Inquiry into international digital platforms operated by Big Tech companies

Submission by the Alannah & Madeline Foundation

February 2023

Contents

Executive summary

We welcome the opportunity to contribute to the inquiry by the Senate Economics References Committee into international digital platforms operated by Big Tech companies. The inquiry's issues paper has a strong focus on the economic risks posed by large international platforms to Australian businesses. However, we believe there are other costs associated with technologies that were not designed with children's rights in front of mind: costs in areas such as privacy, safety and wellbeing.

Our submission addresses the fourth item in the inquiry's Terms of Reference: 'the collection and processing of children's data, particularly for the purposes of profiling, behavioural advertising, or other uses'.

Digital technologies are fully integrated into the lives of most Australian families, with four out of five school-aged children owning at least one personal screen-based device. The average Australian child owns more than three screen-based devices.[1] By age 16-17, approx. 8 out of ten young Australians use social media daily.[2] Many of these products and services are enjoyed and valued by children.

However, many digital platforms derive their profits from user engagement and handling of users' data. This has led to design features which pose threats to children's wellbeing and rights, however unintentionally. Concerns include loss of control over personal information, contact with undesirable individuals, and exposure to manipulative advertising or marketing, age-inappropriate material and anti-social behaviours. We recognise that digital platforms did not intend for these problems to occur. But they are the product of an approach which prioritised commercial gain over the best interests of children.

There are many ways that digital products and services can be made safer for children and we support the 'Safety by Design' work led by the eSafety Commissioner. However, we believe it is unlikely that all digital platforms will introduce safer features proactively and voluntarily – regulation is important.

We hope to see the evolution of Australia's approach to regulating the handling of children's data by digital platforms, moving towards regulation which is drafted and led by legislators and/or public regulators. To align with promising developments in overseas jurisdictions, such regulation would require digital platforms to:

- treat the best interests of the child as the primary consideration in relation to the handling of children's data
- refrain from handling children's data in ways shown to be harmful to children
- recognise children as anyone under the age of 18
- undertake data protection impact assessments, with a particular focus on risks to children that arise from the handling of their data
- set privacy / safety settings to 'high' by default for products and services used by children, unless there is a compelling reason to do otherwise guided by the best interests of the child
- ensure that age assurance mechanisms function to help protect children's rights and are proportionate to the nature and risk of the data processing activities
- communicate with children in clear, concise, accurate, accessible ways
- use parental controls to supplement safety-by-design, not replace or undermine it.

Key overseas models include the UK's Age Appropriate Design Code and Ireland's Fundamentals for a Child Oriented Approach to Data Processing. During the past couple of years, as these regulatory models have emerged, a number of digital platforms have strengthened their protections for children.

In order for legislation and regulatory frameworks to be meaningful, however, public regulatory bodies must be resourced adequately so that they can identify and analyse new and emerging trends, scrutinise the design and function of digital products and services, and address any breaches.

Finally, we welcomed the issues paper's recognition of the rise of the 'metaverse' – although we suspect immersive technologies and 'extended reality' may have implications beyond those identified. We encourage investment in research and policy development to explore the ramifications of new technologies for society, economy and governance and to plan the Australian Government's response. We urge that policy-making in this space be informed by expertise in children's rights and function to uphold the best interests of the child.

About us

The Foundation was established the year after the Port Arthur tragedy, by Walter Mikac AM in memory of his two young daughters, Alannah and Madeline. Our vision is that all children and young people are safe, inspired and have freedom to flourish.

Over the last 25 years our work has grown and evolved but our purpose remains the same. We have three program streams:

- Safe and Strong: recovering and healing from trauma. Very much linked to our origin story, we have a specialist trauma recovery and therapy service for children who have experienced significant trauma. This has grown in recent years to include working with early childcare providers, kindergartens and now primary schools to help them build their trauma informed capability and practices. Most of our work in trauma healing and recovery is Victorian based, with our therapists and consultants working from our client's homes, education and care settings and places of work.

- Safe and Strong: building positive digital citizens. The Foundation works with schools, families and communities nationally to help children build the digital intelligence, skills and competencies they need to stay safe online and to be active, positive digital citizens. With over 10 years' experience working in online bullying and wellbeing, as technology has become ubiquitous, our work has developed into building digital intelligence, digital ethics and media literacy for all children aged 3-18.

- Safe and Strong: bringing children's rights to life. As a rights-based organisation, this is our policy and advocacy work. Since inception, we have advocated for firearms safety, and we convene the Australian Gun Safety Alliance. In other key policy matters related to our programs, we work closely with the Officer of the eSafety Commissioner, the Prime Minister's National Office for Child Safety, and other major agencies such as the Australian Federal Police.

In 2018, we partnered with Kate and Tick Everett, after the tragic suicide of their daughter, Dolly. With them we worked to establish Dolly's Dream.

- Safe and Strong: Dolly's Dream, changing the culture of bullying. The purpose is the same, but the programs and services (Parent Hub, telephone help line, school and community workshops etc.) are specifically designed for remote, rural and regional families and communities, to meet their unique needs and contexts.

Recommendations

1. Support the development of legislator- or regulator-led frameworks in relation to the handling of children's data by digital platforms. Frameworks should require digital platforms to treat the best interests of the child as the primary consideration in relation to the handling of children's data and refrain from handling children's data in ways shown to be harmful to children. We refer here to

leading overseas models such as the UK's Age Appropriate Design Code and Ireland's Fundamentals for a Child Oriented Approach to Data Processing, as well as UNICEF's 'Case for Better Governance of Children's Data: a Manifesto'. Regulatory models should be:

- high-level enough to remain relevant as new digital technologies emerge, such as immersive technologies or 'extended reality' (aka the 'metaverse')
- developed through meaningful engagement with children, parents, caregivers and educators
- define the 'best interests of the child' in line with the United Nations Convention 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' (2013), which aims to ensure 'both the full and effective enjoyment of all the rights recognized in the Convention and the holistic development of the child.'

2. Review the adequacy of resourcing to public regulatory bodies charged with upholding legislation and regulations concerning the handling of individuals' data by digital platforms. Where necessary, increase resourcing to regulatory bodies to ensure they can evolve their capacity and capabilities to meet the need – eg. so they can adequately scrutinise the design and delivery of digital products and services and identify and address any breaches. We refer to the members of the Digital Platform Regulators Forum: the eSafety Commissioner, the Office of the Australian Information Commissioner, the Australian Communication and Media Authority, and the Australian Competition and Consumer Authority. We would also welcome further investment in regular, high-quality, large-scale studies of children's experiences online and any shifts observed following introduction of legislation, regulation and support services. This would help to answer the question (posed in the issues paper) of how effective Australia's legislative framework is in protecting children from online harms.

3. Support investment in research and policy development concerning the likely societal, economic and legislative implications of immersive technologies emerging via pathways like the 'metaverse'. Any policy and legislation developed in response should be informed by expertise on the rights of the child and should treat the best interests of the child as the primary consideration in relation to the handling of children's data by digital platforms.

4. Consider how the recommendations of this inquiry will have regard to the parallel consultation occurring about the Australian Government's response to the Privacy Act Review Report, and the ACCC's Digital Platform Services Inquiry.

The need for safety by design

Many concerns have been raised about how digital platforms handle children's personal information – although we do not believe digital platforms have to be large or based overseas in order to pose a risk.

In their 2019 Digital Platforms inquiry, the ACCC found that digital platforms provided a wide range of services that were enjoyed and valued by their customers. Often, these services appeared to be 'free' – but their profits were made through user engagement and handling of individuals' data. Many platforms collect vast amounts of information about individuals and have broad discretion as to how they use it.[3] These priorities profoundly shape digital products and services at a design level.

The issues paper for this inquiry lists various harms that children may experience via digital platforms: image-based abuse, grooming, cyberbullying, stalking, dis/misinformation, and distressing content. We submit that children's risk of exposure to these experiences – and others, such as dysregulated use of technology,

excessive spending, and threats to privacy – has been increased by design elements in many digital platforms which were placed there in order to drive engagement and data-gathering.

Risks and harms which can be encouraged, facilitated or intensified by design elements include:

- Loss of control over personal data due to platforms' terms of service which effectively make use of the product or service conditional upon individuals 'consenting' to their data being handled in ways they may not even understand. Many digital platforms have terms and conditions and privacy policies which are long and complex, often bundling items together in a 'take it or leave it' format which gives individuals very little in the way of meaningful choice.[4] For example, a 2019 survey of over 1,000 Australian adults found that only 19% agreed 'I fully read and understand the terms and conditions of websites I use'.[5] A recent review of 'edtech' products used in Australian schools found that it was common for these websites and apps to monitor, track or profile students via their data.[6]

- Loss of money or privacy due to manipulative design elements aimed at commercial gain. Features include targeted advertising; advertising disguised as regular content; automatic subscription renewals and subscriptions that are hard to cancel; 'scarcity cues' or notifications about other customers' activities intended to pressure individuals to make purchases quickly; loot boxes and in-game advantages for players who buy extra products; and 'nudging' and 'nagging' techniques to encourage purchases or subscriptions.[7] Recent Australian research found that young people were especially vulnerable to such 'dark patterns' – eg. young people were more likely than the general population to have bought or signed up for something by accident, spent more money than they intended, or shared more information than they wished.[8]

- Exposure to age-inappropriate material – eg. violent, sexual, illegal, extremist or disinformation – due to recommender systems which promote material based on the user's past activity or the activity of 'similar' accounts. Related concerns exist about autoplay functions on video streaming services (designed to keep people watching for longer) and prioritising of paid-for content.[9]

- Contact with strangers encouraged or enabled through direct messaging functions, accounts set to 'public' by default, recommender systems which suggest friends or followers based on similar interests or shared contacts, and popularity metrics which reward high numbers of 'likes'.[10]

- Engagement in, or exposure to, anti-social behaviour. It is harder to attribute this problem directly to design issues, but it seems reasonable to assume the risk is enhanced by features like popularity metrics, which can serve to reward shocking or emotive content; manipulation of user emotions, for example through recommending of extreme material; and 'echo chambers' encouraged by algorithms which sometimes function to normalise anti-social conduct.

If these issues are difficult for adults to manage responsibly, the risks are clearly higher for children, given their inexperience and early stage of development. Some design elements in digital platforms could be seen as increasing the risk that children's rights will be violated, especially:

- Article 16 (United Nations Convention on the Rights of the Child): 'No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.'
- Article 34: 'States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse.'

- Article 36: 'States Parties shall protect the child against all other forms of exploitation prejudicial to any aspects of the child's welfare.'

We recognise that the above-mentioned design features were not intended to cause harm. But they have helped to facilitate it, however inadvertently, due to a prioritising of commercial gain ahead of children's best interests.

The good news is: the design of digital products and services can be altered to strengthen protections for children. Features believed to enhance child safety include:

- setting children's accounts (or everyone's accounts) to the highest levels of privacy and safety by default, recognising that the 'status quo' effect leads many individuals to leave original settings in place.[11] High privacy and safety settings might include: hiding popularity metrics (eg. numbers of likes, followers and views); disabling private messaging features; limiting comments on children's videos to their friends and followers; disabling friend recommendations; ensuring children's profiles are not visible or searchable to adult users; and turning off geolocation functions unless necessary for the service provided.
- avoiding 'nudge' techniques that encourage children to reduce their privacy
- allowing separate privacy settings for different users of the same device – eg. a parent and a child
- turning off mechanisms which allow tracking of children's online activity for advertising purposes
- ensuring that games can be played enjoyably without purchasing extra features and that in-game purchases require explicit, active involvement by the payment account holder – eg. a parent
- making reporting tools and terms of service clearly visible, accessible and understandable
- ensuring any parental tracking measures are transparent to both parent and child
- avoiding collection and processing of children's biometric data
- investing in high-quality moderation to address children's complaints swiftly and transparently
- adding automatic prompts that encourage individuals to moderate any offensive language and read articles before sharing them.[12]

However, given the commercial imperative that has driven digital platforms historically, it is unrealistic to expect they will all introduce such changes voluntarily and proactively. Regulation is needed.

Meanwhile, we support the 'Safety by Design' work led by Australia's eSafety Commissioner. Through guiding principles, resources and engagement with the digital sector and its investors, this project aims to put the safety and rights of users at the centre of the design and development of online products and services. The three principles central to safety by design are: service provider responsibility to evaluate known and anticipated harms in the design and provision of a product or service; user empowerment and autonomy to support safe online interactions; and transparency and accountability by digital platforms and services.

Building protection for children's rights at least equivalent to international good practice

The inquiry's issues paper asks 'How effective is the current legislative framework in protecting children and preventing online harm from occurring?' and 'What more can be done to enhance online safety for child protection in Australia?'

Australia's Online Safety Act was an important step forward in legislating to better address cyber bullying, image-based abuse and illegal content, and to build basic safety expectations into digital services and products, including via industry codes. Some online conduct risks – such as image-based abuse, severe bullying and child sexual exploitation – are also addressed through various federal and state criminal codes. Proposed changes to the Privacy Act will also be relevant to the handling of children's data.

However, there is a gap in regulation in Australia: at present, we do not require digital platforms – across the board – to prioritise the best interests of the child and refrain from using children's data in ways shown to cause harm to children.[13]

This puts Australia at risk of falling behind overseas jurisdictions. Regulatory and policy approaches with a focus on the best interests of the child include the UK's Age Appropriate Design Code; California's Age Appropriate Design Code; Ireland's Fundamentals for a Child-Oriented Approach to Data Processing; the Dutch Code for Children's Rights; the Swedish Rights of Children and Young People on Digital Platforms; and the French Recommendations on the Digital Rights of Children. The European Union's General Data Protection Regulation (GDPR) underpins several of these documents. Also relevant are the OECD Recommendation on Children in the Digital Environment and Guidelines for Digital Service Providers; the Recommendation of the Committee of Ministers of the Council of Europe and the Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment; and UNICEF's Manifesto for the better governance of children's data.[14]

The not-for-profit charity 5Rights Foundation, which advocates for the rights of children in the digital world, analysed respected legislative and policy initiatives about children's data protection from different jurisdictions. They concluded that most, if not all, of the documents had these principles in common:

- Children are defined as anyone under the age of 18.
- The best interests of the child should be the primary consideration whenever children's data is handled.
- Children's data should not be used in ways shown to be detrimental to children's wellbeing.
- Data protection impact assessments are required and should particularly assess risks to children that arise from the handling of their data.
- Privacy / safety settings should be set to 'high' by default for products and services used by children, unless there is a compelling reason to do otherwise guided by the best interests of the child.
- Age assurance mechanisms should function to help protect children's rights and should be proportionate to the nature and risk of the data processing activities.
- Communication with children should be clear, concise, accurate and accessible.

- Parental controls should supplement safety-by-design, not replace it, and children should be told how and when parental controls are being used.[15]

Based on the UK Age Appropriate Design Code, the Irish Fundamentals, and the UNICEF Manifesto, we believe that the following features also have strong potential to help uphold children's rights online:

- Offering a 'floor of protection' – specifying that digital platforms can either use age verification measures which assess user age at a level appropriate to the risk of the service's handling of individuals' data or apply the highest standards of privacy and safety to all users regardless of age.

- Data minimisation – specifying that services should collect and retain only the minimum amount of personal data necessary to provide the elements of the service in which a child is actively and knowingly engaged, and that children's data should not be shared unless there is a compelling reason to do so, taking account of the best interests of the child.

- Keeping profiling options off by default unless there is a compelling reason to do otherwise, taking account of the best interests of the child.

- Meaningfully engaging children and their communities in creation of data governance protocols.

- Recognising that 'consent does not change childhood' – just because a child or a parent has consented to the child's data being handled does not mean it is acceptable for a platform to handle that data in ways detrimental to the best interests of the child.[16]

When backed by strong leadership and resourcing, regulatory frameworks can make a difference. 5Rights Foundation, who were involved in the drafting of the UK Age Appropriate Design Code, have observed that within months of its coming into effect, positive changes appeared in many digital products and services. For example, Instagram banned adults from messaging children, turned off location tracking and introduced prompts to encourage children to take breaks from scrolling, while Google made SafeSearch the default browsing mode for children, turned off YouTube's autoplay function and set YouTube default upload settings to 'private' for under-18s. Many platforms unveiled new user controls and clearer published terms.[17]

Public leadership is important here. We note the analysis of Reset Australia and ChildFund Australia that higher standards of protection for children's rights have been required by online safety codes that were drafted and led by regulators and legislators, compared to those drafted by private industry.[18]

Investing in our public regulatory bodies

Legislation and regulations are only as good as a system's ability to enforce them consistently and reasonably. We urge the committee to reflect on the capacity of our national regulators such as the eSafety Commissioner and the Office of the Information Commissioner. Even at the level of individual complaint-handling, pressure on regulators is growing. For example, in the year between 2020-21 and 2021-22, eSafety received a 65% increase in reports of child cyber bullying and a 55% increase in reports of image-based abuse.[19]

Moreover, these regulators are negotiating with large international digital platforms with immense wealth and lobbying power. This poses challenges for regulators – for example, legislation may allow for digital platforms to be fined for certain practices, but regulators still need the resources to pursue these cases, especially if platforms decide to contest them.

In their manifesto for the better governance of children's data, UNICEF specify the importance of allocating sufficient financial and human resources to ensure data protection authorities have expertise in children's rights and that children's rights are incorporated into data governance regimes. They commented, 'In order to be effective, DPAs (Data Protection Authorities) must have the capacity to litigate, impose fines and other sanctions on lawbreakers, and a mandate to provide remedies to children whose rights have been breached.'[20]

Also relevant are the remarks of the Consumer Policy Research Centre about digital products and services: 'For legislation to be effective, it needs to be supported by regular surveillance and enforcement by the regulator to educate and shift the market towards a more consumer-centric approach to the digital economy. Australia needs a well-resourced regulator with the capacity and capability to audit and enforce breaches in the complex digital environment.'[21]

We would add that regulators also need access to high-quality, up-to-date information about new and emerging developments in digital technology and how these developments – and the relevant laws and regulations – may be impacting on children. Again, we note UNICEF's manifesto for the better governance of children's data, which specifies the need to bridge knowledge gaps about data governance so that regulations have a rigorous evidence base.[22]

We greatly appreciate the research led by eSafety into young Australians' experiences online, such as their recent 'Mind the Gap' report. Ideally, we would like to see further resources in place to enable things like regular, large-scale, ongoing research to track and analyse changes over time. Examples from overseas include the annual Cybersurvey conducted in the UK, led by partners at the University of Kingston and Youthworks Consulting, which has surveyed more than 53,000 school students since 2008, and the Cyberbullying Research Centre in the US, which has surveyed more than 30,000 students since 2002.[23]

We believe resourcing such regular research would help to generate reliable answers to the question posed in the inquiry's issues paper: 'How effective is the current legislative framework in protecting children and preventing online harm from occurring?'

Preparing for the 'metaverse' and its impacts on children

The inquiry's issues paper asks 'Given the currently ambiguous status of the Metaverse and its development, is it necessary to begin regulating it now, or should authorities wait in order to understand better how it will function?'

We believe it is important for legislators and regulators to be on the 'front foot' with regard to new digital technologies. Many decision-makers took years to respond to developments like social media and smartphones; arguably this delay contributed to the many concerns that exist nowadays in relation to children's use of technology.

The future shape and function of the 'metaverse' is uncertain. However, more broadly we must assume that new digital technologies will continue to emerge and evolve and that they will be embedded ever more deeply in the lives of Australians. Therefore, it is important to keep:

- building knowledge of the issues proactively and on an ongoing basis amongst relevant regulators, legislators and policy-makers

- ensuring that regulatory structures and laws introduced to uphold children's rights online are crafted in such a way as to be adaptive to new and emerging technologies.

To this end, we suggest some further clarification of the issues raised in the inquiry's issues paper. The issues paper defines the 'metaverse' in terms of virtual reality, where users can interact with a computer-generated environment and other users in 3D – a parallel life via avatars. Potential threats of the metaverse identified in the issues paper concern addiction and mental health; privacy and data security; currency and digital payments; and law and jurisdiction.

We concur that these are valid concerns but suggest there are other possible ramifications of new technologies not recognised in the issues paper.

There is no single, accepted definition of the 'metaverse' – indeed, many stakeholders don't use the term, preferring other framings such as 'immersive technologies' or 'extended reality'. As a generalisation, these technologies are understood to have the following features:

- Realistic – 3D virtual environments which participants perceive as lifelike
- Immersive – the participant feels partly or fully immersed in this space
- Interactive – participants interact with their surroundings and other participants, engage in transactions, and create content
- Interoperable or integrated – participants travel (fairly) seamlessly between virtual spaces, taking their virtual assets with them
- 24/7 – digital spaces exist in real time and are 'always on'
- Virtual economy – a digital economy powers the metaverse, with blockchain and cryptocurrencies enabling trade and purchase of digital items.[24]

Powerful stakeholders have invested significantly in the metaverse. Corporations, venture capital, and private equity invested more than $120 billion in the first five months of 2022 alone.[25] According to Statista, the global metaverse market was worth US$38.85 billion in 2021.[26] The current foundation for investment resembles that of social media: tracking individuals in order to target advertising and sell goods to them with maximum precision and effectiveness, with the profit motive prioritised.[27]

Virtual reality (VR) has been the focus of most investment to date.[28] However, many commentators predict that augmented reality (AR) and/or mixed reality (MR) technologies will become more common ultimately. AR overlays digital information in real-world settings, while MR enables people to interact with computer-generated images in the real world in real time.[29] Through AR and MR, participants connect with virtual environments while still being consciously present in the real world. Analogies have been drawn to texting, social media and mobile games – these activities became popular partly because they are easy and low-intensity and don't require individuals to distance completely from their real-world surroundings.[30]

It seems likely that gaming will be the first space to really embrace more immersive technologies and 'extended reality'. It's predicted that, over the next decade, such technologies will also become prominent in some areas of entertainment, remote working, education and training, exercise, shopping, telehealth, tourism, and product modelling[31] – and, very possibly, online pornography.

There are many uncertainties here – eg. the nature of the technologies; their prevalence, interoperability and integration into daily life; market leadership and competition; and supply of products and energy.[32]

More pertinent to this inquiry are questioned raised about governance and regulation, including in relation to:

- threats to privacy and security as technologies gather, use and share personal data in precise and invasive ways – eg. eye-tracking, voice recording, measurement of movements and heart rate
- use of metaverse technologies by authoritarian governments and extremist/terrorist groups
- criminal and anti-social behaviours such as grooming, sexual abuse, bullying, discrimination, threats, defamation, identity theft, assault, cyber-attacks and scams
- spread of dis/misinformation in intensive and targeted ways
- harm to participants' wellbeing – eg. loneliness, disassociation, desensitisation, dysregulated behaviours, body image problems, and social and political polarisation.[33]

Consequently, ethical and governance standards will be important, including 'safety by design', relevant online safety legislation and regulation, and 'fast-tracking' the digital literacy of leaders inside and outside of government so that they can make timely, well-informed decisions.[34]

We would welcome the opportunity to discuss any of these matters further. Please contact:

Dr Jessie Mitchell, Manager, Advocacy
jessie.mitchell@amf.org.au

Sarah Davies AM, CEO
sarah.davies@amf.org.au

Ariana Kurzeme, Director, Policy & Prevention
ariana.kurzeme@amf.org.au

---

[1] A. Graham and P. Sahlberg, 'Growing Up Digital Australia: Phase 2 technical report,' Gonski Institute for Education, UNSW, Sydney, 2021, https://www.gie.unsw.edu.au/growing-digital-australia-phase-2-results
[2] P. Rioseco and S. Vassallo, 'Adolescents online (Growing Up in Australia Snapshot Series – Issue 5)', Melbourne, Australian Institute of Family Studies, 2021, https://growingupinaustralia.gov.au/research-findings/snapshots/adolescents-online
[3] Australian Competition and Consumer Commission (ACCC), 'Digital Platforms Inquiry: final report', June 2019, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf
[4] Consumer Policy Research Centre, 'Submission to the ACCC on the Digital Platform Services Inquiry on updating consumer law for digital platform services – Discussion Paper,' 13 April 2022, https://cprc.org.au/wp-content/uploads/2022/04/CPRC-Submission-ACCC-Digital-Platforms-Inquiry-Discussion-Paper-Digital-Platform-Services-April-2022-1.pdf
[5] ACCC, Digital Platforms Inquiry: final report, June 2019; Agatha Court, Bill Browne, 'Devil in the detail: privacy and some popular digital platforms,' Australia Institute, Centre for Responsible Technology, 2020; Essential Research (prepared for the Australia Institute), 'The Essential Report: Data Attitudes,' 2019, https://australiainstitute.org.au/wp-content/uploads/2020/12/Essential-Report-tech.pdf
[6] Tiffani Apps, Karley Beckman, Sarah K. Howard, 'Edtech is treating students like products. Here's how we can protect children's digital rights,' The Conversation, 10 June 2022, https://theconversation.com/edtech-is-treating-students-like-products-heres-how-we-can-protect-childrens-digital-rights-184312

[7] See for example Alison Hung, 'Keeping consumers in the dark: addressing "nagging" concerns and injury,' *Columbia Law Review*, vol.121, issue 8, Dec 2021; Jenny Radesky, MD; Alexis Hiniker, PhD; Caroline McLaren, BS; Eliz Akgun, BA; Alexandria Schaller, BA; Heidi M. Weeks, PhD; Scott Campbell, PhD; Ashley N. Gearhardt, PhD, 'Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children,' *JAMA Network Open*, 5(6), 2022

[8] Consumer Policy Research Centre, 'Duped by design: Manipulative online design: Dark patterns in Australia,' 2022, https://cprc.org.au/dupedbydesign/ ; Consumer Policy Research Centre, 'Submission to the ACCC on the Digital Platforms Services Inquiry on social media services - issues paper,' 15 September 2022, https://cprc.org.au/wp-content/uploads/2022/10/CPRC-Submission-ACCC-Digital-Platforms-Services-Inquiry-Social-media-Issues-Paper-September-2022.pdf

[9] See for example: 5Rights Foundation, 'Risky By Design', https://www.riskyby.design/ ; eSafety, 'Recommender systems and algorithms: position statement,' 2022, https://www.esafety.gov.au/industry/tech-trends-and-challenges ; Eric Osika, 'The negative effects of new screens on the cognitive functions of young children require new recommendations,' *Italian Journal of Pediatrics*, vol.47, 2021

[10] See for example: 5Rights Foundation, 'Risky By Design'; eSafety, 'Recommender systems and algorithms: position statement'

[11] Monika Mandl and Alexander Felfernig, 'Status Quo Bias in Configuration Systems,' Institute for Software Technology, Graz University of Technology, Conference: Modern Approaches in Applied Intelligence - 24th International Conference on Industrial Engineering and Other Applications of Applied Intelligent Systems, 2011

[12] For more, see 5Rights Foundation, 'Risky By Design'; Data Protection Commission, Ireland, 'Fundamentals for a Child-Oriented Approach to Data Processing,' 2021, https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf; eSafety, 'Recommender systems and algorithms'

[13] Centre of Excellence for the Digital Child, 'New partnership tackles children's privacy and digital rights,' 7 July 2022, https://www.digitalchild.org.au/news/new-partnership-tackles-childrens-privacy-and-digital-rights/

[14] For more info, see 5Rights Foundation, 'Approaches to children's data protection - a comparative international mapping,' October 2022, https://5rightsfoundation.com/Approaches-to-Childrens-Data-Protection---.pdf ;Matko Gustin, 'Challenges of protecting children's rights in the digital environment,' *EU and Comparative Law Issues and Challenges Series, Osijek*, vol.6, 2022; UNICEF, 'The case for better governance of children's data: a manifesto,' https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf

[15] 5Rights Foundation, 'Approaches to children's data protection - a comparative international mapping'

[16] Data Protection Commission, Ireland, 'Fundamentals for a Child-Oriented Approach to Data Processing,' 2021; Information Commissioner's Office (UK), 'Age appropriate design code', https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/ ; UNICEF, 'The case for better governance of children's data: a manifesto'

[17] 5Rights Foundation, 'Approaches to children's data protection - a comparative international mapping'; 5Rights Foundation, '5Rights celebrates the first anniversary of the Age Appropriate Design Code', 2022 https://5rightsfoundation.com/in-action/5rights-celebrates-the-first-anniversary-of-the-age-appropriate-design-code.html

[18] Dr Rys Farthing, Reset Australia & ChildFund Australia, 'How outdated approaches to regulation harm children and young people and why Australia urgently needs to pivot', Dec 2022, https://au.reset.tech/uploads/report_-co-regulation-fails-young-people-final-151222.pdf

[19] eSafety, *Annual Report 2021-22* https://www.esafety.gov.au/about-us/corporate-documents/annual-reports

[20] UNICEF, 'The case for better governance of children's data: a manifesto'

[21] Consumer Policy Research Centre, 'Duped by design: Manipulative online design'

[22] UNICEF, 'The case for better governance of children's data: a manifesto'

[23] Justin Patchin, 'Summary of our cyberbullying research (2007-201)', https://cyberbullying.org/summary-of-our-cyberbullying-research ; Youthworks, 'The cybersurvey 2023,' https://www.thecybersurvey.co.uk/

[24] Janna Anderson and Lee Rainie, The Metaverse in 2040, Pew Research Centre, 2022, https://www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040/ ; Deloitte, 'A whole new world? Exploring the metaverse and what it could mean for you,' April 2022, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-ai-institute-what-is-the-metaverse-new.pdf ; Deloitte China, 'The metaverse overview: vision, technology, and tactics,' May 2022, https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/metaverse-report.html ; Joel S Elson, Austin C Doctor, Sam Hunter, 'The metaverse offers a future full of potential – for terrorists and extremists, too,' 8 January 2022 https://theconversation.com/the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too-173622 ; Eric Hazan, Greg Kelly, Hamza Khan, Dennis Spillecke, Lareina Yee, 'Marketing in the metaverse: An opportunity for innovation and experimentation,' McKinsey Quarterly, May 2022, https://www.mckinsey.com/business-functions/growth-marketing-and-sales/our-insights/marketing-in-the-metaverse-an-opportunity-for-innovation-and-experimentation ; Adrian Ma, 'What is the metaverse, and what can we do there?', 23 May 2022 https://theconversation.com/what-is-the-metaverse-and-what-can-we-do-there-179200 ; McKinset & Company, Value Creation in the Metaverse, June 2022, https://www.mckinsey.com/business-functions/growth-marketing-and-sales/our-insights/value-creation-in-the-metaverse; Rabindra Ratan and Yiming Lei, 'What is the metaverse? 2 media and information experts explain,' 12 Aug 2021 https://theconversation.com/what-is-the-metaverse-2-media-and-information-experts-explain-165731 ; Responsible Metaverse Alliance, https://responsiblemetaverse.org/

[25] McKinset & Company, 'Value Creation in the Metaverse', June 2022, https://www.mckinsey.com/business-functions/growth-marketing-and-sales/our-insights/value-creation-in-the-metaverse

[26] Responsible Metaverse Alliance

[27] Tom Boellstorff, 'How we describe the metaverse makes a difference – today's words could shape tomorrow's reality and who benefits from it,' 15 June 2022, https://theconversation.com/how-we-describe-the-metaverse-makes-a-difference-todays-words-could-shape-tomorrows-reality-and-who-benefits-from-it-182819 ; KPMG, 'The Future of Extended Reality: 10 predictions, 15 experts,' Australia, 2022, https://assets.kpmg/content/dam/kpmg/au/pdf/2022/future-of-XR-white-paper.pdf; Randall Mayes, 'The Metaverse: Science Fiction or Reality?,' 14 July 2022, https://quillette.com/2022/07/14/the-metaverse-science-fiction-or-reality/

[28] Deloitte China, 'Metaverse report - Future is here: Global XR industry insight,' March 2022, https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology-media-telecommunications/deloitte-cn-tmt-metaverse-report-en-220321.pdf

[29] Anderson and Rainie, 'The Metaverse in 2040'

[30] Anderson and Rainie, 'The Metaverse in 2040' ; Ma, 'What is the metaverse, and what can we do there?'

[31] Deloitte, 'A whole new world? Exploring the metaverse and what it could mean for you,'; McKinset & Company, 'Value Creation in the Metaverse'

[32] Anderson and Rainie, 'The Metaverse in 2040' ; Deloitte, 'A whole new world? Exploring the metaverse and what it could mean for you'; Deloitte China, 'The metaverse overview: vision, technology, and tactics'; Julie Inman Grant, eSafety Commissioner, 'Will the peril outweigh the promise of the Metaverse?' 21 July 2022 https://www.esafety.gov.au/newsroom/blogs/will-peril-outweigh-promise-metaverse; Institution of Engineering and Technology, 'Safeguarding the metaverse,' UK, 2022 https://www.theiet.org/media/9836/safeguarding-the-metaverse.pdf; Ma, 'What is the metaverse, and what can we do there?'; McKinset & Company, 'Value Creation in the Metaverse'; Piper Sandler, 'Taking Stock with Teens: 21+ years of researching U.S. Teens GenZ Insights', 2022 https://www.pipersandler.com/private/pdf/TSWT_Spring_2022_Full_Report.pdf

[33] Anderson and Rainie, 'The Metaverse in 2040'; Deloitte, 'A whole new world? Exploring the metaverse and what it could mean for you'; Institution of Engineering and Technology, 'Safeguarding the metaverse'; KPMG, 'The Future of Extended Reality: 10 predictions, 15 experts,' Australia, 2022, https://assets.kpmg/content/dam/kpmg/au/pdf/2022/future-of-XR-white-paper.pdf; Pin Lean Lau, 'The metaverse: three legal issues we need to address,' 2 February 2022, https://theconversation.com/the-metaverse-three-legal-issues-we-need-to-address-175891; Cathy Li and Farah Lalani, World Economic Forum, 'How to address digital safety in the metaverse,' 14 Jan 2022, https://www.weforum.org/agenda/2022/01/metaverse-risks-challenges-digital-safety/ ;Joao Marinotti, 'Can you truly own anything in the metaverse? A law professor explains how blockchains and NFTs don't protect virtual property,' 21 April 2022 https://theconversation.com/can-you-truly-own-anything-in-the-metaverse-a-law-professor-explains-how-blockchains-and-nfts-dont-protect-virtual-property-179067; McKinset & Company, 'Value Creation in the Metaverse'

[34] Institution of Engineering and Technology, 'Safeguarding the metaverse'