YOUNG PEOPLE AND ONLINE PRIVACY

REALISING YOUNG PEOPLE'S RIGHTS IN THE DIGITAL ENVIRONMENT

JULY 2023

With thanks to the many young people who gave their expertise and time to support this research.

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 Australian Child Rights Taskforce is a coalition of over a hundred organisations, networks and individuals committed to the protection of the rights of children and young people in Australia.

With thanks to the Internet Society Foundation for supporting this work.

EXECUTIVE SUMMARY

Young people hold nuanced and sophisticated understandings about what privacy means in a digital context.

They see online privacy as a right, but a right that is frequently and routinely violated. Despite this, online privacy is still understood as important and desirable.

Young people want to see fundamental changes to the policy landscape to ensure their rights are prioritised.

This has implications for policy makers as they review the *Privacy Act 1988*. Specifically, it lends support to proposals:

- 4.1 and 4.3; amending the definition of privacy to include metadata and inferred data like digital profiles
- 10.2 and 16.3; requiring privacy policies and collection notices to be clear and understandable, including for children
- 16.2; continuing to use current 'age of consent' guidelines
- 16.4; requiring companies to consider the best interests of children when deciding if data collection, use or disclosure is fair and reasonable
- 16.5, the introduction of a Children's Privacy Code, that covers all services likely to be accessed by children. The Code must be developed in consultation with children and young people, and address how services can function in the best interest of children
- 20.5 and 20.7; prohibiting direct marketing to a child and trading children's information
- Caveated support for 20.6; prohibiting targeting a child unless it is in their best interest. There is strong support to prohibit targeting advertising to children, but given the essential nature of digital products and services as described by young people, prohibiting all targeting would be problematic (For example. products like search engines provide target specific responses to queries). This is not incompatible however, if determinations of children's best interests consider their rights to access and to information for example.

It also has some potential learnings for the next *Online Safety Act* review too.

This report documents findings of mixed methods research undertaken with young people across Australia aged 13-18 between 2022 and 2023. It documents themes that emerged across a wide range of research activities and outputs, and prioritises the words of young people themselves as much as possible.

TABLE OF CONTENTS

1 INTRODUCTION

3 PRIVACY AS CONTROL, IN CONTEXT AND ESSENTIAL TO WELLBEING

5 PRIVACY AS AN UNREALISED RIGHT

8 PRIVACY IS NOT CONSENT

11 PRIVACY AND TRUST

14 WHAT YOUNG PEOPLE WANT TO IMPROVE THEIR PRIVACY

19 CONCLUSIONS

INTRODUCTION

Young Australians live increasingly digital lives—from online classroom teaching to connected toys to digital games to social media—growing up now happens in a digital world.

But this digital world relentlessly collects, collates and analyses data about young people, from their phone ID numbers, to GPS location to the contents of their online browsing history. Young people's data footprint is immense, and growing. Unlike any generation before, children and young people are now 'datafied' from birth.[1]

This has significant implications for young people's privacy. Under the Convention on the Rights of the Child [2] and Australia's privacy laws,[3] children have the right to be free from arbitrary interference with their privacy. These extensive data footprints may be a risk to their privacy.

This research set out with a simple aim, to explore what young people think about their online privacy, if they trust the technology that collects their data and what, if anything, they want done to improve their privacy online.

These insights are timely, in the context of the review of the *Privacy Act 1988*. We began this research before the publication of this review, but a number of relevant themes and conversations have emerged. We have noted key connections throughout this document, to help inform policy discussions.

Children and young people also have the right to be heard on matters that affect them,[4] including in policy discussions about Australia's privacy frameworks. This report is one way to help advance these rights.

These activities were supported by the Internet Society Foundation.

[1] Veronica Barassi (2020) Child | Data | Citizen MIT Press, London

[2] Article 16 UN General Assembly (1989) Convention on the Rights of the Child General Assembly resolution 44/25

[3] Privacy Act 1988 (Cth)

[4] Article 12 in the UN General Assembly (1989) Convention on the Rights of the Child General Assembly resolution 44/25

RESEARCH METHODS AND EVIDENCE

This report draws on mixed methods research from a participatory action research project. Evidence and quotes from young people are drawn from:

- A poll of 506 Australian 16 & 17 year olds, conducted in April 2022
- Repeated workshops with a core group of 12 young people aged between 14 and 17, held between September 2022 and March 2023. This included an initial full day in-person session, and two online follow up sessions, which were attended by an additional 3 young people of the same age
- Hour-long, in-depth interviews with 5 young people aged 13-18 conducted between September and October 2022, to include the voices and perspectives of young people who were unable to attend the workshops
- A youth-authored submission to a Senate Inquiry, written by a group of 8 young people who had participated in this research in February 2023
- A consultation session held between young participants in this research, and a Government Department held in March 2023
- An academic panel event held with the Centre for the Digital Child, involving 3 young panellists
- A policy roundtable event hosted by Reset.Tech involving a young expert
- A civil society panel at RightCon 2023, involving a young panellist

COMPARATIVE FINDINGS

Similar workshops and surveys were held in Antigua & Barbuda, Ghana and Slovenia, and more information is available about these online.[5] This report explores the findings from this research Australia, and expands on what this might mean for privacy policy.

[5] Information about the international research can be found at https://trustech4kids.github.io/

PRIVACY AS CONTROL, CONTEXT AND WELLBEING

Understanding how young people want their privacy improved requires understanding how young people think about privacy in an increasingly digital world.

There are many reasons young people's understandings about privacy may differ to those of previous generations. For example, Gen Z has been 'datafied' in a way that no other generation could have even imagined. Datafication—or "the process in which children's actions online are pervasively recorded, tracked, aggregated, analysed, and exploited by online services in multiple ways that include behavioural engineering, and monetisation"[6]—now defines multiple childhood experiences. For example, children are datafied in the womb with collection and harvesting of pre-natal data from parents,[7] and this continues right throughout childhood, through connected baby devices and toys[8] and in school through digital teaching tools.[9] The sheer prevalence of these privacy invasive extensive data collection and tracking practices may mean they have been somewhat normalised among young people.

The average young Australian now has never experienced a world without digital technologies that routinely track, aggregate and analyse their data to contextualise their experiences.

> **"Because a lot of us, especially in this generation, have grown up with this type of technology. Like I talked to my mum. And she's like, I remember when the internet was still a wire. And I like, for me, I had an iPad at the age of seven."**

> **"It really desensitises a lot of people (to privacy violations) because you can't really think of any other way"**

> **"And also that, it's that everybody's just got acclimatised to it (less privacy). And go 'ahh it's just an everyday thing now'."**

However, the conversations with young people held throughout the course of this research suggested that young people had nuanced and complex understandings about contemporary privacy, and were deeply aware of how the digital environment affected and often violated their privacy.

[6] Wang, G., Zhao, J., Kleek, M.V., & Shadbolt, N. (2022). 'Don't make assumptions about me!': Understanding Children's Perception of Datafication Online. Proceedings of the ACM on Human-Computer Interaction, 6, 1 - 24

[7] Barassi, V. (2020). Child | Data | Citizen. MIT Press

[8] Mascheroni, G. (2018). Researching datafied children as data citizens. Journal of Children and Media, 12:4, 517-523. DOI: 10.1080/17482798.2018.1521677

[9] Jarke, J., & Breiter, A. (2019). Editorial: the datafication of education. Learning, Media and Technology, 44, 1 - 6

> But still, it's creepy that a fridge could be recording what is happening, like your smartphone... watches that track your every move, track your activity movement, things like that. I was a really, really big fan of 1984 (the book). But it kind of comes down to 'well where's the line gonna be?'

> There's a sense of unease from people watching you."
>
> "Privacy is a right to protect and or conceal our personal information.

1. Privacy involves the ability to conceal personal information. The ability to conceal personal information was at the core of the experience of privacy for young people. This confirms with Westin's[10] traditional conceptualization of privacy as 'control over' information. The nature of the information that young people wanted to conceal varied, from more classically understood personal information like names and dates of birth, but also included data derived from a digital world like metadata tracked from apps and websites. In the Australian context, this is an important inclusion. Australia's *Privacy Act* does not necessarily protect this sort of metadata as personal data,[11] but some of the conversations we had with young people suggest that metadata is some of the most sensitive data that young people want to be able to safely conceal, especially GPS locations associated with phone IDs.

Proposals 4.1 & 4.3 of the Privacy Act Review

2. Privacy protects personal information from "others" who might want to interfere. Privacy may have been control over information, but it was also contextual.[12] Young people spoke about wanting to protect a range of different information from different actors. This included protecting some information from friends and family, other information from 'strangers', some from schools and the state, and—as discussed below—privacy from digital platforms themselves. Who young people were protecting information from was as important as what the information was.

3. Privacy creates a sense of security, safety, and wellbeing. Young people spoke about a sense of unease where they felt their privacy was invaded, but they also spoke about privacy making them feel safe and secure when it was realised.

4. Privacy as a right. Privacy was routinely described as a right, or something that young Australians should legitimately be able to expect. Again, this is important to consider in the Australian policy context. Where the *Privacy Act* is being reviewed, young people hold legitimate expectations about their privacy and expect it to be realised and advanced through legal and regulatory frameworks.

> I think what's crazy is like the Snapchat can see can see where all your friends are. I think that's so bad. Because my younger brother, right, he adds random people on Snapchat. And I'm 'do you realise they can see you, like your location is on' and he doesn't even care. That's really bad, like, actually so bad. I think that's crazy.

[10] A. Westin (1967) Privacy & Freedom New York, Athenium

[11] Following a 2017 Federal Court ruling that found that metadata is not personal data Privacy Commissioner v Telstra Corporation Ltd (2017) FCAFC 4

[12] H. Nissenbaum (2004) 'Privacy as Contextual Integrity' 79 Washington Law Review 119

PRIVACY AS AN UNREALISED RIGHT

Despite privacy being understood as a right—including and especially in a digital context—young people did not feel it was a right that was currently respected online.

Instead, privacy and the 'digital world' were often described as a direct trade off; young people felt they had to compromise their right to privacy in order to enjoy their right to access the digital world. For example, young people talked about the experience as being "basically a trade off... Your privacy for something else, or that fun for just a few, like a little bit of information". They talked about privacy never being "complete" and feeling like it was unable to be achieved online "when I use my computer my privacy will never completely be my privacy."

Nowhere was this more apparent than in the conversations among the group of young people at the workshop in western Sydney, around the use of young people's personal data to drive the delivery of targeted advertising. Targeted advertising (or 'behavioural advertising') and data use was discussed at length as the group prepared a submission to a senate inquiry. They opened their submission with an unambiguous statement: "Fundamentally, young people do not want their data used to sell them things."

However, when they went on to unpack their specific asks they did not call for a straight forward end to the practice.[13] Instead they ask for young people to be able to opt-in to targeted advertising. But this was not because they felt young people wanted a choice around targeted ads, but because they wanted to be "realistic" in their policy. The group clearly stated that they "support a ban on behavioural advertising, but we are aware it might be unpopular or difficult to implement".

The desire to be "realistic" highlighted these young people's low expectations about the level of protections they felt their privacy might actually be afforded within the Australian policy environment. In deliberations around what to ask policy makers to consider, the young people involved in this research often tempered their expectations, noting that digital platform's profits would always counterbalance their privacy.

> **"We can't expect the government to, you know, to make (digital products and services) default to 'no, you can't share my data'. ... Because like that wouldn't get passed, like no matter what. Because it's just like, it's really unrealistic for them to be able to do that and then make profit at the same time."**

[13] For comparative insights, the research groups in Antigua & Barbuda, Slovenia and Ghana all called for a straight forward end to the practice.

The young people we spoke to in this research did not appear optimistic that policy makers would advance their rights to privacy against the current business model. "It's not getting better and we don't have a lot of options."

This is not to suggest that young people felt privacy was irrelevant or unimportant. They still wanted privacy online, they just had low expectations of realising this right. As one young person put it "everything that we do is online, friends, work, schools, communicating. We shouldn't have to feel like we're trading off our privacy when we're just trying to stay connected". When we asked young people about the possibility of a better, more privacy realising digital environment they expressed a strong desire, "that would be awesome, to go online and know my privacy will be mine". But they remained sceptical about their prospects, "I'd love an alternative, but there really isn't". As another put it, "if there was somehow a middle, where you could have a decent amount of risk (privacy risks online) and a decent amount of fun, that would be cool".

This is particularly pertinent in the context of the review of the *Privacy Act 1988*. Beyond the more straightforward proposal to prohibit targeted advertising for under 18 year olds—demonstrating that it might indeed be a realistic ask—it shows the clear need for the introduction of the best interests principle for young people. Young people currently do not believe that their right to privacy, which is in their best interest, is prioritised or adequately considered in the data processing practices of the digital world.

Proposal 20.5 of the Privacy Act Review

Proposal 16.4 and 16.5 of the Privacy Act Review

Proposals 20.5, 20.6 & 20.7 of the Privacy Act Review

Young people described multiple common-place experiences where they felt their privacy was not realised in a digital world, which may contextualise their low expectations. These included:

1. Experiencing targeted advertising as violation of privacy

- *"I just feel as if they are storing my data for ulterior reasons, primarily ads"*
- *"I understand where some young people's frustrations may lie, because I guess when you do see an ad that it's targeted to you, kind of like consciously realise that our data is being taken. Where usually when you're using social media, you don't actually realise it. But it kind of is, kind of strange. It's kind of like scary almost to do that. Like your phone is listening to you or the internet is like listening to you. So it can be like frustrating in that sense"*
- *"Not just (big) advertisers, but any companies. Even not for profits will get up in your face sometimes. It's unnecessary. Advertising can be really in your face. It's not looking after young people. It's not the best thing for young people"*
- *"It's pretty bad that people can just pay and have stuff shown to minors. I understand some stuff, like councils (and ads for public interest stuff). But overall, it's hard to pick and choose, for companies. So you shouldn't be able to"*

2. Experiencing hacking, including hacking social media accounts, as a violation of privacy

- *"(I don't trust digital platforms) because hacking is very easy on social media apps and people could get my info such as bank details"*
- *"I have some of my friends and I know 110%, they put everything online, they don't even worry about it. And they just trust and they trust that process, because that's what they've grown up with. That's what they understand. That's what they know. Whereas I had another one of my friends who was incredibly trusting with their privacy online, and then got hacked on their Instagram account. And now doesn't trust putting anything out there"*
- (I think we'll have less privacy in the future) *"Reason why is because it's putting more things in hackers, start to come in, usually just to hack through because more and more technologies connected to each different device"*

3. Experiencing the business model of digital platforms itself as oppositional to their privacy

- *"They are in it for the business of making money they don't care about the individual"*
- *"Because big companies only care about money and will do anything to get more money, including disrespecting privacy"*
- *"It's possible it's all being sold no matter what I do"*
- *"I know that they do not care about me as the individual. They want money"*

4. A lack of transparency about data processing practices also detracted for a sense of privacy

- *"Well I don't read the terms and conditions because they are too long so I don't know what they are doing with my info"*
- This was especially true for data breaches, *"We want to find out if we're in a data breach", "We get told an unacceptable time after it happens. We should be told immediately"*

PRIVACY IS NOT CONSENT

Consent around data collection and use emerged as a hot topic of discussion throughout this research. While consent is often used as a way to justify data processing in the digital world—and therefore the associated, frequent privacy violations that young people experience in the online world—the concept of consent did not match these young people's experience of using the digital world.

As the young people involved in this research explained, to offer meaningful consent you need to be able to meaningfully decline. But this was not the case for Australian young people. Young people's lives are deeply digitally integrated in ways that cannot be declined. For example, many digital platforms are now integrated into, or have replaced, essential services, such as educational tools used at school,[14] to bushfire alerts [15] or news services.[16] In these instances there is very little to no choice to decline, because doing so means removing access to services that are now essential to everyday life. Many products that older people may consider optional are not experienced as 'nice to haves' by younger people. For example, social media services were not seen as optional for young people.

> **"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."**
>
> **"Without social media we'll be unable to connect with friends."**

[14] For example, Human Rights Watch analysed the EdTech products recommended in NSW and Vic during the pandemic at 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

[15] For a description of how social media platforms have become a central part of rapid hazard warnings see Mehta, A., Murray, S., McAndrew, R., Jackson, M. & Tippett, V. (2022) 'Encouraging evacuation: The role of behavioural message inputs in bushfire warnings' International Journal of Disaster Risk Reduction, DOI: 10.1016/j.ijdrr.2021.102673

[16] 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/

More plainly put, young people said that they couldn't really decline to use any digital platform, because "there really isn't any other way" and they had "no choice but to use them". Where declining is not an option users do not freely consent. This is more characteristic of coercion than meaningful consent.

> **"Because you rely on it. So it's not even about whether or not you can, you don't really have the choice to trust it or not (with your privacy). You just have to use it because everyone else is on it. It isn't about whether or not you believe in your privacy."**

Given that young people felt they had to use these products, we asked if young people placed much stock in what it meant to click 'I accept' to a privacy policy or collection notice. Routinely, young people told us that it did not:

> **"I don't really think it means much (to click "accept") since most people don't actually read it or comprehend what they're accepting to. And they I feel like because most people like all their friends and everyone, they've already accepted it. They feel like since it's like safe for them, and everybody's doing it that it's kind of the norm. So most people don't really think twice about it. And they mostly go 'oh, it's just a notification, I'll just get rid of it', and continue because they don't want to spend too much time dwelling on it, or thinking too much about what's actually behind it."**

This does not suggest that the current model is effective at generating meaningful consent to data collection among young people. Existing Australian legal frameworks[17] may also question the validity of this consent.

Despite young people's general malaise around the concept of consenting via accepting a collection notice, there was still a broad appetite among all the young people we spoke to around ensuring that privacy policies and collection notices were comprehensible. "There should be plain wording... of the company and the website... explaining what they can do with our data. A few plain words in normal language and we might be able to see what we agreed to."

Collection notices and privacy policies were still important documents for the young people involved in this research, and they wanted to be able to understand them and inform themselves. They believed that informed knowledge about data processing allowed them to develop their own personalised privacy risk mitigation strategies. As one young person put it, "at the very least we need to know the risks" so they can start to think about "what are the ways to lessen the risk". The *Privacy Act* Review proposes ensuring that policies and collection notices are comprehensible, including to young people. Again, the evidence from young people suggests that this is a desirable approach.

Proposals 10.2 & 16.3 of the Privacy Act Review

At the time of this research, a number of jurisdictions around the US are moving to a model of requiring parental consent until the age of 18 as a move to keep young people off social media.[18] We asked young people if they thought that approach was viable or desirable in Australia. Given that young people described the digital world as compulsory, there was a strong sense that this was not the right approach, and that it would encourage young people to find workarounds; "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 *Privacy Act* Review also raises questions about the age of 'digital consent', and proposes continuing to rely on existing OAIC Guidelines on children and young people and capacity to consent, rather than a blanket increase or decrease of the age. From young people's perspectives this might be the right approach.

Proposal 16.2 of the Privacy Act Review

[17] This may violate the element of voluntariness is section B.38 of the APP Guidelines in itself

[18] For example Utah 2023 S.B. 152 Social Media Regulation Amendments, Arkansas 2023 SB396 - To Create The Social Media Safety Act; To Require Age Verification For Use Of Social Media; And To Clarify Liability For Failure To Perform Age Verification For Use Of Social Media And Illegal Retention Of Data; Louisiana 2023 amendments to HB61 Contracts: Provides for consent of a legal representative of a minor who contracts with certain parties

PRIVACY AND TRUST

In our poll, we asked 16 & 17 year olds if they trusted digital platforms when it came to their privacy. Predominantly, it seemed that 16 & 17 year olds did not trust platforms with their privacy, with 40% suggesting that they distrusted platforms, 32% suggesting they neither trusted nor distrusted platforms and 28% saying that they did trust platforms with their privacy. This suggests a significant trust deficit among Australian teens.

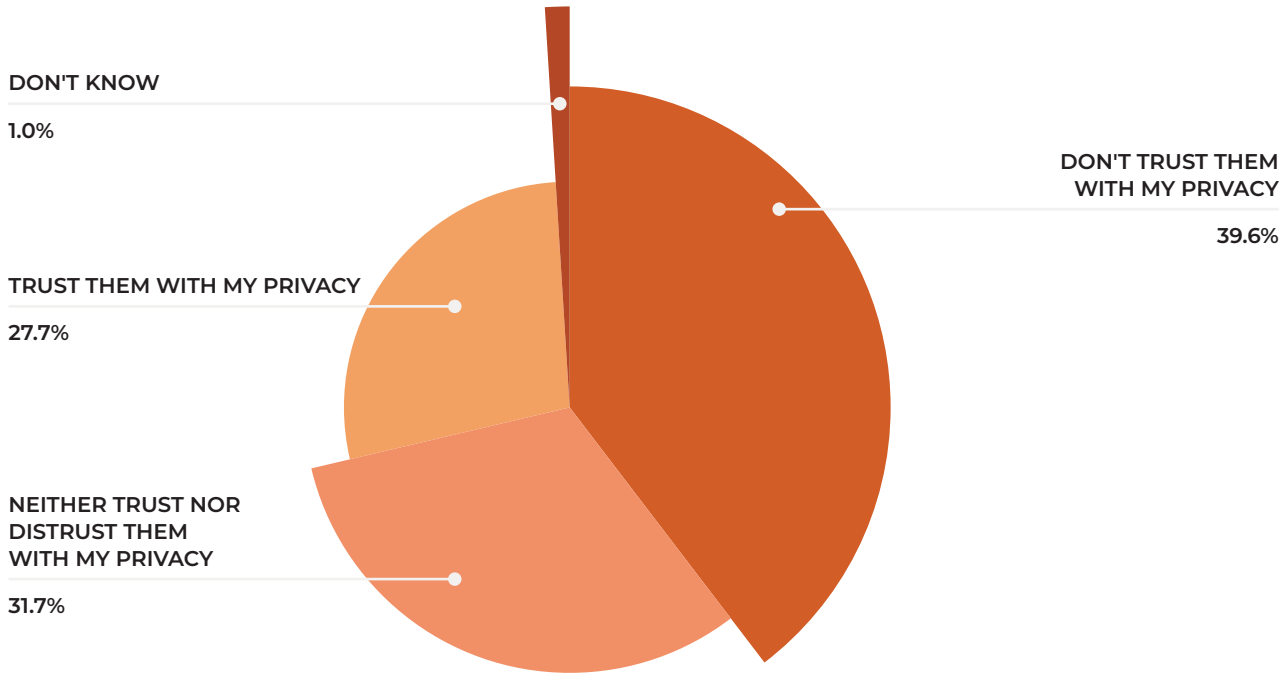

Figure 1: In your opinion, when thinking about whether digital platforms and apps respect your privacy, do you... (n=506)

We also asked if they trusted digital platforms to handle their data carefully. Here too, we found higher levels of distrust than trust; 32.7% of young people did not trust that their information was handled carefully, compared to 26.7% who did trust that it was handled carefully. (Note this polling was done before the Medibank and Optus breaches). It also found significant 'mixed feelings', with 38.6% of young people neither trusting nor distrusting that their data was handled carefully.

Young people who took part in the poll were asked to explain where their trust or distrust came from. A lot of the young people who distrusted digital platforms and services to treat their information with care suggested that advertising, hacking and the business model and profit motives of platforms and lack of transparency were key sources of concern (as discussed above).

For those who neither trusted nor distrusted that their data was handled carefully, many young people just hadn't thought about it yet or just weren't bothered either way, saying things "I don't know what they do with my information but it doesn't bother me enough" or "I tend not to think much about it". But other young people expressed genuinely ambivalent perspectives, saying for example "I neither trust nor distrust digital platforms and apps with my privacy as I generally do know what types of data they are collecting e.g. my interests, and common searches. However, I am unsure of what they use all the data for," or "because sometimes they can check your data when you give them no permission they can probably override the system but sometime(s) I think they do keep privacy".

In our interviews, we also asked young people to help us understand why this might have been the most common response, and one young woman elaborated on the sense of ambivalence this sort of question might generate; "if I was given that question, I'd say 'Sweet Jesus, like no, I don't think I trust them with my privacy.' But at the same time, you know, I'm on every social media that there is so. And I think a large part of that is... not caring".

We also asked about the drivers of trust. Three key arguments drove trust in digital platforms. Firstly, trust emerged because growing up now simply requires the use of these digital platforms and products, as described above. Young people said, for example, that they trusted platforms "because there is no other option." This was reinforced in one of the panel discussions that young participants took part in, where they described trust as emerging from the realisation that some digital platforms were just essential to life. Talking specifically about EdTech platforms—digital platforms used in schools—one young person said "we trust our schools. If these orgs (Ed Tech platforms) are doing bad things with our data, they wouldn't have recommended them", reinforcing the belief that 'everyday' platforms are probably privacy preserving.

Secondly, trust also emerged from a sense of data processing not being that 'important' or a belief that their specific data did not need privacy, with young people commenting "I don't have anything to hide from them" for example, or "I don't have much information that is compromisable."

An effective regulatory framework was also cited as one of the key drivers of trust, with multiple young people noting that their trust came from privacy laws and their rigorous enforcement; "Because of laws to protect consumer privacy", "Because if they don't there are severe repercussions", or "Because they are big companies, and if they don't comply with regulations they will be hit with fines".

This underpins the importance of strong privacy regulations in creating the trustworthy, privacy preserving digital world that young people want to see.

WHAT YOUNG PEOPLE WANT TO IMPROVE THEIR PRIVACY

Young people wanted their privacy improved online, and understood the role of digital platforms and regulation to make that possible.

SUGGESTIONS FOR DIGITAL PLATFORMS

We asked young people in the poll what changes companies could make to improve trust in digital platforms, from a fixed set of suggestions. Transparency, data sale and control (in general and in terms of purpose limitations) emerged as popular controls platforms themselves could implement to improve trust.

WHAT WOULD MAKE YOU TRUST DIGITAL PLATFORMS AND APPS MORE WITH YOUR PRIVACY?

If platforms offered me more transparency (i.e., about what personal data they are collecting and what they do with it)	67%
If platforms did not sell my data to corporate interests	65%
If platforms offered me more control (i.e., more choice over what data platforms can collect and what they do with it)	62%
If platforms only used my information in ways that I had signed up for, and not for other purposes whenever they want	61%
If platforms offered better ways to make complaints and fix privacy problems when something goes wrong	41%
If platforms did not target me with personalised ads	41%
If platforms agreed to respect my rights in general	57%
None of the above	3%

Figure 2: Responses to the question 'What would make you trust digital platforms and apps more with your privacy? (n=506, respondents could select multiple answers).

We also asked respondents to offer their own suggestions and six clusters of suggestions emerged:

1. Choice and control. There were lots of suggestions where young people asked for more choice and control over their data. For example "I know this provision exists with some digital platforms but having the ability to choose what sort of data the platform collects would increase transparency and trust in my opinion", "More control over my privacy and I decide what I wish to disclose and that doesn't restrict my use of the app", "Options", ""Giving me a say in the privacy's control"

2. Transparency. Transparency was also central to many suggestions, e.g.: "Knowing how they use my data", "I would trust them more if they say exactly what they are doing with the data collection", "If the digital platforms and apps where transparent from the beginning about the data collected and whom it is sold or shared to"

3. Data minimisation. Reducing the amount of data collected, shared and retained was also suggested multiple times, for example "Not collect lots of our data", "Don"t store it on databases", "An option to not collect any data would be ideal", "If they didn't use my data" Not having to give away information to gain access to apps"

4. Less data transfer. A number of requests to not sell data or not share data as widely were made. "Them not selling my info", "Not selling my data to third parties, not subscribing me to emails and letting me control what data they collect and having full transparency"

5. Targeted advertising. Targeted ads were also mentioned by multiple young people: "Them not listening to me and giving me targeted ads", "No personalised adverts", "Less ads targeted toward my age group", "Less targeted ads"

6. Improved data security. Security was also a key concern, for example suggestions included "Two factor security", "a VPN", "Make sure no one hacks", "The assurance by the platform to keep my data safe"

SUGGESTIONS FOR POLICY MAKERS

Young people involved in this research also drafted a submission to a Senate inquiry. In their submission, rather than suggestions for platforms to implement, young people spoke about policy principles they felt should be adopted in Australia's privacy frameworks. They came up with a 14 point plan:

"To realise young people's best interests their personal information should:

- Must be only collected and used in ways that advance their best interests
- Be collected and used only when it is needed. No one should be able to collect data that they do not strictly need, including GPS data and "cookies". Don't collect or use these unless they are needed
- Be collected and used only when young people have clearly been asked:
- Agreeing to confusing privacy policies, or out of date policies, is not enough. Fine print isn't okay, it's got to be clear
- Young people should be asked about all the types of information that is going to be collected, and all the ways it is going to be used. A single 'yes' or 'no thanks' button isn't good
- Personal information should not be used in any ways other than what young people were clearly asked about
- Young people should not be pushed or tricked into agreeing to data collection, for example:
- Dark patterns - don't make the 'yes' button bigger than the 'no thanks' button

- Rename “cookies” as “data grabbers”
- Be collected, used and stored in safe and secure ways
- Be kept for as long as is it needed only
- Not be sold or traded to other companies
- Young people should have the right to request it be deleted
- Companies that collect and use young people’s data should be accountable to them. If something goes wrong, it should be the company’s responsibility to provide help and support and fix it
- Not be used in ways that can harm, including in algorithms that make apps addictive or encourage harmful content in ‘for you’ feeds
- Companies should have to be transparent about what information they are collecting, and who they are sharing or selling it to. This means being clear with each individual
- Young people should be supported and educated about privacy, their rights and risks
- Don’t have advertising turned on by default for young people. Young people should be able to opt-in to advertising overall, and also be able to choose if they want their data used to personalise these ads or not.

We want to see all young people under 18 protected, as this is their rights. But we would also encourage you to think about protections right up until the age of 25, to ensure extra safety and privacy for young people as they transition into adulthood.”

Central to the suggestions young people offered to platforms and also to policy makers, which also emerged frequently in the discussions involved in this research, was a desire for a fundamental change to the prioritisation of their privacy online. At the moment, there was a belief that privacy practice and privacy policy prioritised commercial interests. As an example, one young person noted that Instagram did not prioritise young people's privacy, noting that it wasn't in Instagram's interest to do so:

> **"I think things like, you know, people who like just get on Instagram, they're not really like, aware of like, privacy concerns and everything. So when you know, it kind of defaults your account to like public and your location settings are on, you know, everyone can like see you, when (Instagram) have all those like settings as like, all your information is out there. And (Instagram) had like, all of the things like, 'well, we can use your information to give to third party' like all of those are, like clicked on. I wish it was like, kind of like, the opposite. And you can, like, put it on hold. But why would they do that? It's like really convenient for them."**

Wanting the "opposite" is loaded. Young people spoke time and time again about wanting their privacy to come first. They spoke about wanting to "change cookies to opt-in not opt-out, so young people don't feel like they have to click accept", or "change defaults to high security".

Young people spoke about having to do so much to try and protect their privacy online, but to limited effect. "I check my privacy settings every few months. (But companies have) ways to get around it and send suggested posts and ads anyhow. It's annoying", and that placing the burden on users to keep themselves private was unfair, "people shouldnt have to consider buying a VPN if they are scared of people tracking them". As one young person clearly put it "you have to work really hard to be protected online. If there was more effort put into protecting people at this age, it would be really good."

Overall, young people wanted platforms and policy makers to step up and prioritise their privacy. They want the digital world to start putting their best interests first.

CONCLUSIONS

Young people hold nuanced and contextual understandings about privacy in the digital environment.

They talk about online privacy as an important right that they should be able to enjoy. However, this right is violated so routinely and frequently that there is a deep sense of pessimism among young people about the possibility that it could be advanced in practice and in policy.

This should give us all pause for thought. The young people involved in this research feel as if their best interests have so often been overlooked that they question if it is even possible to have their rights prioritised. This is an issue that we can all address, by changing the public discourse and centralising young people's best interests as we think and talk about technology.

As Australian policy makers review the digital policy landscape, including both the *Privacy Act* Review and the *Online Safety Act* review scheduled for later this year, young people's best interests should be prioritised. This requires shifting the burden of responsibility from young people and placing duties of care or other proactive requirements onto digital platforms themselves. It also involves engaging young people directly.

As Australian civil society organisations engage with the public and policy makers, thinking about young people's best interests also matters. Understanding your own advocacy goals, as well as your operational processes, matters.

As technologists develop digital platforms, they should consider the best interests of younger users and design their products and services with young users in mind. Privacy-by-design, alongside child rights-by-design and safety-by-design mindsets need to be adopted. It should not be left to children and young people to keep themselves safe. Engage with young people, and keep their rights in mind.

IMPLICATIONS FOR THE PRIVACY ACT REVIEW

The findings from this research lend support for a number of proposals in the *Privacy Act* Review, as documented throughout this report. Specifically, it lends support for proposals:

- 4.1 and 4.3, which amend the definition of privacy to include metadata and inferred data like digital profiles
- 10.2 and 16.3, which require privacy policies and collection notices to be clear and understandable, including for children
- 16.2 which suggests that current 'age of consent' guidelines stay in place
- 16.4 which requires companies to consider the best interests of children when deciding if data collection, use or disclosure is acceptable
- 16.5, the introduction of a Children's Privacy Code, that covers all services likely to be accessed by children. The Code must be developed in conclusion with children and young people, and address how services can function in the best interest of children
- 20.5 and 20.7 which prohibits direct market to a child and trading children's information
- Caveated support for 20.6, which prohibits targeting a child unless it is in their best interest. There is strong support to prohibit targeting advertising to children, but given the essential nature of digital products and services as described by young people, prohibiting all targeting would be problematic (For example. products like search engines provide target specific responses to queries). This is not incompatible however, and consideration of children's best interests here needs to consider their rights to access and to information.

IMPLICATIONS FOR THE UPCOMING REVIEW OF THE ONLINE SAFETY ACT

The Government has announced a readiness to review the *Online Safety Act* earlier than required, and a review may potentially start this year. While this research focused on online privacy, the broad discussion among young people may have implications for a review of online safety.

- Young people spoke of a desire to have their best interest prioritised by default, and for platforms and regulators to carry the burdens of advancing their rights, which may suggest a need for broader duties of care and enhanced online safety expectations
- Young people spoke about intersections between privacy and safety, such as concerns about location data and privacy settings as part of their experience online. This might suggest a need for a comprehensive exploration of young people's experiences.
- Engaging with young people directly throughout the process must continue


BY
NC