Minderoo Foundation thanks the Committee on the Rights of the Child for leading timely and urgent work on children’s rights in the digital environment. Established by Dr Andrew Forrest AO and Nicola Forrest AO in 2001, Minderoo Foundation is an Australian philanthropic organisation that takes on tough, persistent issues with the potential to drive massive change. As one of Asia’s largest philanthropic organisations, with almost AU$2 billion in funding available for a range of global initiatives, Minderoo Foundation is independent, forward-thinking and seeks effective, scalable solutions. Through the Frontier Technology Initiative, Minderoo Foundation is firmly committed to ensuring the rights and protections of the physical world carry into the digital world. In the spirit of elevating the voices and experiences of cohorts with lifelong digital experience, Minderoo Foundation has worked with three undergraduate students at the Australian National University’s College of Law, who have each focussed on a core area in technology policy. Minderoo Foundation is delighted to help make their voices heard.

*Please note, referencing has been hidden in this document to comply with strict word limits. Please contact the Frontier Technology Initiative for full bibliographic details.*

**SUMMARY**

This submission responds to the OHCHR Draft Comment with a particular focus on the way the digital world impacts on children’s right to privacy and development, by reference to Articles 6 and 16 of the *Convention on the Rights of the Child.*

This submission recommends:

1. The Comment should recognise that under the current preferred legal framework of parental consent models, children’s rights are not adequately protected. Responsibility should not rest with children and their parents to manage the parameters of their rights in the digital world. To ensure States are upholding children’s rights, States should implement specific legal restrictions on companies, requirements for online platforms and new digital privacy rights.
2. The Comment should make clear that businesses trading in data are infringing children's rights and should highlight the dangers of data misuse on children’s future lives. States should be encouraged to States should seek to proactively legislate for a class of protected data that cannot be collected under any circumstances. This could include any data collected from a child that could foreseeably impact that child’s rights, now or in the future.
3. The Comment should provide additional guidance and examples of privacy and safety by design elements that States should require digital platforms to implement to better protect children. For example, States could mandate proactive inservice notification of children’s data collection and use by third parties as well as more understandable, short and clear terms of use policies.
4. The Comment should also look towards an expansion of the right to privacy in the context of the digital world. This could include a ‘right to erase’ where children are able to compel digital platforms to erase any personal data they have collected and stored.

**I THE PROBLEM**

Imagine a child walks into a library. There is someone watching their every move and writing down everything the child does in a notebook - what books they choose to read, which ones they choose to put back, how long they spend browsing the shelves. Once the child leaves the library, the same person follows them, noting location, habits, interactions. At the local playground, someone at the gate asks for sensitive personal information as a condition of entry. They also ask the other children to share their information when they arrive. The person form the library joins the playground gatekeeper and together they watch all children in the playground, noting how they play, what topics they talk about, how long they spend on each piece of equipment, noting down their observations extensively. The librarian and gatekeeper sell excerpts from these notebooks to strangers the child has never met, hours, days, years after the event.

We would never accept this level of intrusion into children’s privacy in the real world - so why do we accept it in the digital world?

*A Surveillance, Data Capture and Data Misuse*

Digital platforms are constantly surveilling their users, including children. They routinely collect data through express disclosure and background tracking.[[1]](#endnote-1) The data targeted includes behavioural information on platform interaction, as well as web browsing history, and geolocation and extends to sensitive personal information such as ethnicity, religion, level of affluence and age group.[[2]](#endnote-2)

The accumulation of the data that users produce through interaction with the platform is an inherent component of the business model of digital platforms.[[3]](#endnote-3) The vast amounts of information gathered becomes the commodity digital platforms utilise to raise revenue.[[4]](#endnote-4) The data helps predict and modify human behaviour as a means of market control, so users become a product that technological companies can sell to advertisers.[[5]](#endnote-5) Companies can also sell and trade in user data to third parties with an interest in accessing personal information.[[6]](#endnote-6) This phenomenon has convincingly been described as “surveillance capitalism”.[[7]](#endnote-7)

Children are particularly vulnerable to these exploitative practices as they are in the primary developmental period of their lives. The nature of the data is highly sensitive and personal, and should not be subject to the trading, selling and sharing that digital platforms engage in to raise revenue. There is an unacceptable risk of this data being misused and potentially impacting their later life.

Evidence of data misuse by digital platforms is prevalent. Ireland’s Data Protection Commission is currently investigating complaints about data misuse by Instagram, who made the email addresses and phone numbers of users under 18 public.[[8]](#endnote-8) Google has already faced a 170 million dollar fine for illegally gathering and distributing children’s data from Youtube to advertisers without parental consent.[[9]](#endnote-9)

The impact of the COVID-19 pandemic has only made these issues more pertinent. Children are required to use online education platforms to participate in their schooling. G Suite for Education apps and Chromebooks, both owned and operated by Google, have become increasingly popular with 80 million students globally using G Suite for Education in 2018.[[10]](#endnote-10) Google has already been accused of data misuse in relation to these education tools, with lawsuits being filed against its use of student data to create face templates and voice prints of children.[[11]](#endnote-11) As the pandemic continues, the risk of data misuse increases due to the compulsory nature of participation through these online educational tools.

**II THREATS TO CHILDREN’S RIGHTS - ARTICLE 6 AND ARTICLE 16**

*A Article 6: Right to Life, Survival and Development*

Article 6 of the Convention outlines children’s right to life, survival and development.[[12]](#endnote-12) Various General Comments from the Committee on the Rights of the Children illustrate that development is a “holistic” concept that should be interpreted broadly.[[13]](#endnote-13) This includes the development of the ongoing “physical, mental, spiritual, moral, psychological and social” wellbeing of children.[[14]](#endnote-14) Thus, states under this right are required to actively create healthy and protected environments so children are able to grow to their fullest potential.[[15]](#endnote-15) As one of the guiding principles, Article 6 has paramount importance and is a baseline informing all the other rights outlined in the Convention.[[16]](#endnote-16)

Considering the broad interpretation of this right, in the context of the digital environment, children should be protected from the potentially adverse effects that data collection and trade practices can have on their future. Routine surveillance, tracking and accumulation of data on users by technology companies has particular risks for children. Their practices have the capacity to harm children’s development as information collected can be used against them later in life.

For example, Human Resource companies across the world are increasingly turning to AI to recruit workers and make hiring decisions.[[17]](#endnote-17) In a 2018 Gartner Inc. study, 23% of organisations were found to be using AI for recruiting purposes.[[18]](#endnote-18) With these AI tools becoming more focused on assisting with employment decision making, they are potentially utilising and buying sensitive user data from other digital platforms, such as academic and health data.[[19]](#endnote-19) Therefore, children’s data that is currently being collected on online platforms has the risk of being used by these AI programs later on in their lives to adversely affect their employment prospects. In future it also seems likely that insurers will draw on data like this for decisions on whether to offer insurance or not.[[20]](#endnote-20)

Ideas, thought and participation more readily shift in childhood and adolescence.[[21]](#endnote-21) Children should not be held to the views they have, groups they participate in or ideas they communicate as adults. This is a fundamental risk to their right to development and the realisation of their full potentials.

*B Article 16: Right to Privacy*

Article 16 states that children’s “privacy, family, home or correspondence” should be protected from “arbitrary or unlawful interference”.[[22]](#endnote-22) The scope of this right remains very broad, especially considering jurisprudence on Article 17 of the ICCPR (which reflects Article 6 of the CRC) has recognised that the right to privacy encompasses rights beyond those listed in the Convention. For example, the right to freely express one’s identity was extrapolated by the Human Right’s Council (HRC) from Article 17 in *Coeriel and Aurik v The Netherlands*.[[23]](#endnote-23) In applying this to the digital environment, the HRC outlined a similarly broad view, commenting that regardless of if the data is actually used, any interception, collection and capture of “communications data” infringes privacy.[[24]](#endnote-24)

Invasive data capture and tracking practices are routine realities for digital platforms under surveillance capitalism. Facebook and Google, the two most popular digital platforms amongst young Australians, have been the pioneers of this system.[[25]](#endnote-25) They offer the promise of a ‘free service’, whether that be a social media networking site or search engine. However, the hidden price has always been the collection, retention and selling of private and sensitive user information. The monopoly Google and Facebook in particular retain of the digital world has only enlarged the information sharing and thus accumulation across these services.

**III PART OF THE PROBLEM - CONSENT MODELS**

The ‘regulatory’ framework used to protect children’s rights against data collection is typically a consent model. Key examples are the Children’s Online Privacy Protection Rule (COPPA) in the United States which prescribes that digital platforms must gain parental consent to their terms and conditions of use (including acceptance of their data collection practices) for users under 13 years before collecting data.[[26]](#endnote-26) The General Data Protection Regulation (GDPR) in the European Union has prescribed similar requirements for online platforms.[[27]](#endnote-27) Although the most common method employed by states, parental consent cannot adequately protect young people from the invasive online surveillance and harmful data collection practices of companies.

Critiques on parental consent have centred around the fact that the interests of the child cannot properly be taken to mean the interest of the parent.[[28]](#endnote-28) Indeed, equating the two seems to go against understandings of children’s right to be heard (Article 12 of the Convention).[[29]](#endnote-29)

However, more than that, parental consent models assume that parents are more capable of making decisions around digital privacy than their children. [[30]](#endnote-30) However in the digital world, “informed” consent is not possible.[[31]](#endnote-31) Digital platforms’ privacy policies are often extensive, vague and complex so individuals are not able to completely understand the implications of consenting to a particular policy. [[32]](#endnote-32)

Meaningful consent would also imply that it is ‘freely given’. Terms and conditions are usually presented as an ‘all or nothing’.[[33]](#endnote-33) Users who may agree with certain terms and not others cannot participate on these platforms at all unless they consent to the entirety of the data use practices outlined.[[34]](#endnote-34) The Australian Competition and Consumer Commission (ACCC) in their *‘Digital Platforms Inquiry’* highlight that there is a fundamental bargaining power imbalance in this exchange.[[35]](#endnote-35) Large digital platforms, particularly social media sites, often offer a non-replaceable service. Clear examples are Instagram and Facebook which are the most popular social media platforms in Australia amongst young people.[[36]](#endnote-36) These platforms have a monopoly over the social networks of their peers. Without any viable alternative platforms, users are inclined to concede terms and conditions they may not completely agree with for the sake of access.[[37]](#endnote-37)

In the physical world, this could be represented by a privately run shopping centre where children are customers. The shopping centre has also become the only place children can socialise and meet with all their friends. Upon entry, a gatekeeper demands full surrendering of their rights to personal information. Children also must provide a full locational history of where they have been before entering, and what their plans are after they exit the shopping centre. On-selling this information is where 98% of the shopping centre’s revenue comes from.[[38]](#endnote-38)

Furthermore, children’s increasingly ingrained social media habits is central to platform companies’ monetisation models.[[39]](#endnote-39) Social media platforms incline individuals towards routine and habitual information disclosure.[[40]](#endnote-40) Hence, individual responsibility put on users and their parents to manage and control their data through consent models is not ultimately effective.

Steeves argues that all consent models have done is legitimise the collection and use of data by digital platforms.[[41]](#endnote-41) This is because despite implementation of parental consent, and general consent regulations by governments, surveillance and data capture have continued.[[42]](#endnote-42) It has done nothing to actively curb the invasive practices of online platforms, but merely allows it to occur under accepted terms.

Therefore, recommendations for regulatory frameworks should move away from consent systems of individual accountability and towards frameworks that shift responsibility back onto digital platforms themselves.[[43]](#endnote-43)

**IV AN ALTERNATIVE FRAMEWORK**

The ‘Safety by Design’ initiative of the Australian eSafetyComissioner is one example of a potential alternative approach. Created through extensive consultation with young Australians,[[44]](#endnote-44) the report outlines a series of voluntary design reforms for digital platforms.[[45]](#endnote-45) It seeks to shift the responsibility for safety away from children and onto technology companies.[[46]](#endnote-46)

1. Key recommendations were focused around three principles: service provider responsibility, user empowerment and autonomy, and transparency and accountability.[[47]](#endnote-47) Privacy recommendations include ensuring terms and conditions of use, and data use policies are easy to find and understand and users should be notified directly of any changes through “in-service communications”.[[48]](#endnote-48) Furthermore, young people should be actively notified of which third party companies have access to their information and how their information is being used.[[49]](#endnote-49) Finally, children should be able to have more active control over what personal data is collected and stored.[[50]](#endnote-50)

These principles should apply not just for children, but across all ages. As we begin to understand the pervasive nature of the problems of digital platform’s data capture and use practices, adequate protection for children involves the strengthening of privacy rights for everyone.

1. The effectiveness of this proposed framework is undermined by the fact that implementation is voluntary for digital platforms. With digital platforms incentivised by existing business models to continue to capture, sell and trade as much user data as possible, it is unlikely that encouraging digital platforms to voluntarily incorporate these design reforms will effectively lead to widespread adoption. Nonetheless, these recommendations are a helpful starting point for ensuring online environment are safer for children.
2. **V RECOMMENDATIONS FOR THE DRAFT COMMENT**

*A Recommendations Under Article 6*

The Draft Comment does not include any discussion of how digital surveillance and data capture practices can impact children’s right to development and life in the long term. This is a significant gap. A paragraph should be inserted that actively acknowledges this risk and makes note of the potential areas of children’s lives where data misuse could be most harmful.

We recommend that, beyond the limitations already present in the GDPR and COPPA, states should legislate for a class of children’s data forbidden from retention, storage, on-selling, or sharing by digital platforms under any circumstances. This could include any data collected from a child that could foreseeably impact that child’s rights, now or in the future. This means there should be certain circumstances where “legitimate, overriding grounds” for the collection and processing of certain data is not a permissible defence for data controllers.

We also suggest that states legislate to make many of the key design recommendations from above **compulsory** for digital platforms with children users. In particular, children and parents must be notified through in-service communication when any third party company gains access to any of their information. Within that notification, third parties should also be required to proactively communicate how they intend to use their data.

*B Recommendations Under Article 16*

The draft comment in its discussion of Article 16 recognises the existence of pervasive data collection and surveillance practices by digital platforms. The Draft Comment should further note that businesses that trade in children's personal data are inherently contravening the right to privacy under the CRC.

The Draft comment also guides states to ensure parental and children’s consent is “freely given” and “informed”. Following on from the discussion above, we suggest that this section of the comment should be revised to recognise that consent cannot be fully “informed and freely given” either by children or their parents. Furthermore, the Draft Comment should urge States to move away from parental consent models altogether.

Although the Draft Comment compels countries to “encourage…privacy by design”, we suggest that the Draft Comment should guide States to oversee the compulsory implementation of these particular design elements on digital platforms with children users. Specifically, having clear, short, accessible and easy to understand data use policies that cannot be changed arbitrarily without actively notifying users.

The HRC has suggested that “individuals should have the right to request rectification or elimination” or any incorrect data that is retained or collected.[[51]](#endnote-51) The Draft comment further outlines that children and parents should have the right to “delete” data that is “unlawfully or unnecessarily” stored. We recommend that this be extrapolated further and formalised to become a ‘right to erase’. States should legislate to support this digital right where children and adults have the right to have any personal data collected by digital platforms erased by those platforms at any point in time.

**Through implementing these recommendations, the Draft General Comment will be able to provide a more comprehensive and effective guide for States to support the protection of children’s rights in the digital world as it relates to Articles 6 and 16 of the CRC.**

1. Valerie Steeves, ‘Terra Cognita: The Surveillance of Young People’s Favourite Websites’ in Tonya Rooney & Emmeline Taylor (ed), *Surveillance Futures: Social and Ethical Implications of New Technologies for Children and Young People* (Routeledge, 1st Edition, 2016). [↑](#endnote-ref-1)
2. Valerie Strauss, ‘Legislators Ask 50-plus Firms to Explain How They Use the ‘Vast Amount of Data’ They Collect on Students’, *The Washington Post* (online, 20 August 2019) <<https://www.washingtonpost.com/education/2019/08/20/legislators-ask-plus-firms-explain-how-they-use-vast-amount-data-they-collect-students-which-ones-facebook-google-blackboard-etc/>>. [↑](#endnote-ref-2)
3. Shoshana Zuboff, ‘Big Other: Surveillance Capitalism and the Prospects of an Information Civilization’ (2015) 30(1) *Journal of Information Technology*, 75, 75. [↑](#endnote-ref-3)
4. Ibid. [↑](#endnote-ref-4)
5. Ibid. [↑](#endnote-ref-5)
6. Ibid 85. [↑](#endnote-ref-6)
7. Ibid 75. [↑](#endnote-ref-7)
8. Aishwarya Nair, ‘Irish Regulator Probes Facebook’s Handling of Children’s Data on Instagram’, *Reuters* (online, 19 October 2020) <<https://www.reuters.com/article/europe-privacy-facebook-idUSKBN27404M>>. [↑](#endnote-ref-8)
9. Siobhan O’Flynn, ‘Protecting Children’s Data Privacy in the Smart City’, *The Conversation* (online, 16 May 2019) <<https://theconversation.com/protecting-childrens-data-privacy-in-the-smart-city-113319>>. [↑](#endnote-ref-9)
10. Rachel Premack, ‘Google is Filling High School Classrooms with Androids and Chromebooks – But the Kids Just Want iPhones’, Business Insider (online, Dec 18 2018). <<https://www.businessinsider.com/google-classroom-dominating-schools-kids-want-apple-products-iphone-2018-12?r=AU&IR=T>>. [↑](#endnote-ref-10)
11. Jane Bailey et. al, ‘Children’s Privacy is at Risk with Rapid Shifts to Online Schooling Under Coronavirus’, *The Conversation* (online, 22 April 2020) <<https://theconversation.com/childrens-privacy-is-at-risk-with-rapid-shifts-to-online-schooling-under-coronavirus-135787>>. [↑](#endnote-ref-11)
12. *Convention on the Rights of the Child*, signed 20 November 1989, UNTS vol. 1577, p. 3, (entered into force 2 September 1990) art 6. [↑](#endnote-ref-12)
13. Committee on the Rights of the Child, *General Comment No. 14 On the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration (art 3, para 1),* 62nd sess, UN Doc CRC/C/GC/14 (29 May 2013) (‘*GC 14*’).  [↑](#endnote-ref-13)
14. Committee on the Rights of the Child, General Comment No. 5 *General Measures of Implementation of the Convention on the Rights of the Child (arts. 4, 42 and 44, para 6)* 34th sess, UN Doc CRC/C/GC/2003/514 (27 Nov 2003) (‘*GC 5*’).  [↑](#endnote-ref-14)
15. Nowak Manfred, *Commentary on UN Convention on the Rights of the Child: The Right to Life, Survival and Development*, (Brill 2005), 2. [↑](#endnote-ref-15)
16. Ibid 1. [↑](#endnote-ref-16)
17. Sara Castellanos, ‘HR Departments Turn to AI-Enabled Recruiting in Race for Talent’, *The Wall Street Journal* (online, 14 March 2019) <<https://www.wsj.com/articles/hr-departments-turn-to-ai-enabled-recruiting-in-race-for-talent-11552600459>>. [↑](#endnote-ref-17)
18. Ibid. [↑](#endnote-ref-18)
19. O’Flynn (n 9). [↑](#endnote-ref-19)
20. Zuboff (n 3) 85. [↑](#endnote-ref-20)
21. Marcia C Linn & Nancy B Songer, ‘Cognitive and Conceptual Change in Adolescence’, 99(4) *American Journal of Education* (1991) 379. [↑](#endnote-ref-21)
22. *Convention on the Rights of the Child*, art 16. [↑](#endnote-ref-22)
23. Human Rights Committee, *Views: Communication No 453/1991*, 52nd sess, UN Doc CCPR/C/52/D/453/1991 (9 December 1994) (*‘Coeriel and Aurik v The Netherlands*’). See also Human Rights Committee, *Views: Communication No 488/1992*, 50th sess, UN Doc CCPR/C/50/D/488/1992 (25 December 1991) (‘*Toonen v Australia’*). [↑](#endnote-ref-23)
24. UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, 27th sess, UN Doc A/HRC/27/37 (30 June 2014). [↑](#endnote-ref-24)
25. Zuboff (n 3) 77. [↑](#endnote-ref-25)
26. *Children’s Online Privacy Protection Act of 1988*, 15 USC §§ 6501–6506 (WestLaw 2020). [↑](#endnote-ref-26)
27. *Regulation (EU) 2016/679 of the European parliament and of the Council 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. [↑](#endnote-ref-27)
28. Simone Van der Hof, ‘I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World’ (2017) 34(2) *Wisconsin International Law Journa*l, 409; Jelena Gligorijević, ‘Children’s Privacy: The Role of Parental Control and Consent’ (2019) 19(2) *Human Rights Law Review* 201, 202..; David D Meyer, ‘The Modest Promise of Children’s Relationship Rights’ (2003) 11 *William & Mary Bill of Rights Journal* 1117, 1118. [↑](#endnote-ref-28)
29. Van der Hof (n 28) 419. [↑](#endnote-ref-29)
30. Ibid 435-440. [↑](#endnote-ref-30)
31. Steeves (n 1). [↑](#endnote-ref-31)
32. Australian Competition & Consumer Commission, *Digital Platform’s Inquiry* (Final Report, June 2019). [↑](#endnote-ref-32)
33. Ibid 498. [↑](#endnote-ref-33)
34. Ibid. [↑](#endnote-ref-34)
35. Ibid. [↑](#endnote-ref-35)
36. Steeves (n 1). [↑](#endnote-ref-36)
37. Van der Hof (n 28). [↑](#endnote-ref-37)
38. 98% of Facebook’s revenue comes from advertising, whereas for Google it is 90% of its revenue; Barbara Kurshan, The Elephant in the Room With EdTech Data Privacy, *Forbes* (online, 22 June 2017) < <https://www.forbes.com/sites/barbarakurshan/2017/06/22/the-elephant-in-the-room-with-edtech-data-privacy/?sh=14aad7e757a5>>. [↑](#endnote-ref-38)
39. Clare Southerton & Emmeline Taylor, ‘Habitual Disclosure: Routine, Affordance and the Ethics of Young Peoples Social Media Data Surveillance’ (2020) 6(2) Social Media and Society, 1, 3. [↑](#endnote-ref-39)
40. Ibid 7. [↑](#endnote-ref-40)
41. Steeves (n 1). [↑](#endnote-ref-41)
42. Ibid. [↑](#endnote-ref-42)
43. Southerton and Taylor [↑](#endnote-ref-43)
44. eSafetyCommissioner, *Safety by Design* (Report, 2019) 7. [↑](#endnote-ref-44)
45. Ibid. [↑](#endnote-ref-45)
46. Ibid. [↑](#endnote-ref-46)
47. Ibid 21. [↑](#endnote-ref-47)
48. Ibid 32. [↑](#endnote-ref-48)
49. Ibid 15. [↑](#endnote-ref-49)
50. Ibid. [↑](#endnote-ref-50)
51. GC 16. [↑](#endnote-ref-51)