

Can the consent model improve the digital world, especially for young people?

Executive summary

This briefing paper emerges from an expert roundtable discussion about the capacity of the consent model to improve the digital world. It was prompted by discussions emerging from the Privacy Act Review, and international policy moves towards using ‘consent mechanisms’ to deny young people’s access to social media.

It explored both the principles of the consent model, and its operationalisation. It notes that the current consent model has systemic issues when applied to children, outlining that:

- ‘Consent’—when deployed by services that are essential for children—could be an abuse of power, and this warrants stronger obligations on digital platforms
- Defining an ‘age of capacity’ may distract focus from fair terms
- Privacy protections should place responsibility on platforms to ensure fair practices, and be proportionate and risk-based

A rights based approach to ‘consent’ may be more appropriate for children, where young people’s best interests are prioritised and to ensure that youth participation informs what consent looks like.

It also noted that the current consent model is operationalised in problematic ways, for all users. Specifically, the current ‘click here to consent’ model is not fit for purpose. More robust consent requirements are needed. Alternative dynamic consent or automated processes may have a role to play, but it is unclear how these could operate and what their impact may be.

These insights are relevant for the ongoing review of the *Privacy Act*, and we recommend:

1. A greater emphasis is placed on the fair and reasonable test, and ensuring a child’s best interests is a key principle in establishing fairness.
2. Engaging children and young people in the process.
3. Exploring how the application of the National Principles for Child Safe Organisations could reframe obligations around privacy and consent
4. Commissioning a targeted review into mechanisms that could improve informed consent, including dynamic consent and automated consent processes.

Beyond the review of the *Privacy Act*, the Government is also considering the Office of the eSafety Commissioner’s *Roadmap to Age Verification*. Here, the principle of proportionality needs to inform considerations about age estimation and verification, including a risk based approach.

Contents

Introduction	1
Provocations: Questions about consent	2
Discussions: Improving consent in the digital world	5
Policy recommendations	9
Conclusions	10

Introduction

The policy briefing summarises discussions held at a roundtable of 18 policy experts with backgrounds ranging from law to privacy to children’s rights, including a young, lived-experience expert. The event was held under Chatham House rules, and this briefing paper presents an overview of the discussion. This summary provides recommendations to diversify data protection away from being overly consent-driven.

The roundtable was prompted by domestic and international policy debates surrounding the role, capacity and efficacy of consent to improve the digital world for users, particularly children. The strengths and weaknesses of the consent model is an active policy consideration, both domestically and internationally. Proposals noted in the Australian *Privacy Act Review*,¹ around the role of user consent—and for younger users, parental consent—are being explored in Australia. In Utah² in the US, the consent model is being deployed as a way to prevent young people accessing social media, with similar moves in Arkansas³ and other states.

Against this backdrop, Reset.Tech Australia convened experts to explore the capacities and limitations of a consent-driven data protection model and its ability to effectively improve the digital experience for all people in Australia.

This roundtable also drew on research undertaken over 2022 and 2023 by Reset.Tech around young people’s perceptions of privacy and trust in digital technology. One of the participants from this study joined the roundtable discussion.

Three key questions around the capacity of consent provoked the discussion, and three key themes emerged from the discussion. Both are unpacked overleaf.

Reset.Tech Australia is an independent, non-partisan policy initiative committed to driving public policy advocacy, research, and civic engagement to strengthen our democracy within the context of technology. We are the Australian affiliate of Reset, a global initiative working to counter digital threats to democracy.

The research into young people’s perceptions of privacy and trust in digital technology was funded by the Internet Society Foundation.

¹ Attorney General’s Department (2023) *Privacy Act Review Report*

<https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report>

² Jess Weatherbed (2023) ‘Utah governor signs new laws requiring parental consent for under-18s to use social media’ in *The Verge*

<https://www.theverge.com/2023/3/24/23654719/utah-social-media-bill-law-minors-age-verification-tiktok-instagram>

³ Brian Bashard (2023) ‘Arkansas Requiring Parental Permission For Kids To Use Social Media—Joining Utah’ *Forbes*

<https://www.forbes.com/sites/brianbushard/2023/04/12/arkansas-requiring-parental-permission-for-kids-to-use-social-media-joining-utah/>

Provocations: Questions about consent

1. Consent vs. Fair Terms, what works?

In most ordinary transactions, including the exchange of data for services in the online world, there is a profound inequality of bargaining power. This means terms and conditions, including for privacy, are imposed not negotiated. This reality of market power should not be a reason for subjecting young people to unfair and overreaching data collection practices that may impact profoundly on their future flourishing.

Both privacy and contract law contemplate age-based approaches to consent. But modern consumer protection law goes further and protects contracting parties against unfair terms despite the appearance of consent. Reforms to the *Privacy Act* propose a comparable requirement of subjective fairness in the requirement of fair and reasonable processing (proposal 12.1), having regard to the best interests of the child.

Requirements for substantive fairness in the data for service exchange might recognise two factors. Firstly, young people's agency in their online dealings, proportionate to their capacity and understanding. (Noting that 'understanding' is a crude form of protection and in most cases all people, not just children, do not understand the privacy implications of online interactions). Secondly, young people's rights not to be subject to unfair practices that would be contrary to their best interests including as to their future flourishing.

The Privacy Act Review proposes an individualised approach to assessing consent, with a back up presumption that children under 15 do not have the capacity to consent (proposal 16.2).

- Age based approaches to consent acts as a *bright line rule*. Bright line rules are clear but risk being problems with being under and over inclusive. Over inclusion potentially denies young people's agency in decisions that are important to them (e.g. health information, freedom of expression), while underinclusion can lead to 'trivialised' gaming (e.g. seeking 'tick-a-box' parental consent).
- The law of contract also adapts a bright line rule for children and young people entering contracts. At common law, contracts are not binding on young people under the age of 18. Importantly, a person under 18 can enter into a contract. However, in most instances the contract cannot be enforced against the young person, other than for contracts for 'necessaries', and even here only a fair price is usually payable.
- The 'capacity rule' in contract can be criticised as out of date with modern sensibilities and human rights frameworks as it adopts a rigid idea of children's capacity to make decisions. But there is a key insight; that young people lack experience in contracting and, in most ordinary contracts, there is a profound inequality of bargaining power which means the terms are imposed and not freely negotiated. This inexperience and inequality should not be reasons for subjecting young people to unfair terms that overreach.
- Modern statutory consumer protection regimes show a deep concern with overreaching terms and a willingness to apply a protective stance to not only young people but all contracting parties. This is done by reference to a normative standard rather than a static rule. Terms should not be unfair regardless of the appearance of consent.
- Suggestions for a fair and reasonable data processing requirement in the *Privacy Act* respond to similar concerns, and may resonate with young people. These recommend that the collection, use and disclosure of personal data must be fair and reasonable.
- Consent can only do so much in the multiple online interactions children and young people may undertake. Consent makes the consumer responsible for assessing whether the transaction promotes their overall wellbeing. Responsibility for fair dealing should also be placed on the entity collecting the data.

2. Agency or deficiency for children?

From a children’s rights perspective, the Privacy Act Review’s proposal that assumes that only those over 15 years old have the capacity to consent is problematic for two reasons: it reflects “capacity scepticism”, and; it impairs children and young people’s ability to enjoy their rights in an online environment.

Under the Australian Privacy Principles Guidelines, if it is not practical or reasonable to assess the capacity of an under 18-year-old to consent, then age-based presumptions apply. This is a presumption of capacity for those over 15 years old, and a presumption of incapacity for those under the age of 15. Proposal 16.2 of the Privacy Act Review Report would see these presumptions continue in the reformed *Privacy Act*. This raises a number of issues:

- The age-based presumptions of capacity and incapacity reinforce the persistent difficulties that children and young people experience in being recognised as having and exercising various rights, including their privacy rights. This is a reflection of ongoing age based prejudice and the power imbalances that adultism both reflects and reproduces.
- These presumptions inform ideas about the vulnerability of children, which is directly referred to in the Privacy Act Review. (E.g. chapter 16 refers to children’s particular ‘vulnerability’ to online privacy harms). A protective narrative of ‘harm’ and ‘risk’ is deployed to justify the age of 15 years as a threshold for presuming capacity.
- It is important not to define children exclusively by reference to their vulnerabilities in their online interactions, because it results in an “overly protectionist agenda”⁴ in privacy law and policy that reinforces assumptions about children’s lack of capacity to protect their own interests. This fails to recognise children’s evolving capacities and agency.
- The *Privacy Act* approaches the question of capacity as a binary: either a child has or does not have capacity to give consent to data processing. This does not appreciate that children’s various capacities—cognitive, emotional, social, cultural & physical—don’t develop in a linear way with age. As their various capacities evolve, so do children’s knowledge and understanding of their rights and how to make good decisions for themselves.
- It doesn’t even allow for the possibility that children and young people may have superior understanding and skills to many adults in digital settings.
- The impact of the Privacy Act Review Report proposals on children and young people’s other rights under the UN Convention on the Rights of the Child – the proposals have the potential to adversely affect other, non-privacy rights under the Convention. Protecting children and young people’s right to privacy in the online and digital environment shouldn’t come at the expense of other rights under the UNCRC.
- The Preamble to the UNCRC does recognise that childhood is a period of “special vulnerability during which children are in need of special protection” – but as the UN Committee on the Rights of the Child (2006: [14]) has explained, the substantive text of the Convention requires that children are respected as “active participant[s] in the promotion, protection and monitoring” of their privacy rights. What this means in practice is that a children’s rights-based approach to privacy reforms must be informed by several other rights under the CRC. These are:
 - Article 5, right to receive appropriate parental direction, recognising evolving capacities
 - Article 12(1), right to freely express their views in all matters affecting them
 - Article 13(1), right to freedom of expression, and;
 - Article 17, right to access information and material from a diversity of sources
- An overemphasis in the Privacy Act Review Report on ‘protecting’ children in the online and digital environment runs the significant risk of undermining these rights.

⁴ John Tobin, ‘Understanding Children’s Rights: A Vision beyond Vulnerability’ (2015) 84 *Nordic Journal of International Law* 155, 167

3. Is consent effective?

The concept of consent relies implicitly on the ability to decline. This is especially true for young people, whose lives are deeply digitally integrated. When users have no choice but to accept, there are no incentives for platforms to change their products.

The concept and practice of consent relies on the ability to decline. Many digital services used in Australia are now integrated into (or have replaced) essential services, such as EdTech⁵ in the classroom or bushfire alerts⁶ or news services.⁷ Some unavoidable social services are now digitised too, such as Centrelink payments.⁸ In these instances there is very little to no choice to decline, because doing so means no access to services that are essential to everyday life. Social media services are too often not optional, especially for young people.

Young expert's perspectives

- *"It's actually very difficult for a young person to just opt out of social media or online sources. For school as well, we use so many digital things, you always have to consent to the cookies. Opting in isn't really a choice anymore."*
- *"We all kind of depend on it, news, education, communication, or just for socialising with friends. If you're not on social media, you feel quite excluded from other people. Sports teams, clubs, group work – all of these take place online [in messenger groups], mainly through social media, which is easier than getting people's phone numbers."*
- *On the topic of requiring parental consent to create a barrier to accessing digital services "Many people would want it because it's quite necessary. (They) would find some kind of like mode of like accessing it ... it wouldn't make much of a difference, I would say."*

The inability to decline raises two questions. Firstly, about the nature of consent itself; where 'opting out' is not an option, users do not freely 'consent'.⁹ Secondly, it raises questions about the effectiveness of the consent model to encourage tech companies and other service providers to make pro-consumer improvements (e.g. stronger default settings, reduced surveillance etc). No matter how low safety, privacy or other standards are, users are compelled to 'consent', creating no incentive for platforms to improve standards.

⁵ See an analysis of the EdTech products recommended in NSW and Vic during the pandemic, for example. Human Rights Watch (2022) *How dare they peep into my private life* <https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments>

⁶ For a description of how social media platforms have become a central part of rapid hazard warnings see Amisha Mehta, Scott Murray, Ryan McAndrew, Michaela Jackson, Vivienne Tippet (2022) 'Encouraging evacuation: The role of behavioural message inputs in bushfire warnings' *International Journal of Disaster Risk Reduction*, DOI: 10.1016/j.ijdr.2021.102673

⁷ See for example, the ABC's move towards a digital first organisation, for example. ABC (2022) *ABC Archives Proposal for Change* <https://about.abc.net.au/statements/abc-archives-proposal-for-change/>

⁸ Sometimes called Alogracy, and often critiqued. (See for example, the critiques that emerged when the Robodebt scandal emerged. Rebecca Turner (2021) 'Robodebt condemned as a 'shameful chapter' in withering assessment by federal court judge' *ABC News* <https://www.abc.net.au/news/2021-06-11/robodebt-condemned-by-federal-court-judge-as-shameful-chapter/100207674>). It is worth noting that digitisation often comes hand in hand with elements of privatisation, adding layers of complexity to the issue. See an analysis of the effect of digitisation and privatisation of social services in Denmark for example. Rosie Collington (2022) *Disrupting the Welfare State? Digitalisation and the Retrenchment of Public Sector Capacity*, *New Political Economy*, DOI: 10.1080/13563467.2021.1952559

⁹ This may violate the element of voluntariness in section B.38 of the APP Guidelines in itself

Discussions: Improving consent in the digital world

1. The current consent model has systemic issues when applied to children

‘Consent’—when deployed by services that are essential for children—could be an abuse of power, and this warrants stronger protections

- For a contract to be valid there is assumed to be a relatively equal power relationship and for contracts to be entered into voluntarily. The significant asymmetrical power relationship between young people and digital platforms makes the ‘consent’ model a form of coercion. This coercion—in principle—invalidates the contract. This raises questions about the validity of the consent sought in the digital world. There was a question raised about whether or not consent in this form is really collusion or coercion and if the language of ‘consent’ is unhelpful in these settings.
- The ‘best interests’ principle alone may not be enough to move away from this coercive misuse of power. There are practical and ethical issues around who gets to determine the best interest of the child, and a lack of youth engagement in these determinations. (And there are examples of digital platforms beginning to outline their own interpretations of this, which may be welcome but also raises questions about determining best interests).¹⁰
- In Europe, we clearly see this issue of power imbalances invalidating consent via the General Data Protection Regulation. What does that mean in the case of a young person using social media or or accessing an essential public service, then the data controller has to be able to point to another legal basis for that use. So that means that we can't place all of this weight on consent in a strictly legal sense.
- Young people are sent very confusing messages about what's expected of them in respect to consent. At the end of the day, we run right over the top of their own capacity to give consent. (For e.g. the digital world makes no provisions for meaningful consent).

Defining an ‘age of capacity’ may be a distraction

- There were questions raised around if capacity to consent matters if an agreement or contract is unfair (as explored in the first provocation). This suggests that defining an ‘age’ for consent could be seen as a secondary consideration *after* fairness
- Capacity was problematised as a concept (as explored in the second provocation, described above), but particularly when converted into bright line rules tied to an age:
 - Firstly, it rests on ageist assumptions that fail to recognise young people's capacity to make good judgements (as well as bad)
 - Secondly, the capacity to make ‘good judgements’ is not used as a criteria to evaluate the validity of any other cohort's consent. It is unclear why this test is uniquely applied to children. Instead, other protections are in place for other consumers (such as the requirement for contracts to be fair). This approach would also offer stronger protections for children
 - Thirdly, as noted it creates issues with over and under inclusion. However, fairness may be a more important framing than inclusion.

¹⁰ See for example Elaine Montgomery and Elaina Koros 2022 *Meta's Best Interests of the Child Framework* <https://www.ttclabs.net/news/metas-best-interests-of-the-child-framework>

Protections should place responsibility on platforms to ensure fair practices, and be proportionate and risk-based

- The consent model places obligations on users—be they children, parents or adults—to manage and mitigate risks associated with data processing. In general, the obligation for safe or fair or reasonable transactions (i.e. service for data) should be placed on the provider not the consumer.
- Alongside thinking about what is meaningful consent (be it dynamic or static) we need to consider what is fair and reasonable to ask for from children when it comes to data processing. More effort should be going into ensuring fair and reasonable processing, as focussing on improving consent alone could be ‘an endless rabbit hole’.
- Important to note that some online decisions have more significant consequences than others. There is value in thinking about what is fair and reasonable to ask of children in terms of this data and service exchange.
- The need for proportionate, risk based approaches were particularly apparent in the implementation of age assurance/age verification practices. There are a lot of good and problematic examples of implementation of age estimation emerging overseas that Australia should keep an eye on. This is especially relevant given Australia might be the first place to provide a comprehensive roadmap towards age verification.¹¹
- A rights based approach may provide a better pathway forward for children.

2. A rights based approach to ‘consent’ may be more appropriate for children

Participatory, rights-based approaches and consent

- A rights informed approach, informed by young people’s participation and experiences, may lead to a better model for a rights-advancing digital world, than consent.
- There is a tendency in Australia to consider young people’s experiences online through a lens of online safety, potentially reflecting Australia’s policy history. Reflecting on safety as a framing device noted that this could both open up new avenues or narrow them:
 - If we place a child in a setting and empower them to be able to talk about what it is that makes them safe and unsafe, (including in terms of data and privacy agreements) and that there’s a different way of looking at the tools that we could develop around ‘consent’ for the digital world. This has particular capacity if young people’s perspectives are understood in terms of our shared responsibility for supporting and empowering them but also being aware of what the risks and dangers are both in terms of privacy.
 - Some of the work that was done through the Child Abuse Royal Commission produced a set of standards¹² that unpacked what safety looks like for children, and recognised it as a broad community responsibility. That responsibility is shared by all organisations who have relationships with children and young people. Critically, that includes ensuring children play a role in how an organisation secures their safety. It’s unclear what this means for the consent model, but it could be helpful for understanding what consent looks like if it is built from a child-centric standpoint.
 - Exploring consent as a child safety issue might overlook other rights, such as privacy, or access. However, if we are able to frame safety broadly and ask young people what is important to them, that might reveal other policy solutions. This could be fruitful given consent is not solving the problem of the digital world not respecting rights.

¹¹Office of the eSafety Commissioner 2023 *Age Verification: Roadmap on Age Verification*
<https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification>

¹² Australian Human Rights Commission 2018 *National Principles for Child Safe Organisations*
<https://childdsafe.humanrights.gov.au/national-principles/about-national-principles>

- We strongly suspect that young people wouldn't be satisfied to only think about privacy through the online safety lens.
- Some recent research highlights what young people think is useful in respect to online safety. This suggests that there's little concern about consent on the part of young people but that privacy is a worry for them.¹³ Young people's concerns about privacy have significantly shifted from talking about interpersonal privacy such as privacy from nosy parents in particular, to privacy breaches by those with commercial interests..
- Young people also want education that moves away from focussing on 'extreme online harms' towards everyday practices that they encounter in digital spaces, such as privacy harms (like excessive data tracking). There is a strong case for developing this curriculum in a close and careful partnership with young people.¹⁴
- Research with young people suggests that online safety and seeking help only really come up when something goes wrong for them online. It's not at the forefront of many young people's minds, except when young people think about the protection of younger siblings/relatives from harm online, or in assisting younger children with navigating complaints systems.¹⁵

3. The current consent model is operationalised in problematic ways, for all users

The current 'click here to consent' model is not fit for purpose. More robust consent requirements are needed

- According to the Australian Consumer Data Right, and aligned with GDPR, consent must be "freely given, specific, informed and unambiguous". In order to obtain freely given consent, it must be given on a voluntary basis. It should not be bundled and can be withdrawn. Recommendation 11.1 of the Privacy Act Review would adopt a GDPR like standard for consent, voluntary, informed, current, specific and unambiguous. If effectively enforced, this should help address some of the shortcomings of the current consent model.

Alternative dynamic consent processes may have a role to play, but it is unclear how these could operate and what their impact may be

- 'Dynamic consent' processes—where users are engaged in an ongoing fashion around their consent—seek to give people a more nuanced opportunity to signal their acceptance of particular types of data collection or use. They aim to temper the power imbalance between digital platforms and their users. This approach would constrain consent within a set of different *specific* parameters. This would also allow users to interact with a specific set of consent requirements, but to do so in a way that could manage consents from a variety of digital platforms and allow users to revoke consent easily. This could be seen as a 'public good'.

¹³ Linda Marsden, Lilly Moody, Betty Nguyen, Lilly Tatam, Louisa Welland, Professor Amanda Third (2022) *Reimagining online safety education through the eyes of young people: co-design workshops with young people to inform digital learning experiences*. Young and Resilient Research Centre, Western Sydney University <https://doi.org/10.26183/3bz3-r451>

¹⁴ Ibid.

¹⁵ Faith Gordon (2021) *Online Harms Experienced by Children and Young People: Acceptable Use and Regulation*

- There have been examples of this in health research where users have been able to use a single consent platform online to consent in a rather more nuanced way than just being in or out, with the ability to change consent preferences over time.
- If dynamic consent processes were developed, they would need to sit on an independent platform with mandated interoperability for organisations that seek consent.
- There was support for this from a young person's perspective *"I do believe having a flexible contract of consent is important for young people where they should be able to opt into specific elements of data collection. However this should be a simple and clear process that does not confuse children such as ticking specific boxes."*
- But it is unclear what the actual effects of dynamic consent platforms are in practice, limited research suggests this approach works in practice.¹⁶ Research suggests that users of dynamic consent platforms don't actually change their preferences often. More research and data would be needed to support the use of dynamic consent platforms. It's a waste of time and resources to create a great dynamic consent platform if nobody looks at it or uses it to change their preferences, or withdraw consent.
- Users struggle to engage with privacy policies and collection notices as they are. Requiring users to do *more* may be unrealistic, especially for young people.¹⁷ As the young representative put it *"for most young people when they go onto a social platform, and they have to like do the terms and conditions and consent, they're not necessarily like, reading much of it. And it's usually just like, click accept"*.
- Some studies in the field of computer science find that users most often just default to what's asked of them.¹⁸
- However, this may be because we do not have a digital environment that has fostered a culture of 'active participation in consent'. It remains to be seen if dynamic consent processes could be effective.

There may be a role for technology in reducing the 'consent' burden on consumers

- Machine learning/semi-autonomous models of consent to reduce the burden on the consumer re dynamic consent.
- There may be benefits to 'machine-consumable' privacy policies, because people could decide ex ante the terms on which they are prepared to share their data and then find 'matching' services via search tools.

¹⁶ See for example, Megan Prictor Megan Lewis, Ainsley Newson, Mathilda Haas, Sachiko Baba, Hannah Kim, Minori Kokado, Jusaku Minari, Fruzsina Molnár-Gábor, Beverly Yamamoto, Jane Kaye, Harriet Teare (2020) 'Dynamic Consent: An Evaluation and Reporting Framework'. *J Empir Res Hum Res Ethics* 5(3):175-186. doi: 10.1177/1556264619887073

¹⁷ For example, polling found that only 4% of Australian 16 & 17 year olds always read the terms and conditions of social media platforms. (See Reset.Tech Australia (2022) *Did we really consent to this?* <https://au.reset.tech/news/did-we-really-consent-to-this-terms-and-conditions-young-people-s-data/>)

¹⁸ For example Jonathan Obar & Anne Oeldorf-Hirsch (2020) 'The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services.' *Information, Communication & Society* 23.1 (2020): 128-147.

Policy recommendations

The *Privacy Act* 1988 is currently subject to an ongoing review by the Attorney-General's Department. While this briefing broadly explores the capacity of consent to improve the digital world for young people, these insights are also directly relevant to this policy discussion. Specifically, some of the shortcomings of relying on consent could be addressed within the *Privacy Act* review to result in greater data agency, autonomy and control. Reset.Tech Australia recommend these include:

1. **Placing a greater emphasis on the fair and reasonable test, and ensuring a child's best interests is a key principle in establishing fairness.** The shortcomings of an over-reliance on consent within data collection and processing can be mitigated via a greater focus on fair and reasonable tests within the *Privacy Act*. For example, rather than being asked to consent to excessive data collection, products should have to reconsider excessive data collection because it is unfair and unreasonable in the first instance. This would shift the burden of responsibility from young people (and parents) to consent or decline data exchange, onto digital platforms to ensure fair data processing in the first instance. Realising this may require clear guidance and strong enforcement from the OIAC.
2. **Engaging children and young people.** Ensuring that children's rights are respected in the process of reviewing the *Privacy Act*, and realising the capacity of young people's engagement to improve policy outcomes requires the careful, sustained participation of children and young people. A youth steering group, or equivalent, could be established to support the Attorney General's Department in this process.
3. **Explore how the application of the National Principles for Child Safe Organisations could reframe obligations** around privacy and consent to create and support mechanisms that guide and inform decisions about consent, privacy, safety and other rights for children, particularly through ensuring a child is meaningfully engaged to understand those decisions to the full extent of their capacity and understanding.
4. **Commission a targeted review into mechanisms that could improve informed consent, including dynamic or automated consent processes.** A deeper understanding is needed about the potential of dynamic consent processes, or other automated processes that could move digital platforms towards informed consent and away from 'tick-box click-to-accept' behaviour.

Beyond the review of the *Privacy Act*, the Government is also considering the Office of the eSafety Commission's *Roadmap to Age Verification*. Considering the role of consent in this process is also important. Specifically:

5. **The principle of proportionality needs to inform considerations about age estimation and verification, including a risk based approach.** Requirements for Age Verification need to develop their own equivalent of the 'fair and reasonable' test. This involves adopting risk-based approaches that compel actors to consider the risks their services potentially pose to younger users, as well as the potential privacy risks introduced by age estimation or verification. Requirements need to ensure digital platforms embed a privacy-by-design approach that also respects children's rights.

Conclusions

Alone, the consent model will not improve the digital world for children and young people. It reflects 'capacity scepticism', can restrict young people's enjoyment of other rights, and is ineffective at incentivising improvements. The asymmetry of power between users, especially younger users, and digital platforms is too great to ensure young people are offered fair terms to consent to. Placing a stronger emphasis on ensuring fairness and reasonableness in data exchange practices may be more transformative.

Likewise, the way consent models have been implemented is problematic. The current 'click here to consent' model is not fit for purpose, and more robust consent requirements are needed. These could be more nuanced and more dynamic, but must not place additional burdens on users.

Placing a stronger emphasis on fairness, and revamping the implementation of consent processes, needs to involve imposing responsibility on platforms themselves. It cannot be up to users to manage privacy risks themselves. This could involve exploring what rights-based approaches to consent look like, and involving children and young people in the process. Re-defining consent requires prioritising fairness and ultimately children's best interests in the digital world.

This briefing paper reflects the expertise of those who contributed to the roundtable, including:

- Prof Judith Bessant, RMIT University
- Alice Dawkins, Reset.Tech
- Dr Georgina Dimopoulos, Southern Cross University
- Dr Rys Farthing, Reset.Tech & Centre for the Digital Child
- Dr Faith Gordon, ANU
- Amy Lamoin, ChildFund Australia
- John Livingstone, Australian Child Rights Taskforce
- James McDougall, Australian Child Rights Taskforce
- Dr Rob Nicholls, UNSW
- Matt Nguyen, Reset.Tech
- Prof Jeannie Paterson, University of Melbourne
- Dr Megan Prictor, University of Melbourne
- Chloe Shorten, Centre for Digital Wellbeing
- Prof Amanda Third, Western Sydney University

All errors and omissions rest with Reset.Tech Australia.