



Law Council
OF AUSTRALIA

Office of the President

16 May 2019

United Nations Committee on the Rights of the Child
Office of the United Nations High Commissioner for Human Rights
Palais Wilson
52 rue des Pâquis
GENEVA SWITZERLAND CH-1201

By email: crc@ohchr.org

Dear Sir/Madam

submission

The Law Council welcomes the opportunity to submit to the United Nations Committee on the Rights of the Child (**UNCRC**) regarding its consultation on a proposed General Comment entitled 'Children's rights in relation to the digital environment'.

The Law Council is grateful for the assistance of its Family Law Section and the Law Society of New South Wales in the preparation of this submission (**attached**).

The Law Council takes this opportunity to outline live issues in the Australian context with respect to children's rights in the digital environment, which may help to inform the UNCRC's General Comment. The attached submission addresses issues relevant to the key groups of rights raised in the UNCRC's Concept Note, and answers questions posed about the obligations and role of States and businesses.

Where relevant, the Law Council draws upon its [Justice Project Final Report](#) findings. The Justice Project was a comprehensive national review into the state of access to justice in Australia focusing on groups experiencing significant disadvantage, released in August 2018. Relevant chapters include those on [Children and Young People](#) and [Legal Services](#). The Law Council also draws upon a number of its previous submissions on children's rights and technology, including its:

- [submission](#) to the Australian Human Rights Commission regarding its consultation on Human Rights and Technology;
- [Alternative Report to the UNCRC](#) regarding Australia's implementation of the Convention on the Rights of the Child;
- [submission](#) regarding the adequacy of existing Commonwealth, state and territory offences to capture cyberbullying;
- [submission](#) regarding the My Health Records Amendment (Strengthening Privacy) Bill 2018; and
- [submission](#) into options for addressing the issue of sexting by minors.

Please contact Ms Leonie Campbell, Deputy Director of Policy, on (02) 6246 3711 or at leonie.campbell@lawcouncil.asn.au or Ms Sarah Sacher, Policy Lawyer, on (02) 6246 3724

or at sarah.sacher@lawcouncil.asn.au in the first instance, if you require further information or clarification.

Yours sincerely

A handwritten signature in black ink, appearing to read 'A. Moses'.

Arthur Moses SC
President

Children's Rights in Relation to the Digital Environment

In the three decades since the United Nations Convention on the Rights of the Child (**UNCRC**) was adopted,¹ there have been rapid advances in technology, with significant implications for children. Digital tools including smartphones and social media platforms are now interwoven into children's daily lives,² and play a pivotal role in the way children learn, socialise and perceive the world. It is therefore appropriate that the UN Committee on the Rights of the Child (**UN Committee**) develop guidance for States seeking to meet their obligations to promote and protect children's rights in light of challenges and opportunities presented by the digital environment.

Access to information and freedom of expression and thought; Right to education and digital literacy

Generally, children and young people face fewer difficulties using technology, compared to adults.³ However for certain subsets, there exists an inequality of access to new technologies and online platforms, in addition to barriers related to the accessibility of online material. In Australia these groups include children with disability, Aboriginal and Torres Strait Islander children, children from regional, rural or remote areas, and from low-income households.⁴

A 2017 study by the Salvation Army surveyed 1,380 of their clients across Australia who accessed emergency relief, and found that 57 percent of children did not have access to the internet, and approximately one in three did not have access to a computer or tablet at home.⁵ In a 2017 submission to the UN Office of the High Commissioner for Human Rights (**OHCHR**) the Australian Government noted that children and adults in remote locations in Australia, 'particularly in remote Indigenous communities' face problems accessing the internet.⁶

There is a real risk that this 'digital exclusion' will contribute to already-marginalised children missing out on new opportunities, or facing further systemic disadvantage, particularly noting the increasing number of educational resources and communications tools requiring internet connectivity and digital literacy. This is relevant to compliance with Article 29 of the UNCRC, which provides for a child's right to education. To address this trend, policymakers, businesses, and the education sector should place a focus on improving the digital ability of people in marginalised groups, including children with disabilities, as well as addressing the affordability and accessibility of digital tools.⁷

Relevantly, a number of countries have formally recognised the right to access the internet. It has been argued that such access is critical, particularly in terms of the right to freedom of expression, and in the redressing of structural disadvantage.⁸ The UN has recommended that specific attention is given to vulnerable groups to facilitate access to technology, in particular the internet.⁹ The Australian Human Rights Commission (**AHRC**) has previously stated that:

In order to ensure that information is truly accessible to all people in Australia, government departments and/or private companies should audit online materials to ensure they are user-friendly for new Internet users; institute educative initiatives on the secure use of the Internet and increase opportunities for meaningful access to the Internet of marginalised groups. Only when these measures are in place can structural vulnerability be identified, 'full inclusion' be achieved and any notion of the 'right' to access the Internet be truly realised.¹⁰

The Australian Government has established a number of programs with the aim of improving internet availability and access for children and adults in remote regions. These initiatives have included support for 301 WiFi Telephone services in remote Indigenous communities, and funding for the Remote Indigenous Internet Training activity, which provides internet access, training and internet infrastructure in remote Indigenous communities to address barriers to access.¹¹

Article 9(2)(a) of the Convention on the Rights of People with Disability¹² requires States to 'develop, promulgate and monitor the implementation of minimum standards and guidelines for the accessibility of facilities and services open or provided to the public'.¹³ The AHRC has observed that such standards could take into account accessibility and inclusivity considerations, and 'pay particular attention to the needs of vulnerable groups' such as children and people with disability.¹⁴ The AHRC has itself developed World Wide Web Access Advisory notes which provide guidance on the requirements for compliance with the *Disability Discrimination Act 1992* (Cth) and practical information on how to make websites more accessible to people with a disability.¹⁵

Relevantly, the Law Council proposes that the adoption of new technologies should be preceded by careful consideration of their appropriateness with respect to the intended audience of users and consumers, their implications for fairness and access and options for mitigating any adverse impact on marginalised groups.¹⁶ A key concern is that policymakers may overlook the realities of target groups' digital exclusion in their overreliance on online solutions at the expense of more effective and targeted strategies.¹⁷ In this regard, it is also important for governments to be cognisant of the geographic inequalities with respect to existing infrastructure, and to avoid assumptions that initiatives appropriate in urban areas will be easily transferable to rural and remote areas.

Access to Justice

The Justice Project explored the impact of new technologies upon access to justice outcomes for groups experiencing disadvantage, including children and young people, and made a number of findings and recommendations in this regard.¹⁸ Access to legal assistance and court processes is relevant to articles 12, 40 and 19 of the UNCRC.¹⁹

Technology is increasingly being adopted to assist people to better access legal assistance and courts. Generally, this is effective for people who have sufficient technological and legal capability, including reasonable literacy and education levels to process the information received, and access to high quality technology. Others will continue to have a strong need for face-to-face services and processes.²⁰

Many children and young people access justice through online legal services. One effective example is the National Children's and Youth Law Centre's national *Lawmail* email-based service. The model has enabled young people to bypass their parents' intervention, removing their physical obstacles, and overcoming their embarrassment about seeking help.²¹ Demand for the service increased 30 percent between 2012 and 2014.²²

However, Australian research indicates that children and young people who are technologically literate and have ready access to the internet may still prefer to seek legal information and advice through face to face services. A nationwide survey found that the 'youngest...respondents were significantly more likely than older respondents to obtain advice only in-person'.²³ This is consistent with the findings of Coumarelos et al – that young people have low rates of using the internet in response to legal problems, despite being technologically literate.²⁴ Pleasence et al has also found that despite young people being technologically literate, 'online legal information does not necessarily improve their legal capability' because they may still 'lack the ability to successfully obtain and apply online legal information in a meaningful way'.²⁵ This is particularly the case for marginalised young people with lower than average literacy levels, and with 'poor functional literacy – that is, low ability for using information in a goal-orientated way to solve problems'.²⁶ In addition to capability barriers, mistrust of the justice system is a primary barrier for many disadvantaged young people, necessitating face-to-face relationships with legal advisers to build trust and a willingness to engage.²⁷

It is well recognised that children require specialised services and tools in order to meaningfully access justice. Correspondingly, caution needs to be taken not to apply technological solutions indiscriminately, given that a 'one-size fits all' approach will not suit many children, particularly those experiencing disadvantage. Careful consideration is needed of possible technological responses: of why and for whom they may be effective, in what circumstances, and the likely costs, risks and benefits.²⁸

Protection of privacy, identity and data processing

The right to privacy is recognised as a fundamental human right, including under Article 16 of the UNCRC.²⁹ Laws protecting individuals against breach of privacy have generally not kept pace with technological developments. It is increasingly common for personal data to be collected with or without knowledge through the internet, apps, and social media platforms which harness Artificial Intelligence (**AI**) technology.³⁰ Data collection is often used to track, profile, and predict the behaviour of the population. It is often a compulsory precondition to the provision of services.³¹

Data sharing tools are vulnerable to exploitation, including by corporations and government. Due to the fast pace of technology, governments may pass data-related legislation without fully exploring the implications for privacy, creating the potential for unforeseen negative consequences. For example, the Law Council has raised concerns about Australian mandatory data retention laws,³² including noting the potential for unauthorised usage and abuses by Government agencies, following reports of warrantless access to metadata information by the Australian Federal Police.³³ The Law Council has called for greater

transparency and accountability in the application of these laws.³⁴ Another example is Australian data sharing legislation for health providers such as the 'My Health Record'³⁵ system. The Law Council raised initial concerns that this system could unintentionally place children at risk from a violent parent or caregiver with the ability or authority to access information on behalf of the child. While the system was subsequently refined, it is yet to be determined whether the amendments will ensure an effective system.³⁶

An additional concern is that data retention and sharing technologies can be utilised to underpin existing discriminatory practices and heighten the associated negative consequences. For example, the Justice Project identified that at-risk young people face heightened exposure to over-policing, including pre-emptive policing and profiling.³⁷ Increased usage of biometric identification and data retention have the potential to increase and worsen the consequences of such practices.

The Law Council considers that data retention and sharing tools must have safeguards in place that uphold human rights, such as the right to privacy and protecting personal information from unauthorised collection and misuse. Further, there should be rigorous analysis at the policy development stage prior to implementation, including an analysis of whether the benefits of the systems are worth the potential infringement of rights, including privacy, together with the risk of breaches in the future.

The Law Society of New South Wales is in favour of a new Federal statutory cause of action for serious invasion of privacy, in line with Australian Law Reform Commission (**ALRC**) recommendations.³⁸ However, the Law Council's Business Law Section's Media and Communications and Privacy Law Committees have previously queried the need for a civil cause of action for serious breach of privacy.³⁹

The ALRC has also recommended that the design of legal privacy protection should be 'sufficiently flexible to adapt to rapidly changing technologies and capabilities, without needing constant amendments'.⁴⁰ Additionally the ALRC stated that 'education about privacy risks and management may be particularly important for children and young persons'.⁴¹ It cited research indicating that the use of privacy settings on social media is higher among older Australians. The ALRC therefore suggested 'privacy awareness campaigns and other strategies targeted at younger Australians'⁴² as a means of protecting children's right to privacy in the digital environment.

Protection from violence, sexual exploitation and other harm

The risks posed by online variables are wide and unpredictable. A nuanced approach is needed to address these risks, recognising the complexities involved. In considering measures to protect children, it is also necessary to uphold children's rights to privacy, freedom of expression and association, and to recognise the role of the digital environment in 'enhancing a child's right to participation, education and information'.⁴³ Additionally it is important to recognise that in the case of, for example, cyberbullying and sexting, the 'perpetrators' are often other children. Further, to ensure legislative responses meet their aim, children should have access to advocates who can act on their behalf and provide advice.

Cyberbullying

The Law Council has previously observed that it is necessary for human rights obligations and rule of law principles to be considered at the outset in order to identify the different interests involved in relation to cyberbullying, and to resolve in a principled manner the tensions which may arise.⁴⁴ The Law Council has proposed the following approach to the Australian Government:

- responses should be framed in light of human rights obligations, including the rights of the child to: be ensured by the State such protection and care as is necessary for his or her wellbeing; for his or her best interests to be a primary consideration; to life, and to survival and development to the maximum extent possible; the right to express those views freely in all matters affecting him or her; to freedom of expression; freedom of association; health; and privacy;
- in discussions of cyberbullying these rights should carry a different resonance depending on whether the child involved is: a victim or possible victim of cyberbullying; a perpetrator or possible perpetrator of cyberbullying; a bystander whose rights are nevertheless engaged in a possible cyberbullying incident;
- in relation to a perpetrator who has been accused or charged with a criminal offence, the following principles should apply:
 - in all actions concerning children, the best interests of the child shall be a primary consideration;
 - the arrest, detention or imprisonment of a child should be used only as a measure of last resort and for the shortest appropriate period of time and pre-trial detention of children should be avoided to the greatest extent possible;
 - every child accused of, or convicted of, a criminal offence should be treated in a manner which:

- is consistent with the promotion of the child's sense of dignity and worth;
 - reinforces the child's respect for the human rights and freedoms of others; and
 - takes into account the child's age, sex or gender and needs and the desirability of promoting the child reintegrating and assuming a constructive role in society;
- any response to cyberbullying should explicitly address these interests and then seek to balance them in a manner which ensures that any limitations placed on individuals' rights are necessary, reasonable and proportionate;
 - depending upon the severity of the conduct, a different kind of response – legislative or otherwise – may be required. The utilisation of a civil penalty regime and other less formal methods (be it school or mediation based) should be considered in less serious cases. Any analysis of proposals of the most appropriate responses to this issue also depends on whether the perpetrators of cyberbullying are children or adults, noting that in the majority of cases, the perpetrators are children; and
 - further, legislation should be adopted to provide minimum standards for the sentencing of young offenders to enhance sentencing practices for young cyberbullying offenders.⁴⁵

Further to the above, the Law Council supports education for young people about the nature and consequences of cyberbullying and recognises the work of the Office of the eSafety Commissioner delivering online safety education to schools.⁴⁶ It has also encouraged the Australian Government to work with social media sites to develop a best practice in response to cyberbullying. It notes that in the European Union (EU), two separate Coalitions consisting of social media companies, and with the support of the EU Commissioner, have been formed to continue working towards effective ways to combat cyberbullying experienced by children.⁴⁷

Sexting

Increased reports of sexting in recent years have been attributed to a corresponding increase in the use of mobile phone and social media technology by young people. Sexting by young people poses a number of challenges for policy makers in terms of its social and legal implications. The Law Council has noted the potential for young people to be charged with child pornography offences in the absence of more specific sexting offences to be particularly concerning.⁴⁸

When considering options for addressing sexting by minors, the Law Council encourages approaches which 'balance the need to eliminate the harms of child pornography and punish the people who create it, with the need to protect offending teenagers from unwittingly committing a serious and punishable offence.'⁴⁹ The Law Council is also in favour of improved education and awareness about the internet and other communications technologies such as the appropriateness of the behaviour of people who distribute intimate images or media without consent.⁵⁰

Image-based abuse

The non-consensual sharing of intimate images, or threatening to do so, may be used in the context of family violence or in the perpetration of sexual assault.⁵¹ This can be identified as 'image-based abuse'.⁵² A 2016 study found that 51 percent of Australian girls believe that girls are pressured into taking explicit photographs of themselves and sharing them.⁵³ In a 2017 report, the OHCHR noted that 'specific groups of women, in particular young women... may experience particularly severe forms of online violence'⁵⁴ that impact on their human rights. Strategies to combat online violence against girls and women canvassed by the OHCHR include legislation, education, preventative measures, and tools within software and social media platforms that promote safety and privacy.⁵⁵

In Australia, the legislative response to online violence and harassment at the federal level has included the *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018* (Cth), which supports the victims of 'image-based abuse' by providing the Office of the eSafety Commissioner with a range of enforcement options to require rapid removal of image-based abuse material and to hold perpetrators to account. Civil penalties under the Act range from \$105,000 for individuals to \$525,000 for corporations; perpetrators may also face penalties of imprisonment for up to five years under the *Criminal Code Act 1995* (Cth). Most Australian states and territories have also introduced specific image-abuse offences or expanded definitions to ensure that such behaviour is captured under existing criminal legislation.⁵⁶

Exposure to adult content online

Adult digital platforms do not generally have effective age restrictions preventing access to children, in the absence of parental locks. The AHRC has observed that 'most children are treated as adults when they use such technology and this can have potentially negative consequences for them'.⁵⁷ Much of the content

readily accessible and viewable to children online would be considered unacceptable and sometimes criminal for children to be exposed to in an offline environment. The Law Council considers that States should look to options for better ensuring such platforms limit access on the basis of age.

A further concern is that children may also be unknowingly targeted by programs and algorithms through digital platforms, with potentially harmful consequences. For example, research indicates that many online games incorporate 'gambling-like elements' which may normalise gambling, lead to 'gaming addiction' and affect mental health outcomes for young people.⁵⁸

Family environment, parenting and alternative care

In Australia, a number of provisions in the *Family Law Act 1975* (Cth) (**FLA**) offer protection for children from and in the use of digital communications, and also provide for the positive realisation of rights associated with digital rights and the family environment. As noted, risks associated with the digital landscape are variable. Much is dependent on a number of other significant environmental factors which vary from family to family.

Inherently problematic direct digital communications between parent and child may contravene many of the rights of the child contained in the UNCRC, including those designed to: threaten, intimidate or otherwise emotionally harm a child; interfere with a child's relationship with a parent or other significant person; and/or maintain a relationship with a child that is contrary to the child's best interests or in a manner that is contrary to those interests.

The FLA provides protections in these circumstances. These include the capacity for the courts exercising jurisdiction under the FLA to make parenting orders dealing with, inter alia, 'the communications a child is to have with another person or persons'.⁵⁹ A court has the capacity to make specific orders about the nature, frequency, media and timing of communications with a child. Specific orders⁶⁰ can address issues of digital risk for children in significant detail.

The FLA also empowers courts to make orders in relation to 'any aspect of the care, welfare or development of the child or any other aspect of parental responsibility for a child'.⁶¹ Parental responsibility is defined as being 'all the duties, powers, responsibilities and authority which, by law, parents have in relation to children'.⁶² Specific orders providing for detailed use of/removal from digital platforms can be used to ensure both protection for the child and compliance with obligations under the UNCRC.

The FLA enshrines in Australian law the 'Paramountcy Principle': the concept that in 'deciding whether to make a particular parenting order in relation to a child, a court must have regard to the best interests of the child as the paramount consideration',⁶³ and sets out the issues to be considered in determining what is in a child's best interest.⁶⁴

One of the 'primary considerations'⁶⁵ includes 'the need to protect the child from physical or psychological harm from being subjected to, or exposed to, abuse, neglect or family violence'. This would include abuse, neglect or family violence arising in a digital forum. In relevant cases the court must also have regard to 'the capacity of: (i) each of the child's parents; and (ii) any other person (including any grandparent or other relative of the child) to provide for the needs of the child, including emotional and intellectual needs'.⁶⁶ This would extend to the consideration of a parent's capacity to ensure that children are not exposed to inappropriate digital material. Although no sections of the FLA make specific reference to digital material or forums in and to which children may be exposed, the Act itself contains existing mechanisms to ensure that children are protected from unacceptable risk of harm via modern communication channels.

Modern communication channels can also be positive elements to 'family environment, parenting and alternative care' and enable the child's right to know and to be cared for by both parents⁶⁷ to be respected. The FLA refers to children's rights to communicate with parents and other significant people on a regular basis.⁶⁸ This can be applied as an order for children to have telephone, SMS, email or other forms of electronic communication (e.g. Facetime) with the parent with whom they are not living. Access to a digital environment by children in order to communicate and maintain a relationship with a parent or a significant person in their life, where the tyranny of distance is a factor, or where face to face visits are not appropriate due to safety issues, is crucial. Parenting orders are often made to ensure the facilitation of the child's relationship/s via such channels.

Non-discrimination

The continued rise of AI across many systems in everyday life has the potential to effectively institutionalise discrimination, diminishing accountability in relation to the making of AI informed decisions.⁶⁹ Data-based decision making can reflect societal prejudices, and can reinforce biases, both explicit and implicit. For example, outcomes may be skewed by how a question is asked or how a proposition is framed, and AI systems have the potential to be manipulated through algorithmic bias if the limitations and possibilities of computers and robot machines are poorly applied or understood.⁷⁰ A lack of diversity and inclusion in the design of AI systems is of concern, as systems may reinforce discrimination and prejudices while having an appearance of objectivity.⁷¹

Decisions made without questioning the results of a flawed algorithm can therefore have serious repercussions for the right not to be discriminated against for characteristics including age, gender, disability, sexual orientation and race. The Law Council considers that there is scope for data-based decisions to be made transparent and be reviewable in the design stage.⁷²

States are grappling with difficulties of how to apply existing legislation to new technologies, and how to develop new regulations to address the gaps that emerge. In the European Union, Article 22 of the General Data Protection Regulation (**GDPR**) contains rules to protect individuals in the context of automated decision-making with a legal or otherwise significant impact on them.⁷³ Provisions in the GDPR protecting individual rights in the face of AI-informed decision making, as well as regulating the type of data that can be used, are a benchmark for how these issues should be approached.

How can States better realise their obligations to children's rights in relation to the digital environment?

Supplementary to the discussion above, the Law Council considers that any legislation protecting human rights in respect of new technologies and the digital environment should be principles-based, to allow for flexibility and adaptability. The principles that the Law Council believes should guide legislation in this area are fairness, transparency, non-discrimination and accountability.⁷⁴

How should business operating in the digital environment support the realisation of children's rights?

Companies that create and operate digital technologies have a responsibility to respect and promote the rights of all people who access their technology, including children. These are articulated in the UN Guiding Principles on Business and Human Rights (**UNGPs**). Under the UNGPs, companies are expected to respect human rights and avoid causing adverse human rights impacts through their activities. The UNGPs recommend that companies ensure compliance with this responsibility to respect human rights through: expressing commitment through a statement of policy; implementing effective human rights due diligence to identify, prevent and address actual or potential human rights impacts; mainstreaming human rights consideration across business operations and activities based on that due diligence; and enabling access to effective grievance mechanisms by affected groups and individuals.⁷⁵

The UNGPs also require States to provide effective guidance to business enterprises on how to respect human rights throughout their operations. In the Australian context, the Australian Government could usefully develop and update guidance for businesses on supporting the realisation of children's rights in the digital environment. Similarly, businesses should proactively consider user safety in the design of digital products, particularly where the product is likely to be used by children and young people, to ensure the child is protected from violence and abuse online. In this regard the Law Council also notes the National Principles for Child Safe Organisations, which were endorsed by the Council of Australian Governments in February 2019. Principle eight requires that 'physical and online environments promote safety and wellbeing while minimising the opportunity for children and young people to be harmed', and includes a number of action areas for organisations to follow.⁷⁶

¹ *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990).

² 'Research Snapshot: Aussie Teens and Kids Online', *Australian Communications and Media Authority* (Web Page, February 2016) <<https://www.acma.gov.au/theACMA/engage-blogs/engage-blogs/Research-snapshots/Aussie-teens-and-kids-online>>.

³ Australian Human Rights Commission, *Human Rights and Technology* (Issues Paper, 2018) 20, 36.

⁴ Julian Thomas et al, *Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2017* (RMIT University, 20 July 2017) 5.

⁵ The Salvation Army, *The Hard Road: National Economics and Social Impact Survey 2017* (2017) 7. This follows a 2013 research study from the Smith Family which found that in Australia's most disadvantaged communities, only 68 percent of children aged 5 to 14 years accessed the internet at home over a 12 month period, compared to 91 percent of children in the most advantaged communities: Anne Hampshire, 'Sport, Culture and the Internet: Are Australian Children Participating',

(Presentation delivered at the Australian Social Policy Conference, Sydney, September 2013)

<https://www.thesmithfamily.com.au/~media/files/research/policy-submissions/aspc_sport%20culture%20internet_sept13.ashx?la=en>.

⁶ Letter from Australian Government to the Office of the High Commissioner for Human Rights, 'Australian Response to OHCHR Questionnaire pursuant to HRC Resolution 32/13', January 2017 <<https://www.ohchr.org/Documents/Issues/Women/WRGS/GenderDigital/AUSTRALIA.docx>>

⁷ For further elaboration on these points, see Law Council of Australia, Submission to the Australian Human Rights Commission, *Human Rights and Technology* (October 2018) <<https://www.lawcouncil.asn.au/resources/submissions/human-rights-and-technology>>.

⁸ Australian Human Rights Commission, *Background Paper: Human Rights in Cyberspace* (September 2013) <www.humanrights.gov.au/our-work/rights-and-freedoms/publications/background-paper-human-rights-cyberspace>.

⁹ United Nations, *World Summit on the Information Society: Plan of Action*, UN Doc WSIS-03/GENEVA/DOC/5-E (12 December 2003) para 10(c) <<https://www.itu.int/net/wsis/docs/geneva/official/poa.html>>.

¹⁰ Australian Human Rights Commission, *Background Paper: Human Rights in Cyberspace* (September 2013) <www.humanrights.gov.au/our-work/rights-and-freedoms/publications/background-paper-human-rights-cyberspace>.

¹¹ Letter from Australian Government to the Office of the High Commissioner for Human Rights, 'Australian Response to OHCHR Questionnaire pursuant to HRC Resolution 32/13', January 2017 <<https://www.ohchr.org/Documents/Issues/Women/WRGS/GenderDigital/AUSTRALIA.docx>>.

¹² *Convention of the Rights of Persons with Disabilities*, opened for signature 13 December 2006, 2515 UNTS 3 (entered into force 3 May 2008).

¹³ *Ibid* art 9(2)(a).

¹⁴ Australian Human Rights Commission, *Human Rights and Technology* (Issues Paper, 2018) 41.

¹⁵ Australian Human Rights Commission, *World Wide Web Access: Disability Discrimination Act Advisory Notes ver 4.1* (2014) <<https://www.humanrights.gov.au/our-work/disability-rights/world-wide-web-access-disability-discrimination-act-advisory-notes-ver>>.

¹⁶ Law Council of Australia, Submission to the Australian Human Rights Commission, *Human Rights and Technology* (October 2018).

¹⁷ Law Council of Australia, *Justice Project Final Report: Regional, Rural and Remote Australians* (August 2018) 21 <<https://www.lawcouncil.asn.au/files/web-pdf/Justice%20Project/Final%20Report/Rural%20Regional%20and%20Remote%20%28RRR%29%20Australians%20%28Part%201%29.pdf>>.

¹⁸ See in particular, Law Council of Australia, *Justice Project Final Report: Children and Young People* (August 2018) 17 <<https://www.lawcouncil.asn.au/files/web-pdf/Justice%20Project/Final%20Report/Children%20and%20Young%20People%20%28Part%201%29.pdf>>.

¹⁹ *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990), arts 12, 14, 19.

²⁰ Law Council of Australia, *Justice Project Final Report: Legal Services* (August 2018) 18, 33.

²¹ National Children's and Youth Law Centre, Submission to the Law Council of Australia, *Justice Project* (6 October 2017).

²² *Ibid*.

²³ Pascoe Pleasence et al, Law and Justice Foundation of New South Wales, *Reshaping Legal Assistance Services: Building on the Evidence Base* (2014) 23-24

²⁴ Christine Coumarelos et al, Law and Justice Foundation of New South Wales, *Collaborative Planning Resource – Service Planning* (2015) 33

²⁵ Pascoe Pleasence et al, Law and Justice Foundation of New South Wales, *Reshaping Legal Assistance Services: Building on the evidence base* (2014) 32.

²⁶ Christine Coumarelos et al, Law and Justice Foundation of New South Wales, *Legal Australia-Wide Survey Legal Need in Australia* (2012) 31.

²⁷ Law Council of Australia, *Justice Project Final Report: Legal Services* (August 2018) 26, citing, eg, Liz Curran, *Draft Working Paper for a Research and Evaluation Report for the Bendigo Health-Justice Partnership: A Partnership between ARC Justice Ltd and Bendigo Community Health Services* (2016) 146-71.

²⁸ See Law Council of Australia, *Recommendations and Group Priorities* (August 2018) Recommendations 2.7 and 4.12 <<https://www.lawcouncil.asn.au/files/web-pdf/Justice%20Project/Final%20Report/03%20-%202018%2009%20-%20Recommendations%20and%20Group%20Priorities.pdf>>.

²⁹ See *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948) art 12; *International Covenant on Civil and Political Rights*, opened for signature 16 December 1976 (entered into force 23 March 1976) 999 UNTS 171, art 17; *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990) art 16.

³⁰ See, eg, Australian Human Rights Commission, *Human Rights and Technology* (Issues Paper, 2018) 15; Digital Rights Watch Australia, *State of Digital Rights 2018* (2018) 14 <<https://digitalrightswatch.org.au/wp-content/uploads/2018/05/State-of-Digital-Rights-Web.pdf>>; Natasha Singer, 'What You Don't Know About How Facebook Uses Your Data' *New York Times* (online), 11 April 2018 <<https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html>>; Privacy International, *Data Beyond our Control, Invisible to the Individual* <<https://privacyinternational.org/recommendation-principle-or-safeguard/data-beyond-our-control-invisible-individual>>.

- ³¹ Ibid. See also Fred H Cate, 'Personal Privacy is Eroding as Consent Policies of Google and Facebook Evoke "Fantasy World"' *The Conversation* (online), 14 December 2014 <<https://theconversation.com/personal-privacy-is-eroding-as-consent-policies-of-google-and-facebook-evoke-fantasy-world-33210>>.
- ³² Law Council of Australia, 'AFP Incident Raises Concerns about Implementation of Mandatory Data Retention Laws' (Media Release, 30 April 2017) <<https://www.lawcouncil.asn.au/media/media-releases/afp-incident-raises-concerns-about-implementation-of-mandatory-data-retention-laws>>.
- ³³ Luke Royes, 'AFP Officer Accessed Journalist's Call Records in Metadata Breach' *ABC News* (online), 29 April 2017 <<https://www.abc.net.au/news/2017-04-28/afp-officer-accessed-journalists-call-records-in-metadata-breach/8480804>>.
- ³⁴ Law Council of Australia, 'AFP Incident Raises Concerns about Implementation of Mandatory Data Retention Laws' (Media Release, 30 April 2017) <<https://www.lawcouncil.asn.au/media/media-releases/afp-incident-raises-concerns-about-implementation-of-mandatory-data-retention-laws>>.
- ³⁵ The My Health Record system contains online summaries of an individual's health information. This includes the medicines they have consumed, the allergies they may experience, and the treatments they have received: see Law Council of Australia, Submission to the Senate Standing Legislation Committee on Community Affairs, *Inquiry into the My Health Records Amendment (Strengthening Privacy) Bill 2018*, 24 September 2018 <<https://www.lawcouncil.asn.au/resources/submissions/my-health-records-amendment-strengthening-privacy-bill-2018>>.
- ³⁶ Ibid.
- ³⁷ See, eg, Law Council of Australia, *Justice Project Final Report: Children and Young People* (August 2018) 60; Law Council of Australia, *Alternative Report to the United Nations Committee on the Rights of the Child* (November 2018) 16-20.
- ³⁸ Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report No 123, 2014).
- ³⁹ See, eg, Law Council of Australia, Business Law Section, Media and Communications Committee and the Working Party on Privacy Law, Submission to New South Wales Law Reform Commission, *NSW Law Reform Commission's Consultation Paper No 1 – Invasion of Privacy* (18 September 2007).
- ⁴⁰ Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report No 123, 2014) [2.30].
- ⁴¹ Ibid [2.54].
- ⁴² Ibid [2.55].
- ⁴³ Australian Human Rights Commission, *Human Rights and Technology* (Issues Paper, 2018) 20.
- ⁴⁴ See Law Council of Australia, Submission to the Senate Legal and Constitutional Affairs Committee, *The Adequacy of Existing Offences in the Commonwealth Criminal Code and of State and Territory Criminal Laws to Capture Cyberbullying* (20 October 2017).
- ⁴⁵ Ibid 4-7.
- ⁴⁶ Ibid 19.
- ⁴⁷ The Coalition to Make the Internet a Better Place for Kids and the ICT Coalition for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU.
- ⁴⁸ See Law Council of Australia, Submission to the Senate Select Committee on Cyber-Safety, *Inquiry into Options for Addressing the Issue of Sexting by Minors* (6 August 2013).
- ⁴⁹ Richards and Calvert, 'When Sex and Cell Phones Collide: Inside the Prosecution of a Teen Sexting Case,' (2009) 32(1) *Hastings Communication and Entertainment Law Journal* 6.
- ⁵⁰ See the recommendations in Katherine Albury et al, *Young People and Sexting in Australia: Ethics, Representation and the Law* (2013) <<https://aifs.gov.au/cfca/pacra/young-people-and-sexting-australia-ethics-representation-and-law>>.
- ⁵¹ Nicola Henry, Anastasia Powell and Asher Flynn, RMIT, *Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse* (2017) 3; See also Senate Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, *Phenomenon Colloquially Referred to as 'Revenge Porn'* (2016).
- ⁵² Ibid.
- ⁵³ Plan International Australia and Our Watch, "Don't Send Me that Pic": *Australian Young Women and Girls Report Online Abuse and Harassment are Endemic* (2016) 2.
- ⁵⁴ UN Human Rights Council, *Promotion, Protection and Enjoyment of Human Rights on the Internet: Ways to Bridge the Gender Digital Divide from a Human Rights Perspective: Report of the United Nations High Commissioner for Human Rights*, 35th sess, UN Doc A/HRC/35/9 (5 May 2017) 36.
- ⁵⁵ Ibid 37.
- ⁵⁶ See eSafety Commissioner, *What's the Law in my State or Territory: Image-based Abuse* (Web Page) <<https://www.esafety.gov.au/image-based-abuse/legal/whats-the-law-in-my-state-territory>>.
- ⁵⁷ Australian Human Rights Commission, *Human Rights and Technology* (Issues Paper, 2018) 16.
- ⁵⁸ Responsible Gambling Victoria, *Literature Review: Online Gaming and Gambling in Children and Adolescents – Normalising Gambling in Cyber Places* (September 2018); Alex-Matthews-Kings, 'Games Like Fortnite Use "Predatory" Gambling Techniques to Make Children Spend, Experts Warn', *The Independent* (online), 28 June 2018 <<https://www.independent.co.uk/news/health/fornite-loot-llamas-payments-upgrades-items-gambling-addiction-a8421201.html>>; Daniel L King and Paul H Delfabbro, 'Predatory Monetization Schemes in Video Games (e.g. 'Loot Boxes') and Internet Gaming Disorder' (2018) 113(1) *Addiction* 1967 <<https://onlinelibrary.wiley.com/doi/full/10.1111/add.14286>>.
- ⁵⁹ *Family Law Act 1975* (Cth) s 64B(2)(d).
- ⁶⁰ Made in conjunction with orders pursuant to the general injunctive relief contained within section 114 of the *Family Law Act 1975* (Cth).

⁶¹ *Family Law Act 1975* (Cth) s 64B(2)(i).

⁶² *Ibid* s 61B.

⁶³ *Ibid* s 60CA.

⁶⁴ *Ibid* ss 60CC(2)-(3).

⁶⁵ *Ibid* s 60CC(2).

⁶⁶ *Ibid* s 60CC(3)(f).

⁶⁷ *Ibid* s 60B(2)(a).

⁶⁸ *Ibid* s 60B (2)(b).

⁶⁹ For further elaboration on these points, see Law Council of Australia, Submission to the Australian Human Rights Commission, *Human Rights and Technology* (October 2018)

<<https://www.lawcouncil.asn.au/resources/submissions/human-rights-and-technology>>.

⁷⁰ See, eg, Australian Human Rights Commission, *Human Rights and Technology Issues Paper* (2018) 13.

⁷¹ See, eg, Jackie Snow, "We're in a Diversity Crisis": Co-founder of Black in AI on What's Poisoning Algorithms in Our Lives', *MIT Technology Review* (online), 14 February 2018 <<https://www.technologyreview.com/s/610192/were-in-a-diversity-crisis-black-in-ai-founder-on-whats-poisoning-the-algorithms-in-our/>>; Danny Guilory, 'Why Adding Diversity in Artificial Intelligence is Non-negotiable', *Redshift* (Web Page, 14 September 2017)

<<https://www.autodesk.com/redshift/diversity-in-artificial-intelligence/>>.

⁷² Law Council of Australia, Submission to the Australian Human Rights Commission, *Human Rights and Technology* (October 2018) 14 <<https://www.lawcouncil.asn.au/resources/submissions/human-rights-and-technology>>.

⁷³ *General Data Protection Regulation (EU) No 2016/679* [2016] OJ L 119, 1, art 22.

⁷⁴ For further elaboration on these points, see Law Council of Australia, Submission to the Australian Human Rights Commission, *Human Rights and Technology* (October 2018) <

<https://www.lawcouncil.asn.au/resources/submissions/human-rights-and-technology>>.

⁷⁵ Office of the United Nations High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* (2011) HR/PUB/11/04 <

<https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf>.

⁷⁶ Australian Human Rights Commission, *National Principles for Child Safe Organisations* (2019)

<<https://www.humanrights.gov.au/sites/default/files/National%20Principles%20for%20Child%20Safe%20Organisation.pdf>>.