



**Australian
Human Rights
Commission**

**National Children's Commissioner
Anne Hollonds**

24 January 2022

Committee Chair

Department of the House of Representatives

Select Committee's Inquiry into Social Media and Online Safety

Dear Committee Chair,

Submission to the House Select Committee on Social Media and Online Safety

Thank you for the opportunity to contribute to the Committee's Inquiry into Social Media and Online Safety, and for inviting me to attend the public hearing as a witness on Friday 21 January 2022. In lieu of attending this hearing, I wanted to comment on the Inquiry's Terms of Reference as they pertain to children's rights.

As National Children's Commissioner, I am in charge of promoting and protecting the human rights of children in Australia. It is my job to monitor how well our policies and services are supporting the rights and wellbeing of all our children, especially those who are living with disadvantage and are likely to miss out on the conditions that support a good childhood. To this end, I welcome this inquiry that seeks to ensure that the online environment is safe for all children.

I am responsible for:

- advocating nationally for the rights and interests of children and young people
- promoting children's participation in decisions that impact on them
- providing national leadership and coordination on child rights issues
- promoting awareness of and respect for the rights of children and young people
- undertaking research about children's rights
- examining laws, policies and programs to ensure they protect and uphold the rights of children and young people.

Australian Human Rights Commission
National Children's Commissioner
Anne Hollonds

I note that submissions to this Inquiry have been made by my colleagues at the National Mental Health Commission and the eSafety Commissioner, as well as the Office of the Children's Commissioner Northern Territory. I have also written to the Attorney General's Department in 2021 about the Online Privacy Bill, in regard to the underlying principles that should inform privacy reform for social media companies.

It is my understanding from reviewing the Terms of Reference that this present Inquiry has a broad focus. Within my remit as National Children's Commissioner, I see it appropriate that I suggest overall principles to guide recommendations rather than responding to specific matters relating to regulation and industry practice. As such, I have responded to two relevant Terms of Reference: (a) and (h) as set out below:

(a) The range of online harms that may be faced by Australians on social media and other online platforms, including harmful content or harmful conduct

The online environment is ubiquitous for children growing up today and it is necessary to consider the benefits as well as mitigate the risks of online platforms. The online environment poses both risks to children, and opportunities for children to realise their rights and contribute to the world around them. Both the risks and opportunities need to be explored when developing law, policies and codes.

Risks include:

- Risks to children's right to life, survival, and development, including but not limited to: exposure to online exploitation or abuse; harassment, and cyberbullying; targeting by criminal entities; and exposure to violent or sexual content.¹ For example, early and frequent exposure to online pornography has been connected to a range of harms affecting children. Nearly half of children between the ages of 9–16 experience regular exposure to sexual images.² Studies have found that 'pornography both contributes to and reinforces the kinds of social norms and attitudes that have been identified as drivers of violence against women',³ and that viewing pornography is 'associated with unsafe sexual health practice'.⁴
- Risks to privacy associated with the collection and aggregation of children's personal data, and the sale and misuse of data, including

through profiling techniques utilised by state and commercial entities that target children for a range of purposes, including marketing.

- Potential for discrimination through exclusion from online services; subjection to profiling or targeting by AI systems on the basis of biased or unfairly obtained data; and receipt of hateful content on online platforms.⁵
- Automated search and information filtering that 'prioritise paid content with a commercial or political motivation' and impinge upon children's autonomy and right to access information.⁶
- Behavioural techniques designed to increase engagement with platforms, which 'trigger impulsive behaviours, influence decision-making, spark fear of exclusion and override privacy concerns'.⁷

Positive elements include:

- Opportunities for children and young people to exercise their right to freedom of expression, which includes the right to access information. Regarding the latter, General Comment 25 of the Committee on the Rights of the Child notes that 'information and communications media, including digital and online content, perform an important function'. It is important that access restrictions and content filtering mechanisms do not impede upon this right, and that 'diverse and good quality information' is readily available online.⁸
- Opportunities for personal development. Children should be free to grow and explore in accordance with their age and development stage, without unnecessary or disproportionate surveillance or interference by commercial and state entities, or by their parents. Social media, for better or worse, is a large part of how children socialise and develop their identity in today's age. The Special Rapporteur on the right to privacy found that 'increasingly, self-esteem, and self-concept, necessary for the formation of personality and identity, are constructed digitally'.⁹ This has only been exacerbated by the COVID-19 pandemic—'daily active accounts for Facebook's Messenger Kids grew by 350 percent from March to Sept 2020'.¹⁰
- Opportunities for children to exercise their right to health and education. For example, children reported to the Committee on the Rights of the Child that they 'valued searching online for information and support relating to health and well-being, including on physical, mental and sexual and reproductive health, puberty, sexuality and conception'.¹¹

(h) any other related matter.

(i) *Overarching Human Rights Principles*

In this response, the Commission focuses solely on the implications for children's rights, and outlines the high-level human rights principles that should be applied by social media companies and government.

The best interests of the child is central as a key principle of reform

It is important that a coordinated approach to reform is undertaken, and that the best interests of the child is actively prioritised across *all* these regulatory processes. The Commission therefore recommends that the principle of the 'best interests of the child' should be used as the primary test across all instruments affecting children online, ideally with a positive duty on relevant actors to demonstrate that the principle is applied as a priority through both the development and application of the instruments. Key considerations for prioritising the best interests of children in the online context are as follows.

The Convention on the Rights of the Child (CRC) requires that the best interests of every child is a primary consideration in actions relating to all aspects of the digital environment.¹² When considering the best interests of the child, regard should be had to 'all children's rights, including their right to seek, receive and impart information, to be protected from harm and to have their views given due weight' in addition to ensuring transparency over the criteria applied to determine best interests.¹³ Where rights are limited to protect children from online harms, limitations must be lawful, necessary and proportionate.

Maximising children's privacy and securing their personal data is itself a 'crucial means of acting in their best interests'.¹⁴ Children's privacy should not be construed narrowly as relating only to data protection measures, and should recognise the importance of children's autonomy and choice over their private lives. Children should have access to complaint and remedial mechanisms if their right to privacy is breached, and child-friendly information about recourses should be readily accessible.¹⁵ To secure children's privacy it is necessary to integrate human rights-by-design into digital products and services and to require high default privacy settings for *all* users of online services.¹⁶

Australian Human Rights Commission
National Children's Commissioner
Anne Hollonds

A best interests approach may require implementing clear boundaries to prevent practices that both infringe upon children's rights and are contrary to their best interests, including by curtailing routine and indiscriminate digital surveillance measures.¹⁷ Practices such as online tracking, profiling, behavioural monitoring and 'nudging', the collection of biometric and geolocation data from children, automated decisions affecting children and the unjustifiable sale or transfer of children's personal data to third parties should be banned or heavily restricted to protect children's rights. For example, among other things, General Comment 25 requires parties to:

[P]rohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children.¹⁸

It is important that best interests considerations are not merely based on assumptions about what is in the interests of children, and that their views are actively considered.¹⁹ In this regard the Special Rapporteur notes that 'adult's interpretation of children's privacy needs can impede the healthy development of autonomy and independence, and restrict children's privacy in the name of protection'.²⁰ He elaborates:

While children's dependency, hence vulnerability, can result in risks, risk does not equate to harm and navigating some risk is necessary for children to develop resilience and coping skills. Defining children by their vulnerability only, without consideration of their capacity or potential, is likely to result in overly protectionist agendas, potentially harmful to children's personality.²¹

In order to ensure that reform is not based on assumptions about children's best interests, and that children's views are properly considered, children should have an opportunity to participate in the process of developing [reform].

The Inquiry is an opportunity to ensure that the reform is informed by human rights principles, and in particular, the CRC. This will provide a framework for assessing the practices of social media companies against Australia's obligations, and will embed a coherent process for balancing countervailing rights and

Australian Human Rights Commission
National Children's Commissioner
Anne Hollonds

interests through an established proportionality test, ensuring that the protection of children's rights are prioritised above other agendas.

In this submission, the Commission draws on Australia's international obligations under the CRC and the International Convention on Civil and Political Rights (ICCPR). The Commission strongly encourages reforms to be developed in light of General Comment 25 by the Committee on the Rights of the Child, dealing with children's rights in relation to the digital environment, and the 2021 Report of the Special Rapporteur on the Right to Privacy on children's privacy (Special Rapporteur). Similar codes in other jurisdictions are also instructive. In particular the Commission draws attention to the United Kingdom's Age Appropriate Design code of practice (UK Code), which sets out 15 standards for online platforms based on the CRC.²²

Children's privacy in context

The primary instrument enshrining children's rights is the CRC, which Australia has ratified. Article 16 of the CRC protects the right to privacy. It states that:

- (1) No child shall be subject to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful interference with his or her honour and reputation.
- (2) The child has the right to protection of the law against such interference or attacks.

Of relevance here are considerations around 'information privacy', which protects information created *about* children.²³ This may include information about 'children's identities, activities, location, communication, emotions, health and relationships'.²⁴ As the Committee on the Rights of the Child has recognised in General Comment 25, there are significant implications for children's privacy associated with increasingly 'routine' practices that include 'automated data processing, profiling, behavioural targeting, mandatory identity verification, information filtering and mass surveillance'.²⁵

Children's right to privacy may only be limited where the interference is not arbitrary or unlawful, and

Any such interference should ... be provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimization, be proportionate

Australian Human Rights Commission
National Children's Commissioner
Anne Hollonds

and designed to observe the best interests of the child and must not conflict with the provisions, aims or objectives of the Convention.²⁶

Children's rights are universal, indivisible, interdependent and interrelated.²⁷ The right to privacy is necessary for the protection of other rights, including rights to freedom of expression, thought and association (Articles 13, 14, 15 of the CRC). The Special Rapporteur has observed that 'the foundations of future intellectual, emotional and sexual life are developed in childhood and adolescence, aided by the conditions of a private life'.²⁸ As such, privacy is essential to children's development.

However, children's privacy is more complex than adult's right to privacy, due to: the particular vulnerability of children; parental rights to raise their child; and children's changing capacities and development that affect, for example, the application of consent mechanisms. The CRC provides State parties and parents with the requirement, where necessary, to restrict children's enjoyment of privacy in line with the child's evolving capacity (Article 5) to secure the best interests of the child (Article 3).²⁹ Article 16 also interacts with obligations to protect children from violence and ill-treatment, and to secure their survival (Articles 19, 37, 6).

Article 12 'enables and informs' the child's rights under Article 16, requiring that children's views are given weight on an individual basis, and '[presenting] children with an opportunity to identify issues which may interfere with their right to privacy'.³⁰ Children should be provided with an opportunity to participate in legislative and policy development processes on issues that affect children's privacy, including those conducted by the business community, and to have an active say in their individual lives over how their privacy is treated in a given circumstance.³¹

(ii) *The specific principles that should inform age verification and parental consent mechanisms.*³²

The Terms of Reference of the Inquiry explicitly refer to identity verification and age assurance processes in (b)(iii), as well as parental consent. The following section addresses this. If the Committee is considering such tools, they should take into account the following rights-based considerations.

Proposals to include age verification and parental consent mechanisms are designed to ensure that children access age-appropriate material and prevent

them from being exposed to privacy infringements and harmful online practices. The CRC provides guidance on this front.

When determining what is 'age appropriate', the evolving capacities of the child must be taken into account. As noted by the Special Rapporteur, 'children vary enormously in their physical, intellectual, social and emotional capacity', and online risks change based on their stage of development, individual circumstances and environmental factors – and are not best determined by reference chronological age alone.³³ A blanket or blunt approach to age restrictions and consent may therefore not be necessary or desirable. Teenagers in their mid-teens will have a greater need for privacy and a stronger ability to understand consent processes than younger children. The UK Code provides useful guidance in this regard, reflecting that different approaches are required for different age ranges, promoting a flexible approach.³⁴

The Special Rapporteur cautioned that the 'notion of age-appropriateness sits uneasily with the principle of evolving capacity' and recommended that State parties 'adopt age-appropriate standards as a regulatory instrument only with the greatest of caution when no better means exist'.³⁵ He made the following points in this regard:

- Material may be age appropriate and still harmful to children and their rights. The mechanism may protect and empower a child when individualized, but may not meet the needs of a cohort of children given the considerable variation in intellectual and emotional development among children of the same age.
- As a generic threshold, age appropriateness poses inequities for children of differing capacity and is a crude measure of their evolving capacities, potentially constraining the development of their personalities and the autonomous exercise of their rights, and is possibly discriminatory.
- When age is the criterion for accessing services, verifiable identity documents are required, raising concerns around security, prescriptive approaches and the lack of age assurance standards, tools and industry certification schemes. Others indicate that age verification processes can be delivered in a way that is compatible with privacy.³⁶

The third point is particularly relevant to a human rights proportionality assessment in relation to age-verification. Age-verification techniques themselves pose risks for children's privacy and data protection, along with the

privacy of *all* users of online platforms who will also be required to verify their ages before use. Age verification measures link a person's identity to their online activity. This can create prospects for surveillance, security breaches, leaks, data sales or criminal misuse of identifying information.³⁷ All age verification techniques must be consistent with privacy and data protection principles; and if this cannot be guaranteed, other approaches to protecting children from online harms may be preferable.

The use of age-verification techniques should also be context-specific. Appropriate techniques may be required where age-verification is necessary to prevent children from engaging in illegal activity, such as buying weapons, alcohol or participating in online gambling,³⁸ and where the potential for harm is high, like pornography websites, but may be disproportionate in other contexts. The UK Code adopts a flexible approach, noting a number of potential age-verification measures, of varying levels of strength, ranging from 'self-declaration' to 'hard-identifiers' (the latter requiring the provision of ID). Notably, it recommends against giving users no choice but to provide hard identifiers:

This is because some children **do not have access to formal identity documents** and **may have limited parental support**, making it difficult for them to access age-verified services at all, even if they are age-appropriate. **Requiring hard identifiers may also have a disproportionate impact on the privacy of adults.**³⁹

The Commission is aware that the eSafety Commissioner is developing a Restricted Access System and a 'roadmap' to age verification for online pornography, in parallel to these privacy reforms.⁴⁰ It is worth noting that the UK abandoned its own plans to adopt nationwide age verification for pornography websites, due to concerns about privacy and data security, and technical challenges.⁴¹ Ideally, the eSafety Commissioner will link and coordinate with the work of Privacy Commissioner and other privacy stakeholders involved in the Privacy Act Review to ensure that an appropriate balance is struck to protect both children's and adult's privacy; and that a range of options are explored that prevent harm to children associated with exposure to pornography without compromising privacy, such as education measures. In this regard Our Watch has observed that 'simplistic approaches that seek to simply ban or discourage [children] from watching [porn] are unlikely to be effective'.⁴²

The provision of parental consent must similarly be approached from a nuanced perspective in light of children's evolving capacity, and in context with other

Australian Human Rights Commission
National Children's Commissioner
Anne Hollonds

rights-protective measures. The Commission notes the following comment by the Special Rapporteur in this regard:

Consent ... neither necessarily expresses a child's autonomy nor protects it, particularly where power imbalances exist. Furthermore, parental consent may not always be in the best interests of the child or aligned to the child's views.⁴³

Additionally:

As they mature, children desire and require privacy, not only from schools, businesses and governments, but also from their parents. That need grows as children grow. While children between the ages of 5 and 7 generally do not consider parental monitoring of their online activities as a violation of privacy, teenagers aged between 15 and 17 are often concerned about parental and school monitoring.⁴⁴

A requirement for parental consent for teenagers aged 15–16 may be overly protective at the expense of their privacy needs. The reality that many children do not have parental support, or have parents who lack technological literacy should also be factored into consent considerations, to avoid situations where children are excluded from opportunities to engage online, in circumstances where it is in their best interests to have those opportunities.

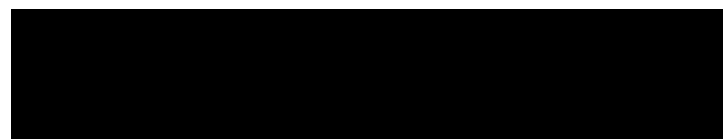
Regardless of the approach adopted, all consent processes should be accompanied by accessible, child-friendly information.⁴⁵ This information should be tailored to accommodate users in different age ranges.⁴⁶

Alternative and additional approaches to protecting children from online harm and securing their privacy should be considered alongside age verification and parental consent. These include stronger privacy protections for *all* users such as default privacy settings that are opt-in; requiring websites to be easily filterable by parental control software to better protect younger children;⁴⁷ and providing education on human rights, online safety and privacy for parents and children.

I would like to provide what assistance I can to the Committee, and would be happy to expand on these points and appear at a later date if the Committee intends to have further public hearings.

Yours sincerely

Australian Human Rights Commission
National Children's Commissioner
Anne Hollonds



Anne Hollonds
National Children's Commissioner



¹ Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [14]-[15].

² Antonia Quadara, Alissar El-Murr and Joe Latham, *The effects of pornography on children and young people* (Australian Institute of Family Studies, December 2017)
<<https://aifs.gov.au/publications/effects-pornography-children-and-young-people-snapshot>>.

³ Our Watch, *Pornography, young people and preventing violence against women* (2020), 14
<<https://media-cdn.ourwatch.org.au/wp-content/uploads/sites/2/2020/11/20022415/Pornography-young-people-preventing-violence.pdf>>.

⁴ Antonia Quadara, Alissar El-Murr and Joe Latham, *The effects of pornography on children and young people* (Australian Institute of Family Studies, December 2017)
<<https://aifs.gov.au/publications/effects-pornography-children-and-young-people-snapshot>>.

⁵ Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [9]-[11].

⁶ Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [53].

⁷ Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [91].

⁸ Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [50] and [53].

⁹ Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [88].

¹⁰ Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [87].

¹¹ Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [50].

¹² Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [12]-[13].

¹³ Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [13].

¹⁴ Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [116].

¹⁵ Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [127].

¹⁶ Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [127].

¹⁷ Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [75].

¹⁸ Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [42].

¹⁹ Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [16]-[18].

²⁰ Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [80].

²¹ Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [118].

²² These cover: best interests of the child; data protection impact assessments; age appropriate application; transparency; detrimental use of data; policies and community standards; default settings; data minimisation; data sharing; geolocation; parental controls; profiling; nudge

techniques; connected toys and devices; and online tools. UK Information Commission Office, *Age appropriate design: a code of practice for online services* (September 2020).

²³ John Tobin (ed), *The UN Convention on the Rights of the Child* (OUP, 2019), 570.

²⁴ Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [68].

²⁵ Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [68].

²⁶ Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [69].

²⁷ Committee on the Rights of the Child, General Comment No. 16 (2013) CRC/C/GC/16 [12].

²⁸ Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [72].

²⁹ John Tobin (ed), *The UN Convention on the Rights of the Child* (OUP, 2019), 555; Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [78].

³⁰ John Tobin (ed), *The UN Convention on the Rights of the Child* (OUP, 2019), 55. See also Committee on the Rights of the Child, General Comment No. 25 (2021) UN Doc CRC/C/GC/25 [17-18].

³¹ Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [17].

³² Please note, this response also partially addresses the Terms of Reference (b)[iii] and (c).

³³ Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [96].

³⁴ UK Information Commission Office, *Age appropriate design: a code of practice for online services* (September 2020), 39-41, 61-62, 74-75, 81-82, 96-100.

³⁵ Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [127].

³⁶ Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [127].

³⁷ 'Restricted Access Systems', *Digital Rights Watch* (Webpage, September 2021) <<https://digitalrightswatch.org.au/2021/09/21/submission-restricted-access-system/>>.

³⁸ Committee on the Rights of the Child, General Comment No. 25 (2021) UN Doc CRC/C/GC/25 [114].

³⁹ UK Information Commission Office, *Age appropriate design: a code of practice for online services* (September 2020) 33.

⁴⁰ 'Age Verification' *eSafety Commissioner* (Web page) <<https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification>>.

⁴¹ Jim Waterson, 'UK drops plans for online pornography age verification system' *The Guardian* (online, 17 October 2019) <<https://www.theguardian.com/culture/2019/oct/16/uk-drops-plans-for-online-pornography-age-verification-system>>.

⁴² Our Watch, *Pornography, young people and preventing violence against women* (2020), 14 <<https://media-cdn.ourwatch.org.au/wp-content/uploads/sites/2/2020/11/20022415/Pornography-young-people-preventing-violence.pdf>>.

⁴³ Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [120].

⁴⁴ Human Rights Council, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on Artificial intelligence and privacy, and children's privacy (2021) UN Doc A/HRC/46/37 [83].

⁴⁵ Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, UN Doc CRC/C/GC/25 [25].

⁴⁶ See examples of age-tailored approaches in the UK Code: UK Information Commission Office, , *Age appropriate design: a code of practice for online services* (September 2020), 96-100.

⁴⁷ 'Restricted Access Systems', *Digital Rights Watch* (Webpage, September 2021) <<https://digitalrightswatch.org.au/2021/09/21/submission-restricted-access-system/>>.