (UK) s 123(1).

209 'Fundamentals' (n 207) 3.

210 Ibid.

211 *UK Children's Code* (n 55) standard 12; 'Fundamentals' (n 207) 14.

212 *UK Children's Code* (n 55) standard 8; 'Fundamentals' (n 207) 64.

213 *UK Children's Code* (n 55) standard 10; 'Fundamentals' (n 207) 64.

214 *UK Children's Code* (n 55) standard 13; 'Fundamentals' (n 207) 64.

215 *Privacy Act* (n 88) s 26GC.

216 The *Privacy and Other Legislation Amendment Act 2024* (Cth) ('*Privacy Amendment Act*') received Royal Assent on 10 December 2024.

217 Kate Bower, 'Sunshine and Double Rainbows: Building a Better Online Environment for Children and Young People', *Office of the Australian Information Commissioner* (Blog Post, 15 April 2025) <https://www.oaic.gov.au/news/blog/sunshine-and-double-rainbows-building-a-better-online-environment-for-children-and-young-people>.

218 *Privacy Review Report* (n 47) 157.

Code will place greater responsibility on EdTech providers to protect children's data and their privacy. In the meantime, however, the *UK Children's Code* and the 'Fundamentals' can serve as examples of what schools could require now, in terms of the practices of EdTech providers.

The *Privacy Review Report*,[219] released in February 2023, built on work done by the previous government in response to the ACCC *Digital Platforms Inquiry* final report in 2019. Aside from the recommended introduction of a Children's Online Privacy Code, the *Privacy Review Report* proposed other changes that will, if enacted, have a bearing on some of the data practices described in Part III. Specifically, it recommended prohibitions on trading in the personal information of children, direct marketing to a child (unless using personal information collected directly from the child and where the direct marketing is in the child's best interests), and targeting to a child (unless such targeting is in the child's best interests).[220] The proposed definition of 'targeting' extends to the collection, use and disclosure not only of 'personal information' but also of 'deidentified' and 'unidentified' information. This prohibition would therefore represent a significant change in the context of the EdTech market. It was also recommended that the *Privacy Act* apply to small businesses, albeit after a period of further consultation and impact analysis[221] – a change that would extend the application of the *Privacy Act* to smaller EdTech providers not currently bound by it. Even pending extension of the Act to all small businesses, however, the *Privacy Review Report* recommended removing the exemption for any small business that trades in personal information, even with consent.[222]

Additionally, the *Privacy Review Report* recommended a number of other protections, some of which would apply specifically to children (to be defined as those under 18), and amendments to the definition of personal information (clarifying that it is information that is connected to, but not necessarily 'about' a reasonably identifiable individual, and providing non-exhaustive examples of personal information).[223] The *Privacy Review Report* also recommended including a requirement that the collection, use and disclosure of personal information be fair and reasonable in the circumstances[224] – extending the current requirement that only the means of collection be lawful and fair[225] – and that entities bound by the Act must have regard to the best interests of the child in determining whether the collection, use and disclosure of personal information is reasonable in the circumstances.[226]

There is no doubt that these recommendations would, if enacted and appropriately enforced, go some way to better protecting the privacy of students whose information is collected and used by EdTech providers. Placing greater

219 *Privacy Review Report* (n 47).
220 See proposals 20.5–20.7: ibid 12–13.
221 See proposal 6.1: ibid 6.
222 Currently small businesses that have consent to trade in personal information are exempt from the *Privacy Act* (n 88), although those that do this without consent are not: see above n 98.
223 See proposals 4.1–4.2: *Privacy Review Report* (n 47) 5.
224 See proposal 12.1: ibid 8.
225 *APPs* (n 85) sub-cl 3.5.
226 See proposal 16.4: *Privacy Review Report* (n 47) 10.

onus on the providers of services likely to be accessed by children to consider the best interests of the child (or, of children generally) during the design stage and throughout the information life cycle would address many of the criticisms of the current notice and consent regime. This, and the restriction of certain practices (such as targeting to a child and trading in children's personal information) would better reflect a child rights approach and respond to calls made by children and young people themselves as reflected in *General Comment No 25*.

That is not to say the proposals are a perfect solution to all the issues canvassed here. For example, one responder to the *Privacy Review Report* has suggested that the recommendations pertaining to targeting and trading in the personal information of children may not prevent some of the most 'egregious data harvesting about children to continue, in large, vertically integrated companies'.[227] That is, there remains a concern about the vast amounts of information collected about (and from) children – even if this is not used for targeting and is not sold or shared for gain – insofar as this may present data security risks as well as risks of being otherwise 'repurposed' for commercial use.[228] The recommended amendments to the *Privacy Act* may also fail to prevent risks to children that arise when data about parents and other family members (such as that collected through technological means including cookies and pixels) is treated as a 'proxy' for children's data. This is because much information about or relating to children can be gleaned from data gathered from their family members, such as where digital products for children (including EdTech products) require the creation of parent or family accounts in place of children's accounts.[229]

A broader concern relates to the proposed definition of 'personal information' in the *Privacy Act*. Identification of an individual (or the ability to reasonably identify a person) is central to that definition. Yet it has been argued that the ability to individuate a person – to distinguish them from another despite never knowing who they are –nevertheless allows for tracking, surveillance, profiling and targeting and can thus have 'significant detrimental privacy impacts for individuals'.[230] Although the *Privacy Review Report* suggested amending the definition of personal information to clarify that it can include technical information (such as device IDs), it specifically argued that information used to 'individuate' a person should 'remain outside the definition of personal information'.[231] According to Salinger Privacy, the lack of a principles-based approach to individuation (choosing, instead, to regulate particular practices that rely on individuation) will lead to the legislation becoming outdated.[232]

---

227 Reset.Tech Australia, Submission No 296061928 to Attorney-General's Department (Cth), *Government Response to the Privacy Act Review Report* (March 2023) 8 ('Reset Response'). See also ARC Centre of Excellence for the Digital Child, Submission No 795769044 to Attorney-General's Department (Cth), *Government Response to the Privacy Act Review Report* (31 March 2023) 7 ('Digital Child Response').

228 Digital Child Response (n 227) 7.

229 Ibid 8.

230 Salinger Response (n 113) 16. Although, as noted above, the proposed definition of 'targeting' would apply to unidentified and deidentified information.

231 *Privacy Review Report* (n 47) 36.

232 Salinger Response (n 113) 16.

The government's response to the recommendations, released September 2023, indicated agreement in principle with the recommendations discussed above.[233] However, none of these recommendations were included in the first tranche of reforms that have come in with the *Privacy Amendment Act*. It remains to be seen which of these will be included in the second tranche of reforms that the government has committed to introducing in 2025.

Additionally, even though the changes will (if enacted) address some of the concerns raised about EdTech providers' data collection and use practices, there will doubtless be enforcement challenges. The European context is illustrative. Despite extensive obligations under the *GDPR*, it has been shown that some BigTech players do not comply with all aspects of the *GDPR*, even in relation to children's data.[234] Adequate resourcing for enforcement bodies (in Australia, the OAIC) will therefore be crucial given that 'large technology companies … often have more resources than regulatory bodies'.[235] In fact, Reset.Tech Australia has remarked on the comparatively low levels of funding received by the OAIC, when compared to the equivalent regulatory bodies in the UK and Ireland. Commenting on the enforcement experience in the UK and Ireland, Reset.Tech observes that '[c]odes will not simply come to life through voluntary adoption by industry; the OAIC needs a muscular response that requires strong powers and adequate resources'.[236]

The *Privacy Review Report* proposals, if enacted in the form recommended, will likely have the greatest impact on sectors of the EdTech market that are most reliant on the monetisation of data. Those whose business model depends on collecting and using children's information to develop profiles and target information (or to sell this or use it to gain a benefit) will need to find new operating models. A possible consequence of this is that EdTech products that are currently offered free of charge may need to start charging, with the result that some products may become out of reach for some schools or students or would become less attractive propositions. That cannot be said to be an unintended consequence of the reforms. Nevertheless, a somewhat perverse outcome could see BigTech players, such as Google and Microsoft, gain an even greater influence over schools, and education in general, with the potential for 'adverse pedagogical impacts [that] result as education itself is fitted to the logic and interests of "profit-seeking technology providers"'.[237] That is not (or not just) a data-protection problem, but implicates much broader questions about educational influence and access, and

233 'Government Response' (n 117).

234 Livingstone et al (n 37) 3.

235 Centre for Responsible Technology, Australia Institute, Submission No 1065763983 to Attorney-General's Department (Cth), *Privacy Act Review: Discussion Paper* (December 2021) 11.

236 Reset Response (n 227) 17. The *Privacy Amendment Act* (n 216) does introduce a tiered penalty scheme which provides a greater range of enforcement options for the OAIC, including the ability to issue infringement notices without needing to apply for a court order: *Privacy Act* (n 88) ss 13G–13K.

237 Livingstone et al (n 37) 2. The influence of BigTech on public education is the subject of an 'increased scholarly attention in the growing critical literature on "platform studies in education"': Niels Kerssens, T Philip Nichols and Luci Pangrazio, 'Googlization(s) of Education: Intermediary Work Brokering Platform Dependence in Three National School Systems' (2024) 49(3) *Learning, Media and Technology* 478, 478 (citations omitted) <https://doi.org/10.1080/17439884.2023.2258339>.

the 'pedagogical autonomy' of schools.[238] In Australia, the extent of that influence is likely to grow, as indicated by partnerships such as that previously established between one of the big professional services firms, PwC, and Microsoft, which launched a school management system, 'Connected Schools Solution'[239] (now owned by Scyne Advisory). In promoted content, it was claimed that:

> By building a data-driven information system that shapes insight around the key elements of running a school and delivering education, the Connected Schools Solution paves the way for a range of innovative teaching technologies including artificial intelligence, augmented and virtual reality, and Internet of Things (IoT) driven smart classrooms and schools.[240]

Among other things, the Connected Schools Solution claimed to 'empower schools to predict a student's future success' by 'tracking performance over time and benchmarking it against previous data'.[241] Some of the risks inherent in this were considered in Part II, although these have not been the focus of this article. At best, we should remain sceptical of these claims: as Selwyn has argued, we should adopt 'a more circumspect approach to making sense of the enactment of digital data within school settings'.[242]

VI CONCLUSIONS AND REFLECTIONS

Ultimately, governments have clear obligations under the *CRC* to respect and promote children's rights. As clarified by the Committee in *General Comment No 25*, States must act to ensure that the use of digital educational technologies is 'ethical and appropriate for educational purposes' and does not expose children to 'misuse of their personal data, commercial exploitation or other infringements of their rights'.[243] The sheer volume of information collected from and about children during their use of EdTech products in a school context – and the extent to which their information is collected by or shared with third parties – clearly exposes children to risk of data misuse and commercial exploitation.[244] In fact, as observed

238 See, eg, Niels Kerssens and José van Dijck, 'Governed by Edtech? Valuing Pedagogical Autonomy in a Platform Society' (2022) 92(2) *Harvard Educational Review* 284 <https://doi.org/10.17763/1943-5045-92.2.284>.

239 Connected Schools is now a platform owned by Scyne Advisory, which was created in 2023 when PwC 'sold its public-sector consulting arm to Allegro for $1 when it was cut off from new government work following the tax leaks scandal': Maxim Shanahan, 'PwC Spin-off Scyne Advisory to Slash Staff and Restructure', *Australian Financial Review* (online, 3 April 2025) <https://www.afr.com/companies/professional-services/pwc-spin-off-scyne-advisory-to-slash-staff-and-restructure-20250403-p5lot3>.

240 Staff Writers, 'Data Analytics Is Helping Schools Embrace Their New Normal', *ITnews* (online, 13 July 2022) <https://www.itnews.com.au/feature/data-analytics-is-helping-schools-embrace-their-new-normal-582578>.

241 Ibid.

242 Neil Selwyn, '"Just Playing Around with Excel and Pivot Tables": The Realities of Data-Driven Schooling' (2022) 37(1) *Research Papers in Education* 95, 97 <https://doi.org/10.1080/02671522.2020.1812107>.

243 *General Comment No 25* (n 10) 17 [103].

244 See *How Dare They Peep* (n 4) 92.

in the context of the Year13 example, the very business model of EdTech providers is often predicated on leveraging user data to attract business partners.[245]

While not limited to the EdTech context, *General Comment No 25* also specifically calls for a prohibition on 'profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics'.[246] As Human Rights Watch has remarked, such profiling and targeting 'not only infringes on [children's] privacy, but also risks abusing or violating their other rights, particularly when this information is used to anticipate and guide them toward outcomes that are harmful or not in their best interest'.[247]

Arguably, legislation is the best way to mitigate these risks by requiring responsible, age-appropriate information practices and prohibiting certain activities, such as targeting. Until such legislation is enacted, schools must proactively uphold standards higher than those legally mandated to better protect children within the digital environment. Even with strengthened legislation, schools should continue to play a gatekeeping role regarding student data and EdTech practices, given that it is not assured that those providers will always comply with their legal obligations. It is also likely that, as in the UK, enforcement action against providers will itself be targeted towards the most significant players and focus 'on organisations and individuals suspected of repeated or wilful misconduct or serious failure to comply with the law'.[248] As schools become more connected, and BigTech (and other big commercial players) exerts increasing influence over schools and education, this is even more of an imperative. As noted in a Digital Futures Commission report: 'School is not optional for children, which makes it a worry if giving up personal data [is] normalised as the price of access to education and school'.[249]

Adopting legislation to enshrine age-appropriate information practices may be perceived as protectionist. Yet, as Archbold et al point out, *General Comment No 25* was developed in consultation with hundreds of children and, in many ways, directly responds to their concerns.[250] Nevertheless, schools should rethink the process of seeking parental consent to the use of third-party apps and services, specifically, whether children's consent should always be substituted by parental consent. Secondary schools, in particular, should seek direct consent from older students to collect and use their personal information, rather than defaulting solely to parental consent (which seems to be common practice). In circumstances where parental consent has been provided on a standing basis (for example, at the time of enrolment), schools should reassess the need to gain the consent of individual students when those students demonstrate capacity to make their own privacy decisions (or, given that this may not be practicable when assessed on an individual basis, at least from the age of 15).

---

245 In the case of Year13, for example, business partners include a bank, a fashion clothing retailer, a travel company and a fast food company: see above Part III(A).

246 *General Comment No 25* (n 10) 7 [42].

247 *How Dare They Peep* (n 4) 67.

248 *UK Children's Code* (n 55) 101.

249 Turner, Pothong and Livingstone (n 17) 4.

250 Archbold et al, 'AdTech' (n 42) 876.

Changing consent practices to involve students, when appropriate, demonstrates respect for the evolving capacity of the child – a concept introduced by the *CRC*, which recognises that children 'progressively acquire knowledge, competencies and understanding, including acquiring understanding about their rights and about how they can best be realized'.[251] Although the *CRC* enshrines the concept of evolving capacities within the provisions pertaining principally to parental guidance,[252] as Sheila Varadan writes, it is a 'broad principle' that should inform 'not only the framework of parental guidance, but the whole of the Convention'.[253]

However, as discussed above, gaining meaningful consent is difficult in the context of complex and opaque privacy policies and practices. Accordingly, alongside legal reforms that place the onus of privacy protection on providers, the consent process should be explicitly coupled with the development of digital literacy (broadly, 'the skills, knowledge or practices required to engage with digital technologies')[254] as well as data literacy. As Pangrazio and Julian Sefton-Green explain:

> Networked interactivity and the economic exploitation of digital data calls for more technical understandings, such as how algorithms work. Data literacy thus involves both critical understandings of the technological infrastructure and the political economy of digital platforms, as well as strategies and tactics to manage and protect privacy and resist being profiled and tracked.[255]

Pangrazio and Selwyn advocate for a critical framework for personal data literacy, which 'requires focusing on the ways in which data are constructed and interpreted by various specialists and social actors within data assemblages'.[256] They argue that individuals should be encouraged to 'ask critical questions of data and datafication processes'– such as how data is 'constituted and collected, who it benefits, and how these processes might be reimagined'.[257]

The Australian Curriculum has included a digital literacy component since 2015.[258] According to Australian Curriculum, Assessment and Reporting Authority ('ACARA'), this 'involves students learning to make the most of the digital technologies available to them, adapting to new ways of doing things as technologies

---

251 Committee on the Rights of the Child, *General Comment No 7 (2005)*: *Implementing Child Rights in Early Childhood*, UN Doc CRC/C/GC/7/Rev.1 (20 September 2006) 8 [17].

252 Sheila Varadan, 'The Principle of Evolving Capacities under the UN *Convention on the Rights of the Child*' (2019) 27(2) *International Journal of Children's Rights* 306, 308 <https://doi.org/10.1163/15718182-02702006>.

253 Ibid 306.

254 Tiffani Apps, Shirley Agostinho and Sue Bennett, '"Maybe It's the Environment You Grow Up In?" Australian Primary School Students' Reflections on Their School-Based Digital Literacy' (2022) 31(2) *Technology, Pedagogy and Education* 231, 231 <https://doi.org/10.1080/1475939X.2021.1973550>.

255 Luci Pangrazio and Julian Sefton-Green, 'The Social Utility of "Data Literacy"' (2020) 45(2) *Learning, Media and Technology* 208, 214 <https://doi.org/10.1080/17439884.2020.1707223>.

256 Luci Pangrazio and Neil Selwyn, '"Personal Data Literacies": A Critical Literacies Approach to Enhancing Understandings of Personal Digital Data' (2019) 21(2) *New Media and Society* 419, 427 <https://doi.org/10.1177/1461444818799523>.

257 Luci Pangrazio and Neil Selwyn, *Critical Data Literacies: Rethinking Data and Everyday Life* (MIT Press, 2023) 75 <https://doi.org/10.7551/mitpress/14155.001.0001>.

258 'Digital Literacy in the New Australian Curriculum', *Australian Curriculum* (Web Page, 2025) <https://www.australiancurriculum.edu.au/resources/stories/digital-literacy-in-the-new-australian-curriculum>.

evolve and limiting the risks to themselves and others in a digital environment'.[259] One of the organising elements within this capability is managing and operating information and communication technology ('ICT'), which includes the ability to manage digital data. Additionally, one of the 'sub-strands' of the Australian Curriculum's Digital Technologies area is 'privacy and security'. By Years 9 and 10, students 'consider the privacy and security implications of how data are used and controlled, and suggest how policies and practices can be improved to ensure the sustainability and safety of information systems'.[260]

Digital Literacy as a capability sits alongside Digital Technologies, which became a learning area in 2015. A key concept underpinning this part of the curriculum is understanding the interactions and impacts of digital systems. According to ACARA, this includes 'all aspects of human interaction with and through information systems, and the enormous potential for positive and negative economic, environmental and social impacts enabled by these systems'.[261] It also entails 'consideration of the relationship between information systems and society and in particular the ethical and legal obligations of individuals and organisations regarding ownership and privacy of data and information'.[262]

Taken together, the Australian Curriculum Digital Technologies learning area and the Digital Literacy capability certainly lend themselves to the development of *critical* digital (and data) literacies on the part of students. It is far from clear, however, to what extent the *critical* aspect of digital and data literacy is being developed and, as a whole, digital literacy skills seem to be going backwards.[263] Clearly there is a need to do more to develop both ICT competencies and critical digital and data literacy, not least to counter what has been described as 'a sense of powerlessness' on the part of young people faced with the complexity of 'digital data assemblages, privacy settings and various "terms and conditions" agreements'.[264] Of course, supporting students to develop critical digital literacy requires resourcing, including training for teachers who themselves may require support to develop and enhance their critical digital literacy skills.

At this point it is worth noting the National AI in Schools Taskforce's response to the exponential increase in the scale and scope of general AI tools. The

---

259 'Information and Communication Technology (ICT) Capability (Version 8.4)', *Australian Curriculum* (Web Page) <https://v8.australiancurriculum.edu.au/f-10-curriculum/general-capabilities/information-and-communication-technology-ict-capability/>.

260 The Australian Curriculum allows learning expectations for different year levels (including Years 9 and 10) to be accessed by viewing selected content online: 'Digital Technologies (Version 8.4)', *Australian Curriculum* (Web Page) <https://v8.australiancurriculum.edu.au/f-10-curriculum/technologies/digital-technologies/>.

261 'Structure', *Australian Curriculum* (Web Page) <https://v8.australiancurriculum.edu.au/f-10-curriculum/technologies/digital-technologies/structure/>.

262 Ibid.

263 See 'Evaluating the Evidence for Educational Technology: Part 2', *Australian Institute for Teaching and School Leadership Limited* (Web Page, March 2024) <https://www.aitsl.edu.au/research/spotlights/evaluating-the-evidence-for-educational-technology-part-2-enabling-learning>.

264 Luci Pangrazio and Neil Selwyn, '"My Data, My Bad …": Young People's Personal Data Understandings and (Counter)Practices' (Short Paper No 52, International Conference on Social Media and Society, 28 July 2017) 4 <https://doi.org/10.1145/3097286.3097338>.

Taskforce recently developed the 'Australian Framework for Generative Artificial Intelligence in Schools'.[265] This is a set of six principles and 25 guiding statements and recognises that in order to 'fully harness the potential of high quality and safe generative AI, schools will need to be supported in understanding and appropriately managing a range of privacy, security and ethical considerations'.[266] Although these principles have been developed in response to generative AI tools, they apply equally to all forms of EdTech, especially given that generative AI (or other forms of AI) are increasingly and seamlessly incorporated into various EdTech products.[267]

In addition to stronger legislative safeguards and building the critical digital and data literacy capacity of teachers and students, it is suggested that education authorities (government DoEs in particular) need to become far more transparent in terms of communicating the methodologies that they use to assess EdTech products proposed for use in schools. With some exceptions, DoEs seem reluctant to share and discuss this methodology, requiring academics to submit for department research approval before engaging in dialogue and, even then, often delaying or rejecting applications.[268] Unless this methodology is available, and therefore subject to scrutiny, it is impossible for an objective assessment to be made of the extent to which the assessment process protects the privacy and data rights of students. Conversely, the framework used to assess products under the ST4S initiative is publicly accessible and thorough. This framework and the ST4S initiative as a whole can provide a useful blueprint for other countries to adopt, although it is, as noted, not without its own limitations and would still need to be adapted to reflect a best (or better) practice approach.

Finally, although better protection of children's rights in the digital environment is crucial, and the EdTech environment a significant component of that overall digital environment, we need to keep our eye on the bigger picture: that is, the influence of BigTech (and other large commercial entities)[269] on pedagogical practice and educational policy. This goes beyond the data practices of such players. As Niels Kerssens and José van Dijck have cautioned:

---

265 National AI in Schools Taskforce, 'Australian Framework for Generative Artificial Intelligence in Schools' (Framework, 2023) <https://www.education.gov.au/schooling/resources/australian-framework-generative-artificial-intelligence-ai-schools>.

266 Ibid 5.

267 See 'Education Services Australia Receives Investment to Guide Generative AI Technology in Schools', *Education Services Australia* (Web Page, 7 December 2023) <https://www.esa.edu.au/resources/news-articles/article-detail/education-services-australia-receives-investment-to-guide-generative-ai-technology-in-schools>, referring to the fact that: 'ESA's research underlines a growing trend among educational technology products to incorporate generative AI features.'

268 See, eg, Anna Bunn and Madeleine Dobson, 'Exploring Researchers' Perspectives and Experiences of Digital Childhoods Research in Schools' (2024) 6 *Computers and Education Open* 100186:1–11 <https://doi.org/10.1016/j.caeo.2024.100186>.

269 Refer to PwC's previous involvement with Microsoft in the Connected Schools Solution, discussed above. Large firms, such as EY and KPMG are increasingly engaged (either directly or indirectly) in the 'business' of education: See, eg, 'Education Services', *EY* (Web Page) <https://www.ey.com/en_au/industries/government-public-sector/education-services>; 'Education', *KPMG* (Web Page) <https://kpmg.com/au/en/home/industries/education.html>.

> The platformization of education – the integration of digital platforms into daily school practices – is a major cause of concern worldwide for the pedagogical autonomy of schools and teachers. First, technology giants like Google (Alphabet), Apple, Facebook (Meta), Amazon, and Microsoft (GAFAM) – Big Tech – are rapidly expanding their services into the edtech market and increasingly seizing control over the shaping and organization of online learning environments in schools around the globe. Second, through increased interweaving of a diverse set of educational platform technologies – digital learning platforms, learning tracking systems, learning apps, learning analytics – in everyday classroom teaching and learning, control over pedagogical decision-making shifts from teachers to platform algorithms and dashboard interfaces.[270]

These concerns should certainly exercise the 'minds' of governments, schools, parents and students. This article, however, has focused on the way in which the flow of information between schools and/or their students, third-party digital products and others (such as companies in the AdTech sector) is regulated (or not) through the policies and practices of education authorities, as well as by existing and proposed information privacy laws. It has argued that ultimately governments need to legislate to improve the practices of the companies behind EdTech products and services to better protect children's rights, and that there is, in Australia, currently reason for cautious optimism on this front following recommendations of the *Privacy Review Report* and development of a Children's Online Privacy Code. However, it has also argued that schools (and their overarching authorities) have a crucial and continuing role to play to afford children the full range of their rights and to protect them within the digital environment: this should include modelling best (or better) practice; building the critical digital and data literacy of students and teachers; and supporting the agency of their students to make decisions, as appropriate to their age and maturity.

270 Kerssens and van Dijck (n 238) 284–5 (citations omitted).