ADTECH AND CHILDREN'S DATA RIGHTS

LISA ARCHBOLD,* DAMIAN CLIFFORD,** MOIRA PATERSON,*** MEGAN RICHARDSON,**** NORMANN WITZLEB*****

The advertising technology industry, known as 'adtech', is a complicated network of organisations and individuals that collect, aggregate and deal with large amounts of personal data. As children engage with digital networks for many aspects of their lives, they are increasingly exposed to adtech practices. Depending on their age, children may have less knowledge of the commercial digital environment and less maturity in their decision-making processes than adults have. Their limited resilience in the face of adtech's onslaught offers a particularly stark illustration of why it is problematic to look to 'consent' as the exclusive or predominant mechanism to control the use of consumer data in the digital ecosystem. This article examines the problems arising from adtech's data practices and makes recommendations on how to strengthen the agency and control exercised by children and protect their best interests in the context of adtech.

I INTRODUCTION

The advertising technology industry, known as 'adtech', has been described as

> a complex ecosystem of many different types of organisations including advertising agencies and networks, data brokers, data analytics companies, publishers and buyers. Those organisations are engaged in high-speed and high-volume digital transactions, selling, sharing, transmitting and aggregating personal data harvested through the use of tracking technologies such as cookies with the aim of serving highly tailored ads to individuals based on what is known or what can be inferred about them.[1]

* PhD candidate, Centre for Media and Communications Law, Melbourne Law School, The University of Melbourne.

** Senior Lecturer, Australian National University, College of Law; Associate Researcher, Information Law and Policy Centre, Institute of Advanced Legal Studies, University of London.

*** Adjunct Professor, Faculty of Law, Monash University.

**** Professor and Co-Director, Centre for Media and Communications Law, Melbourne Law School, The University of Melbourne; Chief Investigator, ARC Centre of Excellence for Automated Decision-Making and Society.

***** Associate Professor, Faculty of Law, The Chinese University of Hong Kong; Adjunct Associate Professor, Faculty of Law, Monash University. The authors would like to thank the anonymous reviewers for helpful advice and comments.

Children as a group seem especially susceptible to these technologies and practices – because of their young age, their knowledge of the commercial digital environment and the maturity of their decision-making processes will often still be developing.[2] Their limited resilience to adtech's sophisticated persuasion techniques offers a particularly heightened example of the problem of relying on 'consent' as an exclusive or predominant control mechanism for their engagements with the digital ecosystem.[3]

Even apart from adtech, the value of consent in consumer data protection (or 'data privacy') regimes has been doubted because consumers often have no real choice but to give up their personal data in exchange for products and services. Critics of the 'notice-and-consent' approach point to the position of dominance held by online companies and its effects on the capacity for individual self-determination.[4] This power asymmetry devalues the validity of user consent and presents a clear barrier to holding companies to account.[5] In the case of children, 'consent' is an even more problematic control mechanism for the use of personal data in the digital ecosystem,[6] and indeed for their engagements with markets generally. Often, the response to these problems has been to empower the user – or, in the case of children who may lack capacity to make valid decisions, to move the decision-making from children to parents. Thus, as Steinberg concludes, the '[c]urrent [United States] laws protecting children's privacy reflect the strong tradition of parental rights to control and shape the lives of their children'.[7] In a similar vein, the Australian Competition and Consumer Commission ('ACCC') in its Digital Platforms Inquiry report[8] includes recommendations to enhance transparency requirements and, in the case of children, to rely on parental/guardian consent for the collection of children's personal information.[9]

---

1 Data Protection Commission (Ireland), 'Fundamentals for a Child-Oriented Approach to Data Processing' (Draft Version for Public Consultation, December 2020) 54 [6.2.2] <https://www.dataprotection.ie/en/news-media/consultations/children-front-and-centre-fundamentals-child-oriented-approach-data-processing> ('Fundamentals').

2 Ibid 12 [1.1], 52 [6.2].

3 Ibid 39 [5.1], 54 [6.2.2].

4 Alessandro Mantelero, 'Competitive Value of Data Protection: The Impact of Data Protection Regulation on Online Behaviour' (2013) 3(4) *International Data Privacy Law* 229, 229.

5 Orla Lynskey, 'Deconstructing Data Protection: The "Added Value" of a Right to Data Protection in the EU Legal Order' (2014) 63(3) *International and Comparative Law Quarterly* 569, 594–5.

6 See 'Fundamentals' (n 1) 54 [6.2.2].

7 Stacey B Steinberg, 'Sharenting: Children's Privacy in the Age of Social Media' (2016) 66(4) *Emory Law Journal* 839, 861, 871.

8 Australian Competition and Consumer Commission ('ACCC'), 'Digital Platforms Inquiry' (Final Report, June 2019) <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report> ('Digital Platforms Report').

9 Ibid 34–7 [16]–[18]. Recommendation 16(c) called for strengthening of consent requirements and included the default setting for collection to be 'off', ie, requiring affirmative action from the consumer to consent. In relation to children, the ACCC recommended that '[w]here the personal information of children is collected, consents to collect the personal information of children must be obtained from the child's guardian': at 35.

In this article, we argue that a regulatory framework governing adtech that relies heavily on parental consent – or indeed any consent – cannot fully address some fundamental weaknesses of the notice-and-consent model. Our specific recommendations focus on Australian reforms, however, we are of the view that the best practice principles – to have the best interests of children as the primary consideration, prohibiting profiling of children in adtech (unless the relevant organisation can clearly demonstrate how and why it is in the best interests of children to do so) and to focus more on fairness instead of consent – are relevant around the globe.[10] At the root of the debates regarding the legitimacy of adtech are questions regarding the suitability of individual consent as a basis for legitimising the gathering of vast amounts of personal data. While parents have an important role in the protection of children's data protection and privacy, they often face dilemmas even when making decisions about their own personal information. Moreover, transferring control to parents, especially where a child has the requisite capacity for consent, is at odds with the value of personal autonomy that underpins data protection and privacy.

More fundamentally, we question the appropriateness of 'data privacy' standards focused exclusively on consent to deal with the challenges raised by adtech for children. We therefore agree with the Irish Data Protection Commissioner's recent statement that

> organisations should not profile children, engage in automated decision-making concerning children, or otherwise use their personal data, for advertising/marketing purposes, unless they can clearly demonstrate how and why it is in the best interests of children to do so.[11]

This call for stricter controls accords with the United Nations ('UN') *Convention on the Rights of the Child*'s ('*CRC*') article 3 mandate that the 'best interests' of the child should be a primary consideration in all actions concerning children[12] – amplified in the UN Committee on the Rights of the Child's recently issued *General Comment No 25*, stating that

> States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling.[13]

---

10 See also Joseph A Cannataci, Special Rapporteur on the Right to Privacy, *Artificial Intelligence and Privacy, and Children's Privacy*, UN Doc A/HRC/46/37 (25 January 2021) 22, recommendation (v).

11 'Fundamentals' (n 1) 54 [6.2.3]. See also Information Commissioner's Office (United Kingdom), 'Age Appropriate Design: A Code of Practice for Online Services' (Code of Practice, 2 September 2020) <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf> 24 and passim. Cf 'Digital Platforms Report' (n 8) 36, recommendation 18 calling for an enforceable code of practice to be developed by the Office of the Australian Information Commissioner, targeting specific data practices.

12 *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990) art 3 ('*CRC*'). See also article 2 (right to equality), article 6 (right to live a full life/right to development), article 32 (right of the child to be protected from economic exploitation).

13 United Nations 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) 7 [42] ('*General Comment No 25*'). See also Cannataci, Special Rapporteur on the Right to Privacy, UN Doc A/HRC/46/37 (n 10) 22, recommendation (v) for a prohibition that is not limited to commercial purposes.

Further, even where consent (along with 'best interests') provides a suitable basis for processing the personal data of children, there is a need to strengthen its operation and, in particular, give children a stronger voice. When children become older, it becomes problematic that the use of their personal data should be determined by their parents' choices. At the very least, standards should be framed to provide opportunities for children to express their views, and to have those views taken into account in the granting of any parental consent, taking into account their age and capacities, in accordance with articles 5 and 12 of the *CRC*.[14] Such an approach would reflect *General Comment No 25*'s position that States parties 'should have regard for all children's rights, including their rights to seek, receive and impart information, to be protected from harm and to have their views given due weight'.[15] Given the *CRC*'s precept that opportunities for participation in decisions, especially those concerning them, are 'vital for children's well-being in the present and for their development towards adulthood', these basic standards should also apply to decisions about the processing of their personal data.[16] Indeed, logically this suggests that children's views should be obtained not just in relation to specific consent decisions arising from adtech, but also in relation to broader data protection issues, including whether there should be specific, actual or prima facie prohibitions on certain adtech practices in the best interests of the child. And we applaud the *CRC*'s drafting team's consultative processes extending to children, and the 700+ children from 27 countries who participated in those processes with consultation responses.[17] In this sense, while we take a protectionist approach by recommending that profiling children in adtech should be prima facie prohibited, this responds to the insights of children obtained as part of this consultation process, thus giving further effect to their participation in policy-making.

14 *CRC* (n 12) art 5 (parental guidance and child's evolving capacities), art 12 (right to an opinion and to be listened to). See also article 13 (freedom of expression including 'freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice'), article 14 (freedom of thought, conscience and religion).

15 *General Comment No 25*, UN Doc CRC/C/GC/25 (n 13) 3 [13].

16 See Office of Research – Innocenti, United Nations Children's Fund, 'Worlds of Influence: Understanding What Shapes Child Well-Being in Rich Countries' (Innocenti Report Card No 16, 2020) 27 ('Innocenti Report Card 16') <https://www.unicef-irc.org/publications/pdf/Report-Card-16-Worlds-of-Influence-child-wellbeing.pdf>.

17 See Sonia Livingstone and Anri van der Spuy, 'Beyond Multistakeholder Tokenism: Promoting Children's Rights in a Digital Age', *London School of Economics and Political Science* (Blog Post, 23 February 2021) <https://blogs.lse.ac.uk/medialse/2021/02/23/beyond-multistakeholder-tokenism-promoting-childrens-rights-in-a-digital-age/>.

II THE EVOLVING ADTECH LANDSCAPE

Personalised advertising works from the premise that accurate targeting increases the likelihood that a user will click on the advertisements and, ultimately, convert into a purchaser. Advertising technologies commonly rely on the use of 'cookies'[18] to track individual users across various domains (ie, all the websites that form part of their network) with the profiles becoming more detailed with each visit. Hence, as noted by Edwards, '[c]ookies in the commercial world are essentially legitimised "spyware", in that they allow businesses to spy on consumers online'.[19]

In digital advertising, the use of cookies can be complicated due to the vast array of different service providers that may be dropping or accessing cookies at any one moment.[20] At its most basic, the adtech ecosystem involves at a minimum three players, an advertising network, an advertiser and a publisher (ie, the website owner). Advertising networks act as intermediaries between publishers and advertisers and provide a bidding service allowing for the delivery of the relevant advertisements into the vacant spaces but may also engage with demand side platforms (used by advertisers to help organise ad-buying) and supply side platforms (used by publishers to automate sales of advertising space), amongst others. In the world of AdExchanges,[21] this is complicated further given the array of players.[22] Figure 1 outlines in a simplified manner some of the entities involved in the filling of available advertising slots when a user visits a webpage.

---

18 Cookies are single alphanumerical codes that are placed on users' web browsers in order to track users' online activity and help select the advertisements they see: Paul Schwartz and Daniel Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86(6) *New York University Law Review* 1814, 1854.

19 Lilian Edwards, 'Consumer Privacy Law 1: Online Direct Marketing' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet* (Hart Publishing, 3rd ed, 2009) 489, 489.

20 'Fundamentals' (n 1) 54 [6.2.2]. See also Forbrukerrådet [Consumer Council] (Norway), 'Out of Control: How Consumers Are Exploited by the Online Advertising Industry' (Report, 14 January 2020) <https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>, which noted at 120 [6.4]:

> The adtech industry is packed with companies that are virtually unknown entities amongst consumers. However, by far the largest actors in the adtech industry are household names, namely Google and Facebook. Although the dominant position of Google and Facebook is outside the scope of this report, it is pertinent to outline the extent of tracking that these companies engage in throughout the mobile app environment.

21 Digital marketplaces such as Google's AdX act as a form of stock exchange, allowing for the trading of advertisements and slots across advertising networks.

22 Given that AdExchanges act as platforms for facilitating the shared bidding/selling of ad space between ad networks, it is possible for advertisements appearing on publishers' websites to make multiple calls outside the minimum three parties (ie, advertiser, publisher, and the ad network).

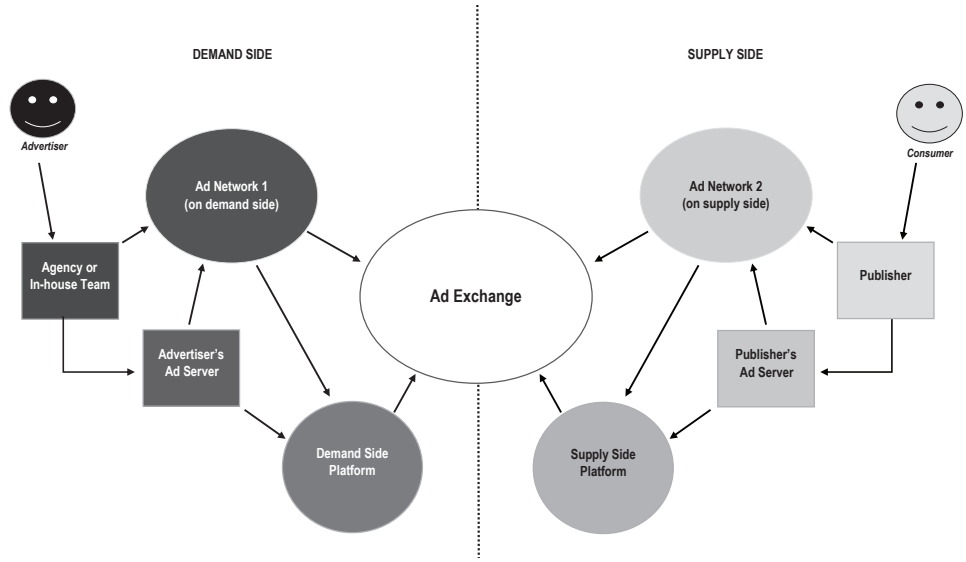

Figure 1: Diagram of main entities involved in the filling of available advertising slots when a user visits a webpage.

The selection of the optimal advertisement has been aided greatly by the emergence of real-time bidding technology also known as 'programmatic buying'.[23] This technology allows advertisers to bid for advertising spaces in real time, through coded preferences, while the selected webpage is loading. These systems analyse the content of a webpage, the user's interests based on past browsing behaviour (through reading the cookies), other relevant information (such as a user's location, gender and age range) often deduced from the analysis of other individuals who exhibit similar behavioural patterns in their browsing, and the available advertisements.[24] Data mining software or predictive analytics are then used to correlate the retrieved data and match particular advertisements to users, enabling advertisers to make automated live decisions in every auction in real time.[25] Without the services provided by the advertising networks, publishers and advertisers would have to resort to directly negotiated sales of ads.

23 There is a useful summary of the issues raised by real-time bidding in Information Commissioner's Office, 'Update Report into Adtech and Real Time Bidding' (Report, 20 June 2019) <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>.

24 Maria Halkidi and Iordanis Koutsopoulos, 'A Game Theoretic Framework for Data Privacy Preservation in Recommender Systems' in Dimitrios Gunopulos et al (eds), *Machine Learning and Knowledge Discovery in Databases* (Springer, 2011) 629.

25 Shuai Yuan, Jun Wang and Xiaoxue Zhao, 'Real-Time Bidding for Online Advertising: Measurement and Analysis' (Conference Paper, International Workshop on Data Mining for Online Advertising, August 2013) <https://doi.org/10.1145/2501040.2501980>.

Concerns regarding the extensive data gathering that facilitates the personalisation of advertising are far from new.[26] However, there is renewed interest in these issues because the adtech industry is about to experience a monumental shift. Google has recently announced that it will phase out its reliance on third-party cookies in Chrome by early 2022 and will not replace them with some other form of unique identifier.[27] More specifically, Google intends to roll out privacy preserving Application Programming Interfaces that will rely on interest-based advertising and eliminate the reliance on third-party cookies. These proposed changes will reduce the number of players gaining access to detailed information relating to individuals, which would align with data security and data minimisation objectives. While these announcements may sound a death knell to the industry as we know it, two important points are to be made here. First, Google's announcement follows those of Apple and Firefox, which means the decision merely tracks a long line of legislative, policy and industry developments and, second, the announcement only refers to cookies originating from other websites (third-party cookies), and not those placed on a user's machine by the website operator. Furthermore, elimination of reliance on third-party cookies is beneficial only in terms of data minimisation and data security – it does not affect the broader invasiveness of profiling and targeted advertising.

Although adtech is currently in a state of flux, the processing of detailed consumer information and targeted advertisements will therefore remain key parts of the ecosystem, and the underlying issues and concerns related to processing of children's data for adtech purposes will also remain. Children as a group seem especially susceptible to these technologies and practices. First, they may not realise that platforms are 'free' to use only because these platforms permit or actively promote the collection and use of their personal data to target them with personalised advertising.[28] Second, even if they do understand that their data are collected and used on some platforms, they are less attuned to appreciate and resist more subtle practices such as cross-device identification, tracking of metadata,

---

26 Indeed, in the EU, the 2009 *Cookie Directive* updated the *ePrivacy Directive* (*Parliament and Council Directive 2002/58/EC of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications* [2002] OJ L 201/37) and mandated user consent for the use of non-functional cookies: *Parliament and Council Directive 2009/136/EC of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws* [2009] OJ L 337/11, art 2(5). Another important example is the demise of the Do-Not-Track ('DNT') policy and technology. The DNT proposal aimed to enable 'users to opt out of tracking by (all) websites they do not visit, including analytics services, advertising networks, and social platforms': European Network and Internet Security Agency, 'Privacy Considerations of Online Behavioural Tracking' (Report, 19 October 2012) 17 <https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking>.

27 See David Temkin, 'Charting a Course towards a More Privacy-First Web', *Google Ads & Commerce Blog* (Blog Post, 3 March 2021) <https://blog.google/products/ads-commerce/a-more-privacy-first-web/>.

28 Karen McCullagh, 'The General Data Protection Regulation: A Partial Success for Children on Social Network Sites?' in Samuli Miettinen and Tobias Bräutigam (eds), *Data Protection, Privacy and European Regulation in the Digital Age* (Unigrafia, 2016) 117.

and profiling. As Stoilova, Livingstone and Nandagiri put it after conducting focus group research with 150 secondary-school-age children in England, Scotland and Wales:

> How their data moves online, who uses it and to what ends, and why their data is valuable are some of the most reoccurring questions that children have. They are often unaware that the same company might be behind different platforms they use (eg, WhatsApp, Instagram and Facebook) … [and they] are also often puzzled by the amount of information they are asked to provide when they register to use product and services, particularly if it seems unrelated to the purpose.[29]

Given that empirical research has found that children 'find the commercial domain perplexing and manage to grasp only some aspects of how it operates',[30] the impact of the commercial adtech industry on children in this changing environment continues to raise significant concerns.

III LAW REFORM

In this part of the article, we consider more closely the challenges posed by adtech in relation to children, proposing a two-pronged model focused on (a) consent, control and agency and (b) the best interests of the child, as independently assessed by the regulator. In particular, we ask what can be done to make consent more meaningful, who should provide consent, and how can potential tensions between children's and parents' concerns be moderated. In designing appropriate law reform, we contend that it is important to show respect for children's agency, in compliance with the *CRC* – and, in particular, the emphasis of article 5 on the evolving capacities of children and the mandate of article 12 that the views of the child in relation to matters affecting them must be given due weight in accordance with their age and maturity.[31] Thus, the discussion in relation to consent and control goes well beyond a narrow adherence to the right not to 'be subjected to arbitrary or unlawful interference with his or her privacy' provided for in article 16 of the *CRC*.[32] Moreover, our recommendations do not stop there. Noting that, under article 3 of the *CRC*, the 'best interests' of the child shall be a primary consideration in all actions concerning them,[33] we make specific recommendations for protecting these interests. While this obligation fundamentally relates to State action, the UN Committee on the Rights of the Child has argued that States also have the obligation to ensure that businesses and the private sector likewise respect children's rights.[34]

---

29 Mariya Stoilova, Sonia Livingstone and Rishita Nandagiri, 'Children's Data and Privacy Online: Growing up in a Digital Age' (Research Findings, Department of Media and Communications, London School of Economics and Political Science, 2019) 22 <http://eprints.lse.ac.uk/101282/> ('Children's Data and Privacy Online').

30 Mariya Stoilova, Sonia Livingstone and Rishita Nandagiri, 'Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy' (2020) 8(4) *Media and Communication* 197, 205 ('Digital by Default').

31 See *CRC* (n 12) arts 5, 12.

32 Ibid art 16.

33 Ibid art 3.

34 *General Comment No 25*, UN Doc CRC/C/GC/25 (n 13) 6 [35].

A Consent, Control and Agency

The Australian legislative standards for processing of personal data in the *Privacy Act 1988* (Cth) ('*Privacy Act*')[35] suffer from a number of shortcomings which limit their ability to operate efficiently.[36] This includes, especially concerningly in this context, that 'consent' is defined in the Act simply to mean 'express consent or implied consent'.[37] The Act does not elaborate how consent is to be manifested and, with the inclusion of implied consent, sets a threshold that has been criticised as too low.[38] In examining the application of the Act to digital platforms, the ACCC noted that several practices 'degrade the quality of consent provided by consumers such as the use of clickwrap agreements, take-it-or-leave-it terms, and bundling of consents'.[39]

An important theme emerging from the ACCC's Digital Platforms Report is the need to enhance individuals' control over the processing of their personal information, including in complex situations, by bolstering individual consent.[40] The Digital Platforms Report's recommendations include an updating of the Act's definition of 'personal information' to 'clarify that it captures technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual'.[41] In addition, it recommends:

> [s]trengthening consent requirements to require that consents are freely given, specific, unambiguous and informed and that any settings for additional data collection must be preselected to 'off'. Consents should be required whenever personal information is collected, used or disclosed by an entity subject to the *Privacy Act*, unless the personal information is necessary to perform a contract to which a consumer is a party, required under law, or otherwise necessary in the public interest.[42]

These recommended changes draw heavily on the European Union ('EU') *General Data Protection Regulation* ('*GDPR*').[43] The *GDPR* is widely accepted

---

35 *Privacy Act 1988* (Cth).

36 These include the narrow definition of 'personal information' in *Privacy Act 1988* (Cth) section 6 (as highlighted in *Privacy Commissioner v Telstra Corporation Ltd* (2017) 249 FCR 24 (Dowsett, Kenny and Edelman JJ)) and the small business operator exemption which has the consequence most businesses with $3 million or less annual turnover do not need to comply with the Act. It should be noted, however, that the latter does not apply to an operator who 'discloses personal information about another individual to anyone else for a benefit, service or advantage': see ibid s 6D (4)(c).

37 Ibid s 6 (definition of 'consent').

38 See generally Moira Paterson and Maeve McDonagh, 'Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data' (2018) 44(1) *Monash University Law Review* 1; Graham Greenleaf et al, 'Regulation of Digital Platforms as Part of Economy-Wide Reforms to Australia's Failed Privacy Laws: Australian Privacy Foundation Submission to the Australian Government on Implementation of the ACCC's Digital Platforms Inquiry – Final Report' [2019] *University of New South Wales Law Research Series* 83 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3443337>.

39 'Digital Platforms Report' (n 8) 466.

40 Ibid 439.

41 Ibid 458, recommendation 16(a).

42 Ibid 24. See also ibid 464, recommendation 16(c).

43 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 ('*GDPR*').

as a global benchmark in data protection, both because of its stringent standards and, more practically, because those standards may be drawn on to assess the 'adequacy' of other States' regulation of business practices that involve collection or processing of personal data from data subjects in the EU.[44] Importantly, 'consent' is defined tightly in *GDPR* article 4 as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.[45]

Regarding children, recommendation 18 of the Digital Platforms Report calls for an enforceable code of practice to be developed by the Office of the Australian Information Commissioner ('OAIC'), in consultation with industry stakeholders, to enable proactive and targeted regulation of data practices,[46] including

> requirements to provide consumers with specific, opt-in controls for any data collection that is for a purpose other than the purpose of supplying the core consumer-facing service and, where consents relate to the collection of children's personal information, additional requirements to verify that consent is given or authorised by the child's guardian.[47]

Here again the *GDPR* serves as an inspiration – although the *GDPR* is more definitive in setting the standards for consent in relation to children's data by placing the obligations in the regulation itself, rather than leaving them to be developed by a code of practice. It mentions children in several of its provisions[48] and recitals. For instance, recital 38 states that '[c]hildren 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'.[49] As to consent, *GDPR* article 8(1) provides that:

> [I]n relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder

---

44 See *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Court of Justice of the European Union, C-311/18, ECLI:EU:C:2020:559, 16 July 2020) 58 [188]–[189] (The Court) ('*Schrems II*').

45 *GDPR* (n 43) art 4(11). Consent is one of the six potential bases for lawful processing in article 6(1) of the *GDPR*. These six justifications are consent, contract, legal obligation, vital interests of the data subject, public interest and legitimate interest.

46 'Digital Platforms Report' (n 8) 481, recommendation 18. The ACCC envisages that the 'code should apply to all digital platforms supplying online search, social media, and content aggregation services to Australian consumers and which meet an objective threshold regarding the collection of Australian consumers' personal information'.

47 Ibid.

48 *GDPR* (n 43). In addition to being the focus of article 8(1) as discussed below, children are mentioned in article 6(1), which regulates the lawfulness of processing, article 12, which regulates transparency, including in privacy notices, article 57 concerning public awareness activities of supervisory authorities and article 40 concerning codes of conduct.

49 Ibid recital 38. See also recital 65 concerning the significance of the right to erasure for children. For a discussion of the protections for children in the *GDPR*, see Eva Lievens and Valerie Verdoodt, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation' (2018) 34(2) *Computer Law and Security Review* 269.

> of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

In addition, *GDPR* article 8(2) states that '[t]he controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology' – a prescription the ACCC also endorses.[50]

In specifying a requirement for consent by the holder of parental responsibility, the *GDPR* appears to have been inspired by the United States ('US') *Children's Online Privacy Protection Act* ('*COPPA*').[51] Despite the US influence on the *GDPR* in this respect, it is important to keep in mind the fundamental differences between both jurisdictions with regard to 'data privacy' regulation. The EU recognises both privacy and data protection as fundamental rights in articles 7 and 8 of the *Charter of Fundamental Rights of the European Union* ('*EU Charter*'), respectively.[52] Thus EU laws (such as the *GDPR*) must be consistent with those rights, including the requirement in article 8 of the *EU Charter* that '[personal] data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[53]

By contrast, the US does not treat data protection as a human rights issue but rather adopts as its starting point that entities may freely collect and use personal data subject to specific prohibitions or restrictions.[54] The US model places stronger reliance on the consumer protection and contractual model and prefers to confine data protection legislation to particular groups or contexts, rather than having broad protections of general application. The *COPPA* states that its focus is the 'regulation of unfair and deceptive acts and practices in connection with collection and use of personal information from and about children on the Internet'.[55] Although the US is a signatory to the *CRC*, it is yet to ratify it. The *COPPA* was introduced in 1998 and came into effect in 2000, ie, after the *CRC* but with scant reference to its rights. In essence, the *COPPA* requires that an operator of a website directed at children or that knowingly collects information about children provide notice about its practices and obtain verifiable parental consent.[56] Hence the emphasis is on finding a modality of consent where the data subject is a child, here reflecting a strong US tradition of 'parental rights to control and shape the lives of their children'.[57] In contrast, article 24 of the *EU Charter*, in a nod to the *CRC*, states more broadly that '[c]hildren shall have the right to such protection and care as is

---

50 'Digital Platforms Report' (n 8) 468.

51 *Children's Online Privacy Protection Act of 1998*, 15 USC §§ 6501–6 ('*COPPA*'). See also Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26(2) *Information and Communications Technology Law* 146.

52 *Charter of Fundamental Rights of the European Union* [2012] OJ C 326/391.

53 Ibid art 8(2).

54 Anupam Chander, Margot E Kaminski and William McGeveran, 'Catalyzing Privacy Law' (2021) 105(4) *Minnesota Law Review* 1733, 1747–8.

55 *COPPA* (n 51) § 6502.

56 Ibid § 6502(b).

57 Steinberg (n 7) 861, 871. See also David D Meyer, 'The Modest Promise of Children's Relationship Rights' (2003) 11(3) *William & Mary Bill of Rights Journal* 1117.

necessary for their well-being. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity'.[58] Macenaite and Kosta note that '[t]he commitment of the EU institutions [in recent years] to promoting, protecting and fulfilling children's rights in all relevant policy areas and actions means that the principles of the UN *CRC* should guide the EU policies directly or indirectly affecting children'.[59]

Both the *COPPA* and the *GDPR* enact cut-off ages for consent: the *COPPA* is currently restricted in its application to children under the age of 13,[60] whereas the *GDPR* allows Member States some discretion. The *GDPR* gives children under the age of 16, or such lower age as Member States prescribe, child-specific protection regarding consent – provided this prescribed age is 'not lower than 13 years'.[61] While some States have adopted this minimum age, a larger number have opted for 14, 15 or 16 years of age.[62] As was pointed out by some children's rights activists when the age of digital consent was considered for the *GDPR*, the *COPPA* offers greater scope for children aged 13 and over to make their own choices[63] – but, in doing so, withholds some of the protections available in the EU.

The ACCC's proposals to strengthen consent requirements reflect the desire to empower individuals to have 'some control and awareness over the extent of acceptable data collection'.[64] Nevertheless, in relation to children, the ACCC recommends, that '[w]here the personal information of children is collected, consents to collect the personal information of children must be obtained from the child's guardian'.[65] Taken literally, this recommendation would require obtaining the guardian's consent whenever the personal information of children is collected. This, we argue, may in fact be a retrograde step for children's evolving agency and participation because the current *Privacy Act* guidelines of the OAIC ('Guidelines') actually call for case-by-case assessments of children's capacity.[66] That said, where

58 *Charter of Fundamental Rights of the European Union* (n 52) art 24(1).

59 Macenaite and Kosta (n 51) 150.

60 *COPPA* (n 51) § 6501(1).

61 *GDPR* (n 43) art 8(1).

62 See Ingrida Milkaite and Eva Lievens, 'The GDPR Child's Age of Consent for Data Processing across the EU: One Year Later' (Research Project, Ghent University, 2 July 2019) <https://biblio.ugent.be/publication/8621651/file/8621654.pdf>.

63 See Lievens and Verdoodt (n 49) 271–2.

64 'Digital Platforms Report' (n 8) 470.

65 Ibid 464.

66 See Office of the Australian Information Commissioner, 'Australian Privacy Principles Guidelines: Privacy Act 1988' (Guidelines, July 2019) 13:

> The *Privacy Act* does not specify an age after which an individual can make their own privacy decisions. An APP entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent. … As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves … 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.

it is 'not practicable or reasonable' to individually assess the capacity (which would likely cover the situation of many adtech players), entities can rely under the Guidelines on a presumption that someone aged 15 has capacity to consent, which creates de facto an age of consent.[67] While recognising the special vulnerabilities of children arising from their physical and mental development is important, viewing children entirely as vulnerable can lead to unintended consequences of eroding children's rights.[68] The idea that parental consent is an appropriate substitute for a child's consent until they turn 18 is indeed difficult to reconcile with the premise that data protection and privacy laws safeguard personal autonomy.[69]

A more graduated approach could assist here. For instance, we accept that for younger children, parental consent may be the only available consent option – however, older children (especially older teenagers) should be granted greater say in decisions concerning them. This may involve the right to be consulted by parents when they are making decisions on children's behalf or even the child's right to consent on their own. For these young people, deficiencies in the consent approach can be addressed through appropriately developed standards around unfair terms and unfair or deceptive practices in consumer law,[70] and requirements for collecting information only by lawful and fair means in the *Privacy Act*,[71] appropriately construed to take account of a data subject's age, experience and vulnerabilities. More broadly, we suggest that there is a need to move beyond a narrow focus on consent to consider the concept of control more holistically. It is clear from overseas research and consultations that children themselves desire and actively seek information and empowerment, 'try[ing] to make sense of how the internet ecology works and create their theories, myths and workarounds'.[72] This resonates with the *CRC*'s mandate that a child who is capable of forming views should have the right to express those views freely in all matters affecting the

67 Ibid.

68 John Tobin, 'Understanding Children's Rights: A Vision beyond Vulnerability' (2015) 84(2) *Nordic Journal of International Law* 155, 156–7, 166.

69 Jelena Gligorijević, 'Children's Privacy: The Role of Parental Control and Consent' (2019) 19(2) *Human Rights Law Review* 201, 202. See also Cannataci, Special Rapporteur on the Right to Privacy, UN Doc A/HRC/46/37 (n 10) 10 [71], 12 [80]–[83].

70 *Competition and Consumer Act 2010* (Cth) sch 2 pts 2–3. See especially section 18 (misleading or deceptive conduct). Cf *Federal Trade Commission Act*, 15 USC § 45(a)(1) (2006) (unfair or deceptive acts or practices).

71 *Privacy Act 1988* (Cth) sch 1 Australian Privacy Principle 3.5. Cf *GDPR* (n 43) art 5 (principles relating to processing of personal data).

72 Stoilova, Livingstone and Nandagiri, 'Children's Data and Privacy Online' (n 29) 22.

child, with their views given due weight in accordance with the age and maturity of the child,[73] a position reaffirmed in *General Comment No 25*.[74]

In fact, the concept of control is a familiar one in EU data protection law, which attaches significance to the individual's ability to determine the fate of their personal data and also provides a robust architecture of control designed to ensure individual autonomy.[75] 'Control' manifests a broader meaning than the mere giving of a formal consent, as it also represents the environmental elements through which control is made effective. This raises the question of how to design a system which embeds effective controls. In relation to children's control over parents' consent, we suggest that, at the very least, design standards should include not only a requirement of 'reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology'[76] but also of reasonable efforts to verify that the views of the child have been given due weight (in the process of obtaining consent) in accordance with the age and maturity of the child, as required by the *CRC*. As noted in *General Comment No 25*, the digital environment provides crucial opportunities for children to participate in society and to 'be effective advocates for their rights, individually and as a group'.[77] We argue that the views of the child should be sought in multiple contexts. This includes the policy level where 'data privacy' regulation affecting children is formulated, but should also extend to requiring organisations to conduct children's rights impact assessments and seek input from children in relation to how they view specific adtech practices.

B Protecting the Best Interests of Children

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. Protecting the best interests of the child, as

---

73 See *CRC* (n 12) arts 5, 12. See also Innocenti Report Card 16 (n 16) 27:

> It is important that children have the opportunity to express their views and are involved in decision-making. This is enshrined in article 12 of the United Nations Convention on the Rights of the Child. Such opportunities are vital for children's well-being in the present and for their development towards adulthood. As children grow up, parents and other adults need to adjust the balance between protecting children and enabling them to have appropriate levels of autonomy'.

See also John Tobin and Sheila Varadan, 'Article 5: The Right to Parental Direction and Guidance Consistent with a Child's Evolving Capacities' in John Tobin (ed), *The UN Convention on the Rights of the Child: A Commentary* (Oxford University Press, 2019) 159, 161: The article 5 right is 'best characterized as *the right of a child* to receive appropriate direction and guidance from his or her parents to secure the enjoyment of his or her rights rather than a right of parents to have their rights regarding their parenting respected by the state' (emphasis in original).

74 *General Comment No 25*, UN Doc CRC/C/GC/25 (n 13) 3 [13]. See also Cannataci, Special Rapporteur on the Right to Privacy, UN Doc A/HRC/46/37 (n 10) 18 [116].

75 Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015). For interdisciplinary perspectives on the control component of data protection, see notably: Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff, 2013); Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press, 2014); Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12(1) *SCRIPTed* 3.

76 Similar to the requirements under *GDPR* (n 43) art 8(2).

77 *General Comment No 25*, UN Doc CRC/C/GC/25 (n 13) 3 [16].

provided for in article 3 of the *CRC*, is an independent consideration. Specifically, article 3 states that the 'best interests' of the child shall be a 'primary consideration' in all actions concerning children, 'whether undertaken by public or private social welfare institutions, courts of law, administrative … or legislative bodies'.[78] As indicated by *General Comment No 25*,[79] this should be taken inter alia to entail an obligation to ensure that, regarding the regulation of advertising and marketing (including the framing, elucidating and enforcement of data protection standards), the best interests of the child are to be treated as a primary consideration.

Protecting the best interests of the child, as provided for by article 3, is supplemented by one of the other guiding principles in article 6 of the *CRC* of safeguarding the child's right to development.[80] As explained by Peleg, the right to development encompasses the child's process of development, as well as its outcomes, 'with the aim of enabling the child to fulfil her human potential to the maximum'.[81] Read together with article 3, the rights under article 6 include not only basic goals such as safety and security but more prospective concerns about the child's development and flourishing in the longer term. Peleg further argues that an assessment of the child's right to development should start with the eight specific developmental domains mentioned in the *CRC* – including physical, mental, moral, social, cultural, spiritual, personality, and talent – but should not necessarily be limited to these.[82] Accordingly, while the right to development requires a distinct assessment, there is substantial overlap with a holistic assessment of the child's best interests.[83]

While the principle of acting in the best interests of the child has been criticised for its indeterminacy, Eekelaar and Tobin argue this may be mitigated by taking an evidence-based approach, which at a minimum would consider the child's views, relevance of other *CRC* rights, parental views, individual circumstances (including developmental needs), and any available empirical evidence.[84] Moreover, as Lievens points out, given that '[a]t this moment in time, it is hard to assess and to predict the impact that practices such as exploitative data collection, processing and profiling activities in commercial environments will have on children's lives in the long term',[85] a precautionary principle (borrowing from environmental policy) is advisable:

---

78 See *CRC* (n 12) art 3(1).

79 *General Comment No 25*, UN Doc CRC/C/GC/25 (n 13) 7 [41].

80 *CRC* (n 12) art 6(2): 'States Parties shall ensure to the maximum extent possible the survival and development of the child'.

81 Noam Peleg, *The Child's Right to Development* (Cambridge University Press, 2019) 203.

82 Ibid 209.

83 Noam Peleg and John Tobin, 'Article 6: The Rights to Life, Survival, and Development' in John Tobin (ed), *The UN Convention on the Rights of the Child: A Commentary* (Oxford University Press, 2019) 186, 224.

84 John Eekelaar and John Tobin, 'Article 3: The Best Interests of the Child' in John Tobin (ed), *The UN Convention on the Rights of the Child: A Commentary* (Oxford University Press, 2019) 73, 94–5.

85 Eva Lievens, 'The Rights of the Child in the Digital Environment: From Empowerment to De-responsibilisation' in 5Rights Foundation (ed), *Freedom Security Privacy: The Future of Childhood in the Digital World* (2020) <https://freedomreport.5rightsfoundation.com/the-rights-of-the-child-in-the-digital-environment-from-empowerment-to-de-responsibilisation>.

> The responsibility for understanding how data is processed and assessing whether it is fair cannot be placed solely on children's shoulders, nor on those of their parents. On the contrary, fair processing of children's personal data requires legal restrictions on certain practices – keeping the precautionary principle in mind; enhanced responsibilities for data controllers – both public and private actors; and stronger enforcement by Data Protection Authorities.[86]

We agree with Lievens that the precautionary principle, 'compell[ing] society to act cautiously if there are certain – but not necessarily absolute – scientific indications of a potential danger and if not acting upon these indications could inflict harm',[87] is crucially important in this context. The special vulnerability that children have, arising from their still-developing abilities, is particularly acute when they encounter the subtle manipulative techniques of the adtech industry. Indeed, one recent survey suggests that children find it especially hard to resist these techniques: reporting that '[f]ew children made the "jump" from giving an account of targeted advertising to recognizing the algorithmic reshaping of the online environment',[88] and 'children tend to miss the "bigger picture," as most are not told or taught how … [personalisation] processes might influence their learning, exposure to diversity, choices or decision-making'.[89] As Susser, Roessler and Nissenbaum summarise the situation generally, '[b]eing steered or controlled, outside our conscious awareness, violates our autonomy, our capacity to understand and author our own lives'.[90] The point is especially pertinent regarding children whose sense of identity is still evolving and who are potentially more liable to influence from numerous unseen and self-interested commercial actors.

In other words, there is a strongly plausible case that adtech practices, which children on current evidence find difficult to fully comprehend and actively resist,[91] could harm their development, and if so, we argue, it is 'better to be safe than sorry' and adopt the precautionary principle when framing regulation.

---

86 Ibid. See also Helen Clark et al, 'A Future for the World's Children? A WHO–UNICEF–Lancet Commission' (2020) 395(10224) *Lancet* 605, 634 ('WHO–UNICEF–Lancet Commission'):

> [The precautionary principle] has been insufficiently applied to protect children from commercial marketing – commercial entities can market products to children with little evidence that they do not pose a threat to their wellbeing. Although evidence is emerging on the harms of commercial sector marketing to children, the fast-paced nature of technological change means children are actively being harmed while the body of evidence grows.

87 Lievens (n 85).

88 Stoilova, Livingstone and Nandagiri, 'Digital by Default' (n 30) 201.

89 Ibid.

90 Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, Autonomy, and Manipulation' (2019) 8(2) *Internet Policy Review* 1, 13.

91 See generally Stoilova, Livingstone and Nandagiri, 'Children's Data and Privacy Online' (n 29); Stoilova, Livingstone and Nandagiri, 'Digital by Default' (n 30).

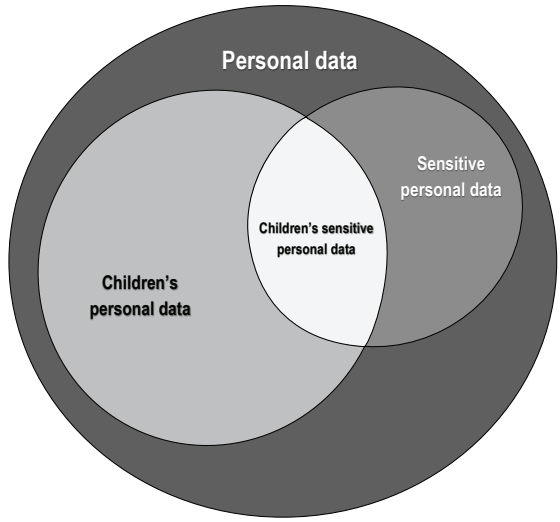

Figure 2: Children's sensitive personal data (eg, information about a child's racial or ethnic origin or a child's health) are particularly sensitive because they combine sensitivities arising from characteristics of the data subject and from the data's subject matter.

Children's special vulnerabilities are compounded where the sensitive data are drawn on or created in the construction of a consumer profile. Figure 2 shows the cumulative effect in terms of sensitivity when 'sensitive data' (eg, information about racial or ethnic origin or health) are combined with children's data. For instance, how are we to know (on present information) that targeting a child on the basis of inferences about their sexuality, state of mental or other health, political opinion or philosophical viewpoint (to give just some examples of commonly prescribed 'sensitive' data in data protection instruments, including the Australian *Privacy Act*),[92] derived from automated processing of their search histories and other accumulated data, will not detrimentally affect that child's development of their identity?[93] This potential for manipulation and impaired development may exist even apart from the special risks posed to children in some societies by disclosure of their sensitive data, for instance as to prohibited sexuality or

92 See *Privacy Act 1988* (Cth) s 6 (definition of 'sensitive information'). Cf *GDPR* (n 43) art 9 (processing of special categories of personal data).

93 See Office of the Australian Information Commissioner, 'Commissioner Launches Federal Court Action against Facebook' (Media Release, 9 March 2020) <https://www.oaic.gov.au/updates/news-and-media/commissioner-launches-federal-court-action-against-facebook>. It points to the ease with which such inferences may be made:

> Facebook's default settings facilitated the disclosure of personal information, including sensitive information, at the expense of privacy. We claim these actions left the personal data of around 311,127 Australian Facebook users exposed to be sold and used for purposes including political profiling, well outside users' expectations.

political or philosophical opinion. Indeed, we can imagine a spectrum of actual and potential risks and harms.[94] Thus, it is not surprising that *General Comment No 25*, referencing the best interests of the child, demands that 'States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling'.[95]

Nor is it just a matter of calling on States to comply with their international obligations under the *CRC*, including measures designed to 'control the gathering and exploitation of children's data and images for commercial purposes'.[96] The European regulatory trend is already moving in this direction by implementing stronger prohibitions on adtech in relation to children's data. Modelled in part on the *CRC*, article 24 of the *EU Charter* frames its own set of rights and obligations regarding children, including that '[i]n all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration'.[97] For instance, article 22 of the *GDPR* states that data subjects shall generally have the right 'not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her', with recital 71 adding that '[s]uch measure should not concern a child'.[98] The European Data Protection Board ('EDPB') has signalled that, although article 22 itself does not expressly prohibit this type of processing in relation to children, the recital flags that 'as a rule, controllers should not rely upon the exceptions in Article 22(2) to justify it'.[99] Further, the specific circumstances in which the EDPB contemplates that solely automated decision-making, including profiling, with legal or similarly significant effects in relation to children may be necessary, 'for example to protect their welfare', do not suggest any great latitude for adtech.[100]

In December 2020, the Irish Data Protection Commission ('DPC') took a decisive step in its draft 'Fundamentals for a Child-Oriented Approach to Data Processing' ('Fundamentals'). It stated that:

> organisations should not profile children, engage in automated decision-making concerning children, or otherwise use their personal data, for advertising/marketing

94 Cf WHO–UNICEF–Lancet Commission (n 86) 634.

95 *General Comment No 25*, UN Doc CRC/C/GC/25 (n 13) 7 [42].

96 WHO–UNICEF–Lancet Commission (n 86) 633. Indeed, the WHO–UNICEF–Lancet Commission proposes adding an Optional Protocol to the *CRC* regarding commercial marketing and targeting of children:

> Given the cross-border effects of commercial marketing, including through the internet and social media, and the multisectoral nature of the threat and needed response, an Optional Protocol to the *CRC* adopted by the UN General Assembly could address the transnational elements of the problem and simultaneously drive national action for legal protection.

97 *Charter of Fundamental Rights of the European Union* (n 52) art 24(2).

98 *GDPR* (n 43) art 22(1) (automated individual decision-making, including profiling), recital 71 (profiling).

99 The European Data Protection Board had endorsed the 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (Guidelines No WP251rev.01, 6 February 2018) <https://ec.europa.eu/newsroom/article29/items/612053> ('Guidelines'), adopted by its predecessor, the Article 29 Working Party. In the Guidelines, see especially Part V: Children and Profiling: at 28–9.

100 Ibid 28.

> purposes, unless they can clearly demonstrate how and why it is in the best interests of children to do so.[101]

The DPC added that:

> For the avoidance of doubt, the DPC does not consider that it is in the best interests of children to show them advertisements or auto-suggestions for other games/ services/ products/ videos etc which they might be interested in where such advertisements or suggestions are based on profiling. Accordingly there is a high burden of proof on the organisation to show how it is in the best interests of children to process their personal data for the purposes of profiling and/or automated decision making, or otherwise, in order to advertise/ market/ make auto-suggestions to them.[102]

Thus, quite neatly, the DPC is proposing that any use of adtech involving profiling or automated-decision making or auto-suggestive practices must be demonstrably in the best interests of children, adopting 'a high burden of proof' for the organisation concerned, or else the organisation must desist from engaging in such practices. Of course, it might legitimately be asked whether such stringent measures are required if lesser ones will suffice. The UK Information Commissioner's Office ('ICO') has published its own 'Age Appropriate Design: A Code of Practice for Online Services' ('Code') likely to be accessed by children.[103] This Code is more qualified in saying that the best interests of the child need merely to be 'taken [into] account' by the organisation and that 'essential features' are exempted:[104]

> You need to switch any options within your service which rely on profiling off by default, unless you can demonstrate a compelling reason why this should not be the case, taking account of the best interests of the child. You need to assess this in the specific circumstances of your processing.
>
> In practice it is likely to mean that any non-essential features that rely on profiling and that you provide for commercial purposes are subject to a privacy setting which is switched off by default.[105]

In short, the suggestion is that profiling should be turned off by default (rather than prohibited), unless there is demonstrably a compelling reason that it should be automatically turned on, taking account of the best interests of the child. However, it should be noted that these principles are not specifically concerned with adtech technologies and practices but are intended to be of general application. (In fact, the ICO is conducting a separate inquiry into adtech, which may not only explain the absence of their specific mention in the Code but may also provide further guidance in due course.) Further, the focus of the ICO's Code is on privacy-by-design principles that must be observed from the outset in developing services

---

101 'Fundamentals' (n 1) 54 [6.2.3].

102 Ibid.

103 The development of this Code was mandated by the *Data Protection Act 2018* (UK) and the Code was approved by the UK Parliament: see Information Commissioner's Office (n 11) 3.

104 Ibid 68. See Information Commissioner's Office, 'Our Work on Adtech' (Web Page, 2019) <https://ico.org.uk/about-the-ico/what-we-do/our-work-on-adtech/>.

105 Information Commissioner's Office (n 11) 68. Note also the ICO's general comment at 26, that '[t]aking account of the best interests of the child does not mean that you cannot pursue your own commercial or other interests. Your commercial interests may not be incompatible with the best interests of the child, but you need to account for the best interests of the child as a primary consideration where any conflict arises'.

used by children, whereas the focus of the DPC's draft Fundamentals is somewhat broader. The DPC concludes that 'the "Fundamentals" are entirely consistent with the UK Code and in particular it is clear that the best interests of the child principle underpins both'.[106] Our view is that the DPC's approach is more attuned to the precautionary principle advocated by Lievens, more likely to be fully compliant with the *CRC* best interest standard (as construed by *General Comment No 25*),[107] as well as matching the *EU Charter*'s requirement that that '[i]n all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration'.[108] While a prohibition on profiling for adtech is a strong protectionist measure in relation to children, it responds to the concerns of the 700+ children that were consulted for *General Comment No 25* in relation to commercial adtech practices.

In Australia, the ACCC's Digital Platforms Report recommends that the proposed enforceable privacy code to be developed by the OAIC should include 'additional restrictions on the collection, use or disclosure of children's personal information for targeted advertising or online profiling purposes and requirements to minimise the collection, use and disclosure of children's personal information'.[109] This code is likely also to result in some constraints being placed on adtech to protect the best interests of children, taking into account inter alia the strictures of the *CRC* and regulatory trends noted above. Of course, much will rest on the specific terms of the code as developed by the OAIC. We note also that the ACCC is currently conducting a review of adtech, with the Interim Report of the review signalling that 'the widespread collection and use of data for targeting purposes also has the potential to cause consumer harm if consumers are not sufficiently informed or do not have sufficient control over how their data is collected and used for ad targeting purposes'.[110] For the reasons discussed above, we hope that this review will further inspire effective controls in the OAIC code to address proactively the risks of adtech technologies and practices in relation to children, adopting a precautionary principle that takes into account the potential risks of harm to a child's development and their flourishing in the longer term.

---

106 'Fundamentals' (n 1) 54 [6.2.3].

107 See also United Nations Committee on the Rights of the Child, *General Comment No 16 (2013) on State Obligations Regarding the Impact of the Business Sector on Children's Rights*, UN Doc CRC/C/GC/16 (17 April 2013) 17 [62] ('[w]here there is a high risk of business enterprises being involved in violations of children's rights because of the nature of their operations or their operating contexts, States should require a stricter process of due diligence and an effective monitoring system').

108 *Charter of Fundamental Rights of the European Union* (n 52) art 24(2).

109 'Digital Platforms Report' (n 8) 481, recommendation 18. The ACCC also suggests that the issue of 'whether the *Privacy Act* should offer protections for inferred information, particularly where inferred information includes sensitive information, such as information about an individual's health, religious beliefs, or political affiliations' should be considered: at 476, recommendation 17.

110 See Australian Competition and Consumer Commission, 'Digital Advertising Services Inquiry' (Interim Report, 28 January 2021) 56 <https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-advertising-services-inquiry/interim-report>.

IV CONCLUSION

Children are amongst the most active users of digital services. It is possible that powerful platforms and businesses will have accumulated detailed profiles on every aspect of a young person's life by the time they reach adulthood. We believe that children's data protection should not simply be contingent on parental action or inaction. This is essential to ensure that children can effectively participate and flourish in an online environment in which business technologies and practices are adopted and extended at rapid pace. Thus, there is a real need for more effective regulation of the scale and character of personal data processing in ways that provide an appropriate balance between data privacy and the protection of competing rights and interests. Apart from improving processes of parental and children's consent, it is important also to consult children on their perspective of how that balance should be achieved and to give effect to their best interests. Policies that embed children's capacity and agency throughout legal design and implementation – as well as more stringent prohibitions on privacy-invasive adtech practices designed with children's best interests in mind – are more likely to respect children's freedoms and uphold the principles of the *CRC*.

The Australian Government has taken the positive step of undertaking to implement the ACCC's recommendations for a 'binding privacy code' covering children and other vulnerable groups – stating that the code to be developed by the OAIC will require digital platforms

> to be more transparent about data sharing; to meet best practice consent requirements when collecting, using and disclosing personal information; to stop using or disclosing personal information upon request; and include specific rules to protect personal information of children and vulnerable groups.[111]

In the meantime, the ACCC has commenced its digital advertising inquiry, as also tasked by the government. Ideally, these tandem law reform processes will enable a properly informed and considered approach to implementing desirable changes to the regulation of the technologies and practices of adtech that will benefit Australia's youngest digital citizens.

111 Treasury, Australian Government (Cth), 'Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry' (Report, 12 December 2019) 5 <https://treasury.gov.au/publication/p2019-41708>.