alannah & madeline foundation

Inquiry into social media and online safety:

A submission by the Alannah & Madeline Foundation

December 2021

alannah & madeline foundation

Safeguarding our children's future together

Contents

Executive summary 3
About us 4
Recommendations 4
Growing up in digital spaces 6
The context of reform 7
The best interests of the child as a guiding principle 8
Hearing the views of children and young people 9
Age assurance 10
Identity verification and antisocial behaviour online 11
Handling of personal data 12
Building strength in schools, families and communities 13

alannah & madeline foundation

Safeguarding our children's future together

Executive summary

We welcome the Government's decision to inquire into the harms Australians face online, with particular attention to children and young people. Digital technologies are fully integrated into the lives of most Australian families, bringing benefits, risks, harms and opportunities. At the Alannah & Madeline Foundation, we are passionate about bringing to life children's rights and making the online and offline worlds positive, empowering places for children to learn, play, express themselves, and connect with family and friends.

Digital technologies bring many positives for children and young people in areas such as education, social connection, entertainment, service access, and participation in public life. Unfortunately, the digital world was not designed originally to be safe and appropriate for children, and too many young Australians have had risky or harmful experiences online, such as exposure to violent or extreme content, contact from strangers, involvement in cyber bullying or image-based abuse, and threats to their privacy and personal data.

It is unreasonable to place responsibility for avoiding these problems solely with children and their families, especially when many parents and carers have limited digital literacy themselves. We are particularly concerned about our most isolated and disadvantaged families. They tend to have the least access to the positive benefits of digital technologies and the highest risk of harmful experiences online.

In light of these concerns, we welcomed the ground-breaking position of the Government's recent Exposure Draft of the Online Privacy Bill: that digital platforms operating within the proposed Online Privacy code should consider the best interests of the child as the primary principle in relation to handling children's personal data. We encourage the Select Committee to follow this example and adopt 'the best interests of the child' as a primary guiding principle in any future reforms recommended here. There are several broad approaches the Select Committee could take which we believe would help uphold children's best interests.

Firstly, we encourage the Select Committee to engage with the National Commissioner for Children, as well as the eSafety Commissioner and the Information Commissioner, to place a child-rights lens over any recommended reforms. In particular, we encourage this approach in relation to the new Social Media (Anti-Trolling) Bill. This Bill raises questions about the handling of children's personal data by digital platforms and the responses to children who behave antisocially online.

Secondly, it is important that children and young people have meaningful opportunities to contribute to this inquiry. We welcomed the announcement that the Government will set up an Online Safety Youth Advisory Council in 2022, but we are concerned that this inquiry's timeframes will not allow for much meaningful child or youth engagement. We encourage longer consultation times and targeted resourcing to address this.

Thirdly, we hope to see an undertaking from the Select Committee that any approaches recommended to address online harms will function to uphold all of children's rights – including children's rights in relation to privacy, safety, dignity and expression – not further endanger them. For example, age assurance mechanisms (mentioned in the inquiry's terms of reference) should not be discriminatory, should not exclude children from beneficial, age-appropriate experiences online, and should not escalate digital platforms' collection of children's personal data for commercial purposes.

Ultimately, we wish to see digital platforms align with the National Principles for Child Safe Organisations, with standards equivalent to those found in trusted offline spaces where children live, learn and play. We encourage the development of codes and guidance for industry to assess how the design and function of digital platforms affects children's ability to enjoy their rights, and to address any concerns identified.

Legislative and industry changes should be complemented by investment in schools, early childhood settings, families, and support services. Educators and other professionals who work with children and young people are under great pressure to help families prevent and address problems online; their roles should be recognised and adequately supported.

Finally – and crucially – we note that this is a period of significant review and reform of digital technologies in Australia, with multiple pieces of legislation and industry codes being developed and implemented. We trust the recommendations of this Select Committee will have regard to this wider context.

About us

The Alannah & Madeline Foundation is the leading national not-for-profit organisation working to protect children from the effects of violence and bullying.

We care for children who have experienced or witnessed serious violence; reduce the incidence of bullying, cyber bullying and other cyber risks; and advocate for the safety and wellbeing of children.

Our programs are in close to one third of Australian schools and more than 80% of Australian public libraries. We also support 10,000 children in refuges or foster homes across the country every year through our Buddy Bags program.

We have reached more than 2.7 million children and their families nationwide since the Foundation started.

Recommendations

1. In line with the approach proposed in the Exposure Draft of the Online Privacy Bill, adopt 'the best interests of the child' as a primary guiding principle for any reforms recommended by the Select Committee. A definition of 'the best interests of the child' should be guided by and align with the United Nations Convention on the Rights of the Child. General Comments No.14 and 25 are especially relevant, stating that the best interests of the child should be assessed and taken into account as a primary consideration in all actions and decisions that affect children under 18 in the public and private spheres. This includes all actions regarding the provision, regulation, design, management and use of digital technologies.

   For example, specific steps to uphold children's best interests on digital platforms might include:

   - providing the highest privacy settings by default
   - providing prominent, accessible tools for children to report concerns on the platform
   - not disclosing children's data to third parties, unless there is a compelling reason to do so in the best interests of the child
   - collecting only the minimum personal data necessary to provide the elements of the digital platform in which the child is actively and knowingly engaged
   - not 'nudging' children to supply additional personal data or choose weaker privacy settings.

2. Before drafting recommendations, engage the National Commissioner for Children, as well as the eSafety Commissioner, to ensure any proposed reforms have been considered through a child rights lens and align with the best interests of the child.

3. Ensure the recommendations of the Select Committee have regard to, and align with, the substantial work being undertaken in related spaces, including the development of an age verification roadmap and Restricted Access Systems declaration by eSafety; the development of industry codes concerning Class 1 and 2 harmful material; public consultations on the Online Privacy Exposure Draft and Online Safety (Basic Online Safety Expectations) Determination; the anticipated introduction of an Online Privacy Code for industry and a BOSE instrument to guide industry in complying with the Online Safety Act; civil society input concerning the Social Media (Anti-Trolling) Bill; and the release of the National Strategy to Prevent and Respond to Child Sexual Abuse.

4. Set aside an additional consultation period for this Select Committee to engage directly with children and young people, and their families and educators, to give them meaningful opportunities to make considered contributions to this inquiry. Consultations should be appropriately resourced and might be achieved through partnerships with the National Children's Commissioner, the eSafety Commissioner, research institutes and/or civil society organisations with expertise in child-rights practice. It is especially important to engage with rural, regional and remote communities, and with communities experiencing high levels of disadvantage, as they face higher levels of digital exclusion and online vulnerability than the rest of the country.

5. Consult with the National Commissioner for Children, the eSafety Commissioner and the Information Commissioner about the Social Media (Anti-Trolling) Bill, to ensure its final wording upholds children's rights and the best interests of the child. In particular, we refer to the United Nations Committee on the Rights of the Child, General Comment No.25, which specifies that state policymakers should consider the effects of cybercrime laws on children, focus on prevention, and make every effort to create and use alternatives to a criminal justice response. This approach recognises that children have unique vulnerabilities and unique potential for positive change and deserve to be treated differently to adults, even when they behave antisocially.

6. Invest in initiatives to build strength in early childhood settings, school communities, families and support services. There should be a focus on Australia's most digitally excluded and disadvantaged children and young people. In particular, we encourage investment in:

    - high-quality digital literacies education, aligned with developmentally appropriate education about respectful relationships, with expert support for educators to prevent and address antisocial behaviours online and offline
    - high-quality social and emotional learning initiatives, structures and programs
    - meaningful partnerships for early childhood settings and schools with trusted providers of high-quality digital literacies education
    - targeted interventions to build the skills and supports of professionals who work with vulnerable children and young people to address their needs, strengths and concerns online and offline
    - targeted interventions to build the strengths, skills and support networks of parents and carers in communities with low levels of digital inclusion, to better enable them to support children and young people online. Supporting rural, regional and remote communities should be a particular priority. These interventions should be responsive to local circumstances, culturally appropriate, and built on trusting relationships.

7. Adopt the position that digital platforms used by children should be supported to align with the National Principles for Child Safe Organisations, as offline spaces frequented by children are increasingly expected to do. Digital providers might move towards this goal through greater child safety risk assessment and high-quality training in child-safe planning and practice, delivered by reputable providers. There may be a need to fund the development of training that is specific and relevant to digital platforms.

8. Articulate that any mechanisms for age assurance on digital platforms should be guided by the best interests of the child as the primary consideration. We submit this means that any such mechanisms should be non-discriminatory and accessible to all families, should have regard to all of children's rights, and should function to strengthen children's privacy, safety and dignity, not further endanger these things. For example, personal data provided for purposes of age assurance must not be processed for any other purposes. See the principle of data minimisation articulated by the European

Union General Data Protection Regulation, as well as the UN Convention on the Rights of the Child, General Comment No. 25. (Significant work in this space is also being undertaken in relation to the Online Privacy Bill and proposed Online Privacy code.)

9. Ensure that any age verification mechanisms to restrict access to adult content uphold the highest standards of protection for personal data. While children should be denied access to adult-only websites, it is vital that their personal data is not stored by age verification providers or shared with age-restricted websites or any other third parties. (See the work being led by eSafety.)

10. Support the development of an Online Privacy (OP) code by the Information Commissioner, in close consultation with the eSafety Commissioner and the ACCC, as provided for in the Exposure Draft of the Online Privacy Bill. We urge that this code also be developed in close consultation with the National Commissioner for Children. The code should align with the Basic Online Safety Expectations developed through the Online Safety Act, while also enhancing children's overall experience online by ensuring that any handling of children's data by digital platforms is guided primarily by the best interests of the child.

11. Support the development, implementation, evaluation and refinement of child-friendly standards for the published terms of digital platforms.* Published terms should be clear, child-friendly, prominent, easy to find and navigate, timely, accurate, concise, and current.

12. Continue to support the 'Safety by Design' principles and initiatives being led by the eSafety Commissioner to help digital platforms to anticipate, detect and eliminate harms before they occur.

13. Invest in robust research, analysis and evaluation to assess the short- and long-term impacts of reforms in this space, notably the Online Safety Act, Online Privacy Act and the Social Media (Anti-Trolling) Act. It is especially important to identify any impacts on children and young people, and the findings should be shared with the whole community.

Growing up in digital spaces

Digital technologies are fully integrated into the lives of most Australian families, with 4 out of 5 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 10 young Australians use social media daily.[2]

There are many positive uses for digital technologies. For example, 90% of Australian parents agree that digital technologies have made it easier for children to stay in touch with family and friends.[3] And in a study of 30 countries, Australian children scored well above the global average on a number of positive measures, such as digital empathy, managing their 'digital footprint', and thinking critically about things they see online.[4]

However, too many children and young people continue to have risky or harmful experiences. For example, half of all young Australians aged 15-17 have experienced cyber bullying or other hurtful behaviours online at some point.[5] Compared to the global average, Australian children are at relatively high risk of encountering cyber bullying and/or risky content online. They also tend to receive quite scarce guidance about online issues from their parents and carers, compared to children in many other countries.[6]

* Published terms include privacy policies, community standards, terms of service, cookie policies, and other important published documents.

In many cases, this is because parents and carers have low levels of digital literacy themselves. For example, a survey by the Australian Centre to Counter Child Exploitation found that parents commonly reported feeling overwhelmed and struggling to keep up with their children online.[7] At our online safety

workshops, many parents tell us that they struggle to support their children online and would welcome stronger built-in safeguards within digital products and services.

Some families are especially vulnerable. Families who struggle with disadvantage and isolation are at higher risk of missing out on the positive benefits of digital technologies. Levels of 'digital inclusion' (access, ability and affordability of technology) are much lower in Australian households where the adults are unemployed, earning very low incomes, and/or without post-school qualifications. Rural and remote communities also continue to be much less 'digitally included' than major cities.[8]

Meanwhile, research from the UK shows that children and young people who are very vulnerable in the offline world are at higher risk than their peers of having negative experiences online. These include young carers, children and young people in out-of-home care, and those with disability, long-term illness, mental health concerns and/or eating disorders. These vulnerable children and young people are more likely than their peers to have negative or risky experiences online, such as sharing nudes, being the victim of image-based abuse, feeling controlled or stalked, viewing violent material, and/or visiting sites meant for adults.[9]

Other risks exist for all users at a basic design level – for example, when accounts are set by default to the lowest privacy settings. In a recent research project, the 5Rights Foundation created avatar child profiles on social media and found that within days these accounts were being followed by strangers and receiving unsolicited messages and pornography, as well as being prompted towards harmful content (eg. suicide or eating disorders) based on any signs of interest from the child.[10]

Unfortunately, despite their higher vulnerability online, children and young people are relatively unlikely to report concerns to digital platforms. Surveys of Australian, British and American young people showed that only 8-14% of those who'd had a negative experience online reported it to the site where it happened.[11] And while many children and young people don't make a formal report because they are not upset or cope in other ways, there are many who don't report because they do not understand the reporting processes or do not believe that reporting will help.[12]

The context of reform

Addressing all the concerns listed in the previous section (and others) is a long-term, complex challenge for governments, industry and civil society. We note that significant reform is already underway in several areas, which we have been grateful for the opportunity to take part in.

Key reforms include:

- development of a 'roadmap' for the introduction of age verification for online pornography (eSafety)
- drafting of a Restricted Access Systems declaration (eSafety) concerning children's exposure to R18+ or Category 1 Restricted material online
- development of industry codes for Class 1 and 2 harmful material in response to the Online Safety Act.
- consultation on the Online Privacy Exposure Draft and anticipated development of an Online Privacy code for industry
- consultation on the Online Safety (Basic Online Safety Expectations) Determination and development of a BOSE instrument to guide industry's compliance with the Online Safety Act
- release of the National Strategy to Prevent and Respond to Child Sexual Abuse, which includes a focus on preventing and addressing online harms
- introduction of the Social Media (Anti-Trolling) Bill 2021, which we understand this committee will also scrutinise.[13]

In order for the recommendations of this Select Committee to be meaningful and beneficial for children and young people, it is important that they communicate clearly how they will align with the above work.

We also support the approach of 'Safety by Design', which is being developed and promoted by the eSafety Commissioner, to help digital platforms to anticipate, detect and eliminate harms before they occur. We support its guiding principles of service provider responsibility, user empowerment and autonomy, and transparency and accountability.[14]

The best interests of the child as a guiding principle

At the Foundation, we are passionate about bringing to life children's rights. As such, we welcomed the ground-breaking position of the Government's recent Exposure Draft of the Online Privacy Bill: that digital platforms operating within the proposed Online Privacy code should consider the best interests of the child as the primary principle in relation to collecting, using and disclosing children's personal information.[15] With the right leadership, expert guidance, and resourcing in place to realise its aims, this provision has the potential to be a 'game changer', putting children's rights front and centre in the digital world.

We encourage this Select Committee to follow the example set in the Online Privacy Bill and adopt 'the best interests of the child' as a primary guiding principle in any future reforms recommended.

As a starting point, we refer to the United Nations Convention on the Rights of the Child, and its General Comments 14 and 25 (The right of the child to have his or her best interests taken as primary consideration, and children's rights in relation to the digital environment). They state that the best interests of children should be assessed and taken into account as a primary consideration in all actions that affect children in the public and private spheres. This includes all actions regarding the provision, regulation, design, management and use of digital technologies.[16]

To uphold children's best interests, we need online and offline environments which:

- uphold children's right to survival and positive holistic development
- are non-discriminatory and respectful of children's dignity
- enable children to express their own views and be listened to by decision-makers
- uphold all of children's rights, including rights to health, education, play, cultural life, protection from sexual exploitation and abuse, and protection from illegal or arbitrary interference in their privacy.[17]

It can be complex and challenging to determine what is in 'the best interests of the child', and sometimes decision-makers must balance various factors, such as the conflicting interests of different children. However, the commercial interests of digital platforms should not outweigh the rights of children.

We believe there should be a clear, enforced expectation that digital platforms have a duty of care to children who use their products and services, and that the standards of digital spaces used by children should be in line with community expectations and equivalent to that expected of in-person spaces where children live, learn and play.

To this end, we have called for child safety training, planning and risk assessment for digital platforms, with the aim of bringing them in line with the National Principles for Child Safe Organisations. These processes should cover risks associated with contact, content, conduct, system design and data collection and use.[18]

The National Principles, while not mandatory, can be used by businesses which provide services to, and work with, children and young people. We believe it would make sense for digital platforms to engage with the National Principles, in the spirit of ensuring children enjoy the same safety standards online as they do offline.[19]

We have also encouraged the development of codes and guidance for industry to assess how the design and function of digital platforms affects children's ability to enjoy their rights, and to address any concerns identified.

For example, we note the development of an age-appropriate design code in the UK. The code sets out steps that digital platforms could take to help protect children's best interests, for example undertaking to:

- collect and retain only the minimum personal data necessary to provide the elements of the digital platform in which the child is actively and knowingly engaged
- provide the highest privacy settings by default and do not disclose children's data to third parties, unless there is a compelling reason to do otherwise in the best interests of the child
- provide prominent, accessible tools to help children report concerns
- give clear, accurate information to children about any parental controls provided
- not 'nudge' children to provide unnecessary personal data or turn off privacy protections
- consider how, in their use of data, the platforms can help to keep children safe from exploitation, support children's healthy development, and uphold children's rights to expression and play.[20]

It is also important that children are respected as digital citizens. Children should not be excluded from beneficial experiences online on the grounds that their needs are 'too hard' to meet. The aim of reforms should be to bring about a digital world which upholds the best interests of the child in line with community expectations, to help enable children to thrive.

Hearing the views of children and young people

In order to uphold the best interests of the child, it is important that we enable children to express their views freely in all matters that affect them and have their views given due weight by decision-makers in line with the evolving maturity of the child.[21]

This approach aligns with the United Nations Committee on the Rights of the Child, General Comment No.25, which states 'When developing legislation, policies, programmes, services and training on children's rights in relation to the digital environment, States parties should involve all children, listen to their needs and give due weight to their views. They should ensure that digital service providers actively engage with children, applying appropriate safeguards, and give their views due consideration when developing products and services.'[22]

Hearing directly from children and young people also helps policymakers to gain original insights and build a clearer picture of the strengths, risks and priorities of young Australians online and offline. This approach also helps policymakers and digital platforms to design more effective interventions, and to evaluate the outcomes of these interventions with greater accuracy and insight. This approach also aligns with Australia's Safety by Design principle of user empowerment and autonomy, as championed by eSafety.[23]

To this end, we express concern about this inquiry's timeframes, with submissions due 12 January 2022 and the Select Committee's final report due 15 February 2022. This very brief consultation period during the summer holidays is unlikely to yield much meaningful input from children, young people or their families.

We welcomed the announcement that the Federal Government will establish an Online Safety Youth Advisory Council to provide a direct voice to government.[24] However, as the selection process will not commence until 2022, it seems unlikely the council will be able to feed into this inquiry.

We encourage putting in place an additional consultation period with appropriate resourcing to facilitate meaningful engagement with children and young people, as well as parents, carers and educators. This might be achieved through partnerships with the National Children's Commissioner, research institutes and/or civil society organisations with expertise in child-rights practice, as well as the eSafety Commissioner.

Past research with children and young people has shown that they have varied and valuable insights to contribute. Children and young people have shared their views on (amongst other things):

- their favourite activities and greatest concerns online
- their exposure to risky or harmful experiences online, how this affects them, and how they cope
- their use of digital technologies during COVID-19 and the benefits and problems of this
- the commercial uses of their data by digital platforms and the gaps in children's knowledge and empowerment to respond
- the types of support children want from adults, schools and digital platforms to improve their experiences online.[25]

We submit that it is especially important to engage with rural, regional and remote communities, and with communities experiencing high levels of disadvantage, as they face higher levels of digital exclusion and vulnerability online than the rest of the country.

Age assurance

The inquiry's terms of reference ask about Australians' experiences of age assurance policies and practices. It is important to note the work has commenced on the issue of age verification by the eSafety Commissioner in response to the recommendations of the parliamentary report 'Protecting the age of innocence: Report of the inquiry into age verification for online wagering and online pornography'. Meanwhile, the Online Privacy Bill, for which consultations have just closed, provides for the development of an Online Privacy code for industry, which would address the issue of age assurance in relation to social media companies' handling of children's personal data.

We were grateful for the opportunity to contribute to both these consultation processes, and we trust that any future reforms will have regard to these significant pieces of work.

It is important that children can use digital products and services freely without encountering harmful content. For example, we have stated that we would welcome regulation at a structural level to make pornographic content inaccessible to children by default (eg. placed behind a separate domain) and only accessible to adults via age verification. The aim should not be to restrict children's access to digital technologies, but rather to make the digital world into a place that is safer for children.

At the same time, we stress that any mechanisms to restrict age-inappropriate content should be designed and function in ways which uphold the best interests of the child, including the highest standards of protection for children's personal data. Any age assurance mechanisms should function to protect children's privacy, safety and dignity, not further endanger them. For example, age assurance should not result in digital platforms intensifying their collection, storage or sharing of children's data for commercial purposes.

Indeed, the recent parliamentary report into age verification (a more stringent approach than age assurance) observed that such processes can be conducted by certified third parties and need not necessarily involve identity verification.[26]

We urge that any age assurance mechanisms align with the guidance of the United Nations Convention on the Rights of the Child, General Comment No. 25: that when children's data is gathered for a defined purpose (eg. to determine or estimate the child's age), that data should be protected and exclusive to this purpose and not retained unlawfully or unnecessarily or used for other purposes.[27]

Also significant is the European Union General Data Protection Regulation (GDPR), which states that data should only be processed for the legitimate purposes specified explicitly to the individual when the data was collected; organisations should only collect and process as much data as absolutely necessary for the

purposes specified; personally identifying data should only be stored as long as necessary for the specified purpose; and processing of data must be lawful, fair and transparent to the individual whose data it is.[28]

Meanwhile, it is important that any age assurance mechanisms are non-discriminatory, so that particular cohorts of children are not unfairly restricted from accessing and using the system on an equal basis with their peers. For this reason, we discourage mechanisms which require high levels of digital literacy or English-language proficiency in order to use them, or mechanisms which require significant official documentation. The latter is especially difficult for vulnerable children, such as those in out-of-home care.[†]

'Hard' age verification regimes requiring official forms of ID may well be appropriate for keeping adult material (eg. pornography and gambling) away from the under-18s. However, such stringent requirements are usually inappropriate elsewhere and can prove discriminatory. Lack of official identification should not exclude children from using digital products and services which are age-appropriate and beneficial or necessary to their learning, play, social connections and/or wellbeing.

It is also worth noting that age assurance mechanisms are not a 'magic wand' to keep children safe online. Well-designed age assurance mechanisms with clear and reasonable messaging can be useful: they help to set boundaries, making it harder (although not impossible) for children to access age-inappropriate digital products and services, and communicating to children that using certain products or services is unusual and unacceptable for their age group.[29] However, age assurance mechanisms do not make digital platforms into safe, age-appropriate places for children or young people. To achieve this, a broader 'safety by design' approach is needed. We refer to the work being undertaken by the eSafety Commissioner in that space.[30]

Identity verification and antisocial behaviour online

The inquiry's terms of reference ask about Australians' experiences of identity verification policies and practices. This question has arisen in the context of the new Social Media (Anti-Trolling) Bill, which states that in instances of alleged defamation online, social media companies, to avoid liability, would have to release the name, phone number and email address of the commenter to the applicant who has made the complaint of defamation, if the commenter consents. Otherwise, the applicant may request a court order to access the commenter's contact details in order to lodge a defamation case against the commenter.

We strongly encourage the Select Committee to engage with the National Commissioner for Children on this matter, along with the eSafety Commissioner and the Information Commissioner, to consider the ramifications for the collection, storage and sharing of children's personal data, as well as children's capacity to give informed consent to having their contact details released or withheld. It is important that the legislation functions to uphold the best interests of the child and all of children's rights.

It is also important to recognise that children, even when they behave antisocially or harmfully, are different to adults and warrant legal responses which are appropriate to their age, recognising their vulnerability and their potential for change. It is important to focus on rehabilitation, address the drivers of the behaviour, and set the child up to make positive, pro-social choices in the future. (It should also be recognised that many children who behave antisocially online have been the targets of antisocial treatment themselves.[31])

We refer to the United Nations Convention on the Rights of the Child, General Comment No.14, which underlines the importance of rehabilitation when dealing with child offenders, in recognition of children's early stage of development and particular vulnerabilities.[32]

More specifically, the U.N. Convention on the Rights of the Child, General Comment No.25, states that any interference with children's privacy should serve a legitimate purpose, uphold the principle of data

[†] To learn more about how age assurance mechanisms can be designed to uphold children's best interests, see 5Rights Foundation, "But how do they know it is a child?' Age Assurance in the Digital World'.

minimisation, be proportionate and designed to observe the best interests of the child. General Comment No. 25 also specifies that state policymakers should consider the impacts of cybercrime laws on children, focus on prevention and make every effort to create and use alternatives to a criminal justice response.[33]

Handling of personal data

The inquiry's terms of reference ask Australians about their experiences of the collection and use of relevant data by industry in a safe, private and secure manner.

This is a significant topic. Recent surveys found that 9 out of 10 Australian adults were concerned about their children's privacy and their children's data being misused online, while 7 out of 10 felt uncomfortable about businesses tracking their children's location without permission and/or obtaining and selling their children's personal information.[34]

These are valid concerns. As the Australian Competition and Consumer Commission (ACCC) has observed, the business model of many digital platforms centers around attracting large numbers of users, maximising their engagement, and building rich data sets about them, which can be monetised.[35] Meanwhile, research by 5Rights Foundation found that the design of many digital products and services – intended to maximise attention, spread and interaction – had the effect of putting children's privacy and safety at risk.[36]

Of course, digital platforms did not intend to cause harm to children, and some have taken positive steps for their younger users recently. However, more work is needed to deliver safe, age-appropriate standards to all digital products and services used by children. For example, the Government has raised concerns about the sharing of personal data for advertising purposes and the use of tracking, profiling and targeted marketing towards children.[37]

For this reason, in our submission to the Exposure Draft of the Online Privacy Bill, we expressed our support for the development of an Online Privacy (OP) code for industry by the Information Commissioner. The Exposure Draft proposes that the Information Commissioner be empowered to register an OP code or develop one directly if the Commissioner cannot identify a suitable code developer from within industry.

We believe that the Information Commissioner is the most suitable party to develop this code, in consultation with the ACCC, the eSafety Commissioner, and the National Commissioner for Children. The Commissioner is a trusted, independent national regulator directly accountable to the Australian public, with unique expertise in the field and authority to engage the wider community on this issue.

The Exposure Draft of the Online Privacy Bill contains a number of other welcome elements. Notably, it provides for the creation of an OP code with more stringent expectations about how digital platforms will communicate with their users in relation to their handling of personal data, and about how digital platforms will obtain meaningful consent from individuals to handle their personal data.[38]

These approaches have the potential to be very valuable. For example, there is much scope for improving the published terms of digital platforms. The ACCC found that digital platforms' published terms tend to be too long and complex for most adults to engage with meaningfully,[39] making genuine engagement by children unlikely. In their consultations with young people, 5Rights Foundation found that many did not understand digital platforms' published terms and did not feel empowered to make genuine choices.[40]

Ultimately, we hope to see the development of minimum standards requiring the published terms of digital platforms to be child-friendly, clear, accurate, concise, prominent, appropriate for different age and literacy levels, easy to find and navigate, timely and up to date.[41] This would align with Australia's Safety by Design principle of transparency and accountability.[42]

Moreover, we believe that if digital platforms were guided by the best interests of the child, the terms offered would be more beneficial and age-appropriate, and consent would be more meaningful. For example, children would be able to choose which elements of a digital product or service they wish to use, and

therefore how much personal data they need to provide, with products and services only collecting the minimum data necessary in order to deliver that aspect of the service to the child. In other words, children should have other choices online besides 'agree all' and 'reject all'.[43]

Building strength in schools, families and communities

To help deliver the best outcomes for children, legislative and industry changes should be complemented by initiatives to build strength in schools, early childhood settings, families, and community services. There should be particular consideration for the needs of Australia's isolated and disadvantaged families.

In our experience, families and educators are keen to support children to enjoy the benefits of digital technologies and avoid the harms. But many adults have limited skills and knowledge themselves. For example, at our Connect workshops, which we deliver in schools, many parents and carers want guidance about how to use online tools and services to help filter content and stop contact from strangers. The current approach for opt-in tools and services is insufficient and assumes a high level of digital literacy (and financial resources), which many parents and carers do not have. For example, parents often ask us questions like "What is an ISP?" and "How do I install and control a filter on my family's devices?" Research shows that only a minority of Australian parents (possibly a third) make successful use of tools like filters, software, privacy settings and passwords to help protect their children from risky content and contacts online.[44]

Parents also need help to have effective conversations with their children about sensitive topics. For example, parent surveys from the UK and New Zealand indicate that a large minority of parents (perhaps 40%) say they don't feel comfortable talking with their teens about online pornography or don't know where to find the right information about it.[45]

Parents who are struggling with these issues often look to trusted educators for advice. And when children behave antisocially online, parents tend to expect the school to lead a swift, effective response. This places stress on both schools and families. School communities need the skills, resources, capacity and supportive networks in place to deal with these increasingly complex demands.

To support school communities to build their strengths, eSmart (Alannah & Madeline Foundation) offers a suite of products which reach thousands of students, parents and teachers each year. They include:

- high-quality educational resources to build students' digital intelligence, such as Digital Licence+ and Media Literacy Lab
- partnerships with trusted Connect providers of high-quality digital literacy information for parents, educators and students
- eSmart Schools advisors, who support schools to put in place conditions to prevent and address antisocial behaviours online and offline. This includes engaging positively with parents about behavioural expectations online and offline, and supporting students to develop their own messaging and resources about smart uses of digital technologies.

School communities also need effective approaches to social and emotional learning which enable students to build empathy skills, recognise and respond to problems early, de-escalate situations, and appropriately support peers who have had upsetting experiences online or offline.

Meanwhile, targeted interventions are needed to build the strengths, skills and support networks of our most digitally excluded and disadvantaged families and the services that support them. Vulnerable children – such as those living in out-of-home care – are less likely than their peers to have received cyber safety education that was relevant to them, and are less likely to have trusted, digitally literate adults in their lives.[46]

More work is needed to build the skills and supports of professionals who work with vulnerable children and young people, to address their needs, strengths and concerns online and offline. These professionals include youth workers, social workers, other allied health workers and school wellbeing staff.

We also encourage more investment in high-quality support for parents and carers living in communities with low levels of digital inclusion, to better enable them to communicate with their children about what's happening online, set clear, consistent and reasonable expectations, and support children and young people effectively if things go wrong. Vulnerable parents and carers are often the ones least likely to benefit from 'standard' cyber safety products, like standalone online resources and school information sessions.

To build their strengths, we need interventions that are responsive to local circumstances, culturally appropriate, and built on positive and trusting relationships.

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

Sarah Davies, CEO, [redacted]
or
Ariana Kurzeme, Director, Policy & Prevention, [redacted]

[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] Graham and Sahlberg, 'Growing Up Digital Australia'
[4] DQ Institute, 'Child Online Safety Index 2020: Australia', https://live.dqinstitute.org/impact-measure/#cosi_page
[5] Headspace, 'National Youth Mental Health Survey 2020: Experiences of cyberbullying over time', 2020, https://headspace.org.au/our-impact/evaluation-research-reports/
[6] DQ Institute, 'Child Online Safety Index 2020: Australia'
[7] Australian Centre to Counter Child Exploitation, 'Online Child Sexual Exploitation', Research Report, February 2020, https://www.accce.gov.au/resources/research-and-statistics
[8] J. Thomas, J. Barraket, S. Parkinson, C. Wilson, I. Holcombe-James, J. Kennedy, K. Mannell, A. Brydon, 'Australian Digital Inclusion Index: 2021,' Melbourne, RMIT, Swinburne University of Technology, and Telstra, 2021, https://www.digitalinclusionindex.org.au/download-reports/
[9] Adrienne Katz and Dr Aiman El Asam, 'Refuge and Risk: Life Online For Vulnerable Young People', Internet Matters, 2021, https://www.internetmatters.org/about-us-3/refuge-and-risk-report/
[10] 5Rights Foundation, 'Pathways: How digital design puts children at risk', 2021, https://5rightsfoundation.com/uploads/PathwaysSummary.pdf
[11] Ofcom, 'Online Nation: 2021 Report, UK', 2021, https://www.ofcom.org.uk/__data/assets/pdf_file/0013/220414/online-nation-2021-report.pdf; Office of the eSafety Commissioner, 'State of Play: Youth, Kids and Digital Dangers,' 3 May 2018 https://www.esafety.gov.au/sites/default/files/2019-10/State%20of%20Play%20-%20Youth%20kids%20and%20digital%20dangers.pdf; Justin Patchin, 'Teens Talk: What Works to Stop Cyberbullying,' Cyberbullying Research Centre, https://cyberbullying.org/teens-talk-works-stop-cyberbullying
[12] For example Ofcom, 'Children's Media Lives - Wave 6', 2020, https://www.ofcom.org.uk/__data/assets/pdf_file/0021/190524/cml-year-6-findings.pdf
[13] Attorney-General's Department, 'Social Media (Anti-Trolling) Bill,' 2021, https://www.ag.gov.au/legal-system/social-media-anti-trolling-bill

[14] eSafety Commissioner, 'Safety By Design: Principles and Background', https://www.esafety.gov.au/about-us/safety-by-design/principles-and-background
[15] Australian Government Attorney-General's Department, 'Explanatory paper: Privacy Legislation Amendment (Enhancing Online Privacy and Other Measure) Bill 2021', October 2021; Parliament of the Commonwealth of Australia, Exposure Draft: Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021
[16] United Nations Convention on the Rights of the Child, 'General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)', 29 May 2013; United Nations Convention on the Rights of the Child, General comment No.25 on children's rights in relation to the digital environment, 2 March 2021
[17] From United Nations Convention on the Rights of the Child, 1990, https://www.ohchr.org/en/professionalinterest/pages/crc.aspx . Also United Nations Convention on the Rights of the Child, 'General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)', 29 May 2013, https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf
[18] Alannah & Madeline Foundation, submission to the Draft Online Safety (Basic Online Safety Expectations) Determination 2021, October 2021
[19] Australian Human Rights Commission, 'National Principles for Child Safe Organisations', 2019, https://childsafe.humanrights.gov.au/national-principles
[20] U.K. Information Commissioner's Office, 'Age appropriate design: a code of practice for online services', https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/
[21] United Nations Convention on the Rights of the Child, 'General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration'
[22] United Nations Convention on the Rights of the Child, 'General comment No.25 on children's rights in relation to the digital environment', 2 March 2021, https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx
[23] eSafety, 'Safety by design: principles and background'
[24] The Hon. Scott Morrison, Prime Minister, the Hon. Paul Fletcher, Minister for Communications, Urban Infrastructure, Cities and the Arts, the Hon. Luke Howarth MP, Assistant Minister for Youth and Employment Services, Joint Media Release, 'A voice for young people on online safety,' 15 December 2021
[25] For example, 5Rights Foundation, 'Tick to Agree: Age appropriate presentation of published terms,' September 2021, https://5rightsfoundation.com/TicktoAgree-Age_appropriate_presentation_of_published_terms.pdf; Global Kids Online, 'Children globally rely on the internet during Covid19,' 23 April 2021, http://globalkidsonline.net/covidunder19-summit/ ; Global Kids Online, 'Global Kids Online: Comparative Report', UNICEF Office of Research – Innocenti, 2019, https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html ; S. Livingstone, M. Stoilova, and R. Nandagiri, 'Children's data and privacy online: Growing up in a digital age. An evidence review, London: London School of Economics and Political Science, 2019, https://eprints.lse.ac.uk/101283/ ; Mariya Stoilova, Sonia Livingstone, Rishita Nandagiri, 'Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy,' *Media and Communications*, 8(4), Sep 2020; D. Smahel, H. Machackova, G. Mascheroni, L. Dedkova, E. Staksrud, K. Ólafsson, S. Livingstone and U. Hasebrink, 'EU Kids Online 2020: Survey results from 19 countries,' 2020, https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/eu-kids-online-2020
[26] Parliament Of The Commonwealth Of Australia, 'Protecting the age of innocence: Report of the inquiry into age verification for online wagering and online pornography,' House of Representatives Standing Committee on Social Policy and Legal Affairs, February 2020. Also Simone van der Hof, 'Age assurance and age appropriate design: what is required?,' 17 Nov 2021, LSE, https://blogs.lse.ac.uk/parenting4digitalfuture/2021/11/17/age-assurance/
[27] United Nations Convention on the Rights of the Child, General comment No.25 on children's rights in relation to the digital environment, 2 March 2021 (para 73)
[28] General Data Protection Regulation, 'What is GDPR, the EU's new data protection law?', https://gdpr.eu/what-is-gdpr/
[29] 5Rights Foundation, ''But how do they know it is a child?' Age Assurance in the Digital World', https://5rightsfoundation.com/in-action/but-how-do-they-know-it-is-a-child-age-assurance-in-the-digital-world.html

[30] For more information, see eSafety, 'Safety by Design: Principles and background'
[31] Office of the eSafety Commissioner, 'State of Play: Youth, Kids and Digital Dangers'
[32] United Nations Convention on the Rights of the Child, 'General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)', 29 May 2013
[33] United Nations Convention on the Rights of the Child, 'General comment No.25 on children's rights in relation to the digital environment', 2 March 2021
[34] Consumer Policy Research Centre, 'CPRC 2020 Data and Technology Consumer Survey', 2020 https://cprc.org.au/publications/cprc-2020-data-and-technology-consumer-survey/; Office of the Australian Information Commissioner, 'Australian Community Attitudes to Privacy Survey 2020,' 2020, https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page
[35] Australian Competition & Consumer Commission (ACCC), 'Digital Platforms Inquiry: Final Report', June 2019 https://www.accc.gov.au/focus-areas/digital-platforms
[36] 5Rights Foundation, 'Disrupted Childhood: The cost of persuasive design,' June 2018 https://5rightsfoundation.com/uploads/5rights-disrupted-childhood-digital-version.pdf; 5Rights Foundation, 'Pathways: How digital design puts children at risk,' July 2021, https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf
[37] Australian Government Attorney-General's Department, 'Explanatory paper: Privacy Legislation Amendment (Enhancing Online Privacy and Other Measure) Bill 2021', October 2021, pp.9-10
[38] Parliament of the Commonwealth of Australia, Exposure Draft: Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, p.10, 12-13
[39] ACCC, 'Digital Platforms Inquiry: Final Report'
[40] 5Rights Foundation, 'Tick to Agree: Age appropriate presentation of published terms'
[41] See for example 5Rights Foundation, 'Tick to Agree: Age appropriate presentation of published terms', and the UK Age Appropriate Design Code.
[42] eSafety Commissioner, 'Safety By Design: Principles and Background'
[43] 5Rights Foundation, 'Tick to Agree: Age appropriate presentation of published terms'
[44] Dr Anthea Rhodes, 'Screen time and kids: What's happening in our homes?', RCH Child Health Poll, 2017
[45] Internet Matters, 'We need to talk about pornography', https://www.internetmatters.org/about-us-3/we-need-to-talk-about-pornography-report/ ; Netsafe NZ, 'Children's exposure to sexually explicit content: Parents' awareness, attitudes and actions,' Dr Edgar Pacheco and Neil Melhuish, 2018, https://www.netsafe.org.nz/wp-content/uploads/2018/12/Parents-and-Pornography-2018_10Dec2018.pdf
[46] Adrienne Katz and Aiman El Asam, 'Look at me: Teens, sexting and risks', Internet Matters, 2020, https://www.internetmatters.org/about-us-3/sexting-report-look-at-me/; Adrienne Katz and Dr Aiman El Asam, 'Refuge and Risk: Life Online for Vulnerable Young People', Internet Matters, 2021; Adrienne Katz and Aiman El Asam, 'Vulnerable Children in a Digital World', Internet Matters 2019, https://www.internetmatters.org/wp-content/uploads/2019/04/Internet-Matters-Report-Vulnerable-Children-in-a-Digital-World.pdf