



Submission to the United Nations Special Rapporteur on Children's Right to Privacy

September 2020



251 Morphett Street, Adelaide, SA 5000
GPO BOX 1146, Adelaide SA 5001
08 8226 3355 | commissionercyp@sa.gov.au

Introduction

As South Australia's Commissioner for Children and Young People, my mandate under the *Children and Young People (Oversight and Advocacy Bodies) Act 2016* is to advocate for the rights, interests and wellbeing of all children and young people in South Australia. It is also my role to ensure that the State, at all levels of government, satisfies its international obligations under the United Nations Convention on the Rights of the Child.

I welcome the Special Rapporteur's investigation and the opportunity to contribute to a better understanding of children's right to privacy. Today's children and young people have been described as the "most watched-over generation in memory".ⁱ This raises many complex issues and questions about a child's right to privacy.

Since 2017, I have spoken with thousands of children and young people across South Australia about what is important to them. They have consistently told me that the online world is just another place where they live their lives, where they learn, play, connect with others and with services, make and create, relax, and share and receive information.

Where children and young people see their online and offline lives as inextricably linked, adult decision makers and the media often treat the digital and offline worlds as separate. This is evident in discussions about a child's right to privacy, which are often primarily confined to online environments.

While much of the discussion about children's privacy focuses on being wary of and protecting children's privacy against threats from strangers, predators and companies online, some of the most common breaches of privacy can come from those closest to children and who children should be able to trust the most: parents and schools. These are the people and institutions most responsible for educating and supporting the healthy development of children, including the growth of their independence.

For many parents across Australia, monitoring children's online behaviour and (over)sharing information about children online have become standard behaviours. These actions are often framed in terms of safety and protection and hallmarks of "good parenting". Schools have also increasingly become sites of surveillance, with recent South Australian legislation granting school staff the authority to search a student's belongings as an appropriate form of "maintaining order and discipline".

This submission focuses on these issues, related research and research gaps that highlight the difficult balance between protection and control, the inadequacy of adult-centred conceptions of and assumptions about privacy, and the need for child-centred rights-based approaches to privacy in all settings, both online and offline.

Balancing risk with opportunity and agency

The "three Ps" that underpin the United Nations Convention on the Rights of the Child (UNCRC) are provision, protection and participation. When it comes to online safety, there is a tendency to disproportionately emphasise protection.

Yet a focus almost exclusively on risks and protection can lead to approaches that heavily monitor or restrict children's behaviour. Such approaches can undermine a child's right to privacy as well as their rights to access information, to freedom of expression and participation and access to education, justice and healthcare.

While there are indeed very real risks associated with technology, a growing body of research suggests that risk does not equate to harm and that navigating some level of risk allows children to foster resilience and develop skills to minimise the potentially negative impacts of engaging online.ⁱⁱ

This is in line with what children and young people are telling me: that they want the tools to feel empowered to navigate the digital world confidently and creatively.

Children and young people identify trust as fundamental to strong communities as well as their own wellbeing, safety and privacy. One of their biggest concerns online is "feeling that they can trust the sites they visit to not try to take advantage of them". They want to be able to trust adults, institutions and technology companies, service providers and websites to not take advantage of them and their personal information.

"We need trust to engage, listen + participate + make sure we are constantly working towards the best outcomes for all. Without trust, there is only apathy + paranoia, meaning we'd have a very unhappy community."

"Educate children and young people on what their rights are, what violations of those rights may look like, while encouraging them to have confidence in their autonomy and in their ability to identify when they feel uncomfortable."

Children and young people see risks to their privacy coming from within their own "sphere" (family members and education institutions) as well as from outside their "sphere" (governments and commercial interests).

This highlights the need for a balanced approach that protects children and their rights from harm while also empowering them to feel confident and embrace opportunities online.

The inadequacy of adult assumptions about children's privacy and the need for child-centred approaches

There is a significant lack of research about the rights, needs and interests of children in privacy and their perceptions of privacy. Where child-focused research does exist, policymakers often overlook the findings when making decisions and laws.

We urgently need to understand privacy through children's eyes and enact child-centred approaches and definitions of rights, risks and opportunities.

Dominant conceptions of privacy treat it as an issue only relevant (or primarily relevant) to adults. However, applying adult-centred conceptions of privacy to children is inherently flawed because:

- Adult-centred understandings of privacy often focus on the divisions between the individual and others. Given that children are inherently connected to and dependent on others, this applies awkwardly (if at all) to children.

- Children’s needs, including their need for privacy, differ from adults.
- Younger children’s needs differ from needs of older young people.

The work of the 5Rights Foundation provides a useful framework to underpin a better understanding of children’s right to privacy. 5Rights have articulated children’s existing rights for the digital environment, acknowledging that “if children and young people’s rights are not upheld in one environment, they are denuded in all environments”:

1. **Right to remove** or easily edit content they have created or data that refers to them.
2. **Right to know** where their information is going, who is using it or profiting from it, what their information is being used for, and whether it is being copied, traded or sold.
3. **Right to safety and support** that is age-appropriate and easily accessible and understandable by children and young people.
4. **Right to informed and conscious use** that empowers children and young people to benefit from creative places online but also to have support to easily disengage.
5. **Right to digital literacy** where children and young people learn how to be digital makers and digital thinkers as well as consumers and to critically understand the structures and norms of the digital world.ⁱⁱⁱ

Parental surveillance: mistaking control for care?

In the context of fears about online risks and cybersafety, there is increasing pressure on parents to track and monitor their children online, and this surveillance is often framed in terms of care, protection and “good parenting”.

When parental control is synonymous with care, the implications for children’s privacy, wellbeing and autonomy are not well understood. This merits further attention.

A wide variety of “tracking” software and applications are available to parents to monitor their children’s online behaviour, including their children’s location, conversations, posts, and microphones.

Recent international research shows that parental surveillance increases with a child’s age. That is, parental surveillance typically increases at a time when young people are (or should be) becoming more independent.^{iv} Instead of teaching children how to navigate the digital world safely, parental surveillance can undermine a child’s autonomy, privacy and independence.

A poll by the New South Wales Advocate for Children and Young People (ACYP NSW) found that the most popular strategy that parents used to manage their child’s internet use was to friend their child on social media. This was more common than discussing online safety concerns and talking to their child about their use of the internet.

“Sharenting”: children’s right to privacy versus adult’s right to freedom of expression

Parents and parents-to-be are increasingly using the internet, particularly social media, to post stories, information, pictures, videos and other updates about their children online. Known as

“sharenting” (a combination of the words “sharing” and “parenting”), this practice shapes a child’s online identity long before the child has the capacity to give consent or begins creating their own digital footprint. It also breaches a child’s right to privacy.

A 2018 study by the London School of Economics revealed that three in four parents who regularly use social media, posted pictures and videos of their kids online. The study found that the parents who were most likely to engage in “sharenting” were the same parents who reported being concerned about privacy.^v While many parents can “sharent” with caution and the best of intentions, it is still seen as solely the adult’s decision to make.

When parents engage in “sharenting”, their right to share information competes with their child’s right to privacy. If a balance cannot be established between both of these important rights, this can create tension. If a parent shares something that their child would prefer to keep private, this can lead to social discomfort and feelings of betrayal, which may impact trust between children and parents. These psychosocial impacts sit alongside concerns that “sharenting” can publicly disclose identifying information about children, such as where they live or play.

While sharing certain milestones or information is not necessarily harmful, research shows that children do not always enjoy being featured in their parent’s online profiles. In a survey of 10–12 year olds in 2017, more than 1 in 4 said that they felt anxious, embarrassed or worried when their parents posted pictures of them online.^{vi}

Where parents do not ask their children for permission or children are unable to consent, children may grow up and be shocked to find that they already have a digital footprint that can be difficult to change or remove.

The complexity of this issue highlights the need for parents to speak often and openly with their child about what they’re sharing. This is especially important given that one of the main reasons that 10–12 year olds gave for being unhappy about “sharenting” was “not being asked first”. My [“sharenting” fact sheet](#) outlines ten key points for parents to consider when navigating their own and their child’s information online.

Privacy at school: mistaking control for “maintaining discipline and order”?

Researchers have noted that there are often lowered expectations of privacy at school given the responsibility of schools to provide children with a safe school environment.^{vii} In the same way that parents have always been able to read their child’s diaries or search their school bags, teachers have been able to read out students’ private note in class. While it is known that punitive approaches do not engender trust and respect between teachers and students, evidence suggests that schools have become sites of increasing surveillance.

Where South Australia has no state privacy legislation, Australia’s Commonwealth *Privacy Act 1988* only covers Commonwealth agencies and private schools. It does not cover public schools or state or territory government agencies. Although the [Information Privacy Principles](#) apply to the public education system, a child’s right to privacy at school is not legally protected in South Australia.

On the contrary, section 29 of South Australia’s most recent piece of education legislation, the [Education and Children’s Services Regulations 2020](#), gives school staff and principals the

authority to search students' bags or other property based merely on reasonable belief as a means of "maintaining order and discipline". There is a penalty of \$100 for students who fail to comply.

A similarly punitive approach is evident in the bans on mobile phones in schools across Australia. Although the South Australian government has not banned mobile phones at government schools in South Australia, it has indicated it is considering the issue and monitoring outcomes in Victoria, where a blanket ban has been imposed.

While concerns about privacy have been used to support a ban, there is also evidence that bans may raise more concerns. For example, if phones are taken away as punishment or "behaviour management", where will the devices go if they are kept on-site and what measures are in place to protect child's privacy and foster trust?

An independent review into the non-educational use of mobile devices in schools in New South Wales (NSW) found that there was a "mismatch between student and teacher expectations about what constitutes a positive and engaging learning environment".^{viii}

The NSW Review also benefited from the contributions of many young people. Students described how they use their devices to access information that directly relates to their schoolwork, the benefits of using their phones to maintain wellbeing (mindfulness and meditation apps, listening to music), to help concentration in class, to communicate with parents, carers and employers, to monitor healthcare, and for safety.

Where a survey of adults found that 80% of parents supported a mobile phone ban, the unique views of young people painted a more complex picture of the issue. The divergence between adult and child views highlights the need for approaches that capture the complexity of issues related to privacy and are informed by children's perceptions and online and offline experiences.

"I wouldn't trust the school with my phone ... like I don't know them."

– year 9-10

Schools exist to practically equip children with skills they need to navigate their adult lives both online and offline. Given that mobile phone use is a significant and rapidly growing part of everyday life, this office is of the view that restrictions or bans fail to prepare children and young people for their futures.

In 2015, New York City lifted its ban on mobile phones in schools, which had been in place since 2006. The principal of New York's High School of Telecommunication Arts and Technology, Xhenete Shepard highlighted that approaches to technology and to privacy that are based on education and empowerment are more effective and best support child safety:

"Our time is better spent not fighting technology, but rather helping students recognise how to use technology productively and responsibly."^{ix}

The best way forward

We need to empower children through education and respectful conversations and two-way dialogue that respect their rights to privacy and foster confidence and autonomy.

Despite being framed as “protecting” children, many dominant understandings of privacy are entrenched in risk and are based on adult-centred conceptions of privacy. Such approaches commonly serve to control, restrict or punish children and young people. Given the flaws of applying adult assumptions about privacy to children, there needs to be:

- **More opportunities for children and young people of all backgrounds and abilities to be involved in research and in the design and delivery of new frameworks, policies and educational programs about privacy.**

Children and young people’s perceptions and experiences of privacy, both online and offline, capture a more complete and complex picture of privacy. When children and young people are actively consulted and engaged, a sense of shared responsibility and understanding is fostered as well as greater trust between children and young people and others, including their parents and teachers.

- **Education-based approaches have the best chance of striking a balance between children’s rights to protection, provision and participation as well as the balance between children’s rights to privacy and adult rights.**

A 2017 report by Australia’s eSafety Commissioner found that the overwhelming majority of young people (71%) who had negative experiences online turned to their friends and family for informal help. If this is the case, friends and families need to be informed and supported in order to have open conversations with and provide the best possible support to children. Active and shared family screen time should be encouraged for children, parents, carers and families as a way of raising awareness about positive and empowering online interactions. Furthermore, while schools are key gatekeepers of children’s information and privacy alongside parents, school policy rarely reflects this and must change to do so.

- **Greater regulation of companies and a legally enforceable duty of care that places the onus on the companies and service providers to take responsibility for the safety and privacy of their users, particularly children and young people.**

Self-regulation by social media and technology companies has failed and the effectiveness of opt-in tools and filtered services is limited insofar as they place the onus on the public rather than the companies. Nevertheless, given that the online world is an extension of the offline world, technical solutions to issues relating to privacy alone are insufficient.

-
- ⁱ Gabriels, Katleen. “I keep a close watch on this child of mine’: A Moral Critique of Other-Tracking Apps.” *Ethics and Information Technology* 18, no. 3, 2016, 175-184.
- ⁱⁱ Young and Well Cooperative Research Centre, “Children’s Rights in the Digital Age: A download from children around the world,”
- ⁱⁱⁱ 5Rights Foundation, “The 5Rights Framework”, Available at <https://5rightsfoundation.com/about-us/the-5-rights/>.
- ^{iv} Blecher-Prigat, Ayelet. 2019. “Children’s Right to Privacy”, *The Oxford Handbook of Children and the Law*, p. 373.
- ^v London School of Economics, 2018, ‘What do parents think, and do, about their children’s online privacy?’
- ^{vi} BBC Newsround, 7 February 2017. “‘Sharenting’: Are you OK with what your parents post?” Available at <https://www.bbc.co.uk/newsround/38841469>.
- ^{vii} Blecher-Prigat, Ayelet. 2019. “Children’s Right to Privacy”, *The Oxford Handbook of Children and the Law*, p. 373.
- ^{viii} New South Wales Government, 2018. Review into the non-educational use of mobile devices in NSW schools. Available at https://education.nsw.gov.au/about-us/strategies-and-reports/our-reports-and-reviews/mobile-devices-in-schools/review-into-the-non-educational-use-of-mobile-devices-in-nsw-schools#Personal_29
- ^{ix} Tonkin, Casey, 2020. “Four states have banned phones in schools,” *Information Age*, Available at <https://ia.acs.org.au/article/2020/four-states-have-banned-phones-in-schools.html>.