Australian Council on Children and the Media (ACCM)

Report on Australian privacy law as it applies to children's online engagements with commercial interests

April 2021

https://childrenandmedia.org.au/resources/australian-privacy-law-is-it-protecting-our-children-when-online

Contents

1. The current law of privacy in Australia

Too complex and fragmented to be understood?

In a recent submission, privacy law expert Prof Kimberlee Weatherall of the University of Sydney Law School, commented that:

> 'the privacy regime in Australia is … too complex and fragmented. *Specialists* already struggle to parse Australian privacy law.
>
> 'The 1988 [Privacy] Act was originally designed to cover the Commonwealth public sector, but it has been amended at least 10 times since (5 times in the last 10 years), creating specific rules for certain kinds of data… As a result, the Act is now over 300 pages long.
>
> '… And privacy is also governed by other areas of law (such as in relation to the workplace). Separate laws address various kinds of law enforcement, supplemented by non-transparent practices. Then there is an additional layer of State legislation. And of course, this is all before anyone reads any one of the many privacy policies to which they are subject, which are routinely very long and written to require a university degree to make any sense of them.'

Despite such difficulties, this report gathers information about the legal protection of privacy in Australia, including its history and current developments.

Background

As a starting point, it is useful to consider the conceptual background to privacy protection and the relevance of its cultural origins. Prior to the 1990s, when the development of the internet gave rise to a rapid growth in the spread of personal information, privacy was little known or recognised as a legal or regulatory issue in Australia. Concerns about privacy were also considered as heavily culturally based, that is, interests and expectations of privacy were not internationally consistent. Privacy is considered a fundamental human right in Europe, and highly regarded as a personal freedom in the US, but has been slow to emerge as an interest in many Asian countries. In multicultural Australia there may not be a consistent community view about the importance of privacy, and there most certainly was not at the time that the first legislation to protect privacy was enacted, in 1988. This is a very difficult starting point for a coherent regulatory framework.

Over 40 countries worldwide have a right to privacy within either their Bill of Rights or their Constitution. As Australia lacks such protection, it was necessary for the parliament to enact it through legislation.

The first privacy law in Australia, the *Privacy Act 1988* (Cth), was enacted following a major 1983 inquiry into the issue by the Australian Law Reform Commission (ALRC). That inquiry, in turn, was instigated largely in order to implement Australia's obligations under the International Covenant on Civil and Political Rights.

The pathway from an international treaty right to a local statute is an unusual one for the development of law in Australia, and this history possibly goes some way to explain why privacy, as a legal concept, remained poorly understood and underdeveloped until recently. Other explanations for privacy law being underdeveloped in Australia include the breadth of interests involved in protecting privacy, the ongoing development of new privacy threats over time, and the challenges associated with ascertaining the level of public interest in and concern about privacy in the community. Given that privacy means different things to different people, it is unsurprising that consumers of online social media and gaming have called for a 'balanced' approach to privacy and downplayed the importance of privacy protections.

It was not until 2008 that the ALRC settled on a broad definition of privacy as 'a bundle of interests that individuals have in their personal sphere free from the interference of others'. It also identified four separate interests covered by privacy:

- *Information privacy* – or data protection, involving the collection and handling of personal data such as credit information, medical and government records;
- *Privacy of communications* – involving the security of mail, telephone, email and other forms of communication;
- *Territorial privacy* – involving intrusion into environments such as domestic, workplace or public including search, video, surveillance and ID checks;
- *Bodily privacy* – involving a person's physical selves and invasive procedures such as genetic tests, drug testing and cavity searches.

All of these interests, with the exception of bodily privacy, may be relevant to the ways in which children engage with online content.

Privacy protection in Australia has largely developed through the introduction of a Commonwealth framework of legislative safeguards and regulation, although most states also have local law which covers their own state government agencies.

The *Privacy Act* – a 'principles-based' approach

The *Privacy Act* adopts what it terms a 'principles-based', rather than a prescriptive, approach to regulation. The Act sets out 13 Australian Privacy Principles (or APPs) which apply to the operation of all Australian Government agencies, all businesses and not-for-profit organisations with an annual turnover greater than $3 million, and all health service providers and organisations trading in personal information. These are called 'APP entities'. Generally speaking all corporate entities with whose media and entertainment products children engage are subject to the APPs.

The APPs govern the collection, storage, use and disclosure of personal information, as well as providing individuals with certain rights to access their personal information and correct errors. There are specific APPs that apply to open and transparent management of personal information, direct marketing, cross-border disclosure of personal information and government identifiers.

Other important features of the *Privacy Act* are:

- Sensitive personal information, including health information and financial information, has higher protections than other types of information such as basic identity information. These higher protections do not apply to children's information as such.
- The Act does not currently recognise a general civil cause of action for breach of privacy. Without a cause of action it is argued that the *Privacy Act* has 'no teeth'.
- There is a range of enforcement actions to be taken by a specialist Commonwealth regulator, the Office of the Australian Information Commissioner ('OAIC').

Enforcement by the OAIC

Under the *Privacy Act* a person can make a complaint directly to the OAIC about the handling of their personal information by an APP entity. The OAIC also has power to:

- commence a Commissioner-initiated investigation (CII) into an incident or practice that might breach the *Privacy Act*;
- conduct an assessment of whether an organisation is maintaining and handling personal information in accordance with the *Privacy Act*;
- require an organisation to develop an enforceable code, and register codes that have been developed on the initiative of an entity;
- direct an agency to give the OAIC a privacy impact assessment about a proposed activity or function; and
- recognise some approved external dispute resolution schemes to handle particular privacy-related complaints.

The OAIC also has a range of responsibilities under other laws, including laws relating to data matching, eHealth, spent convictions and tax file numbers. In addition it has an education and advisory role, giving information and advice on privacy to individuals, businesses and agencies through an enquiries team and their website. Overall, the *Privacy Act* creates a complex task of

regulation for the OAIC and unfortunately a task not without significant political interest and sometimes interference.[1]

Other privacy regulations – breach notification and consumer data rights

Since 2016 the OAIC has also managed a mandatory data breach notification system that covers all organisations subject to the *Privacy Act*. A data breach is deemed to happen when personal information stored by an organisation is accessed or disclosed without authorisation, or is lost. When a data breach occurs involving personal information that is likely to result in serious harm, the organisation must notify affected individuals and the OAIC.

Serious harm, in this context, may include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach. Although individuals may be distressed or otherwise upset at an unauthorised access to or unauthorised disclosure or loss of their personal information, this would not itself be sufficient to require a notification. A duty to notify is most likely to arise from a risk of financial, economic or physical harm. Where an eligible data breach involves health information or other personal 'sensitive information', a reasonable person may conclude in some cases that a likely risk of serious harm would exist. It is unlikely, however, that a breach of children's data, per se, would invoke these regulations.

In 2020 a further regulatory measure in relation to privacy took effect, known as the Consumer Data Right (CDR) rules. The CDR has commenced in the banking industry and will be rolled out to telecommunications and energy industries to assist customers of those industries to gain more seamless access to competitive contract opportunities without compromising their privacy. The CDR scheme is managed by the OAIC and the Australian Competition and Consumer Commission (ACCC), and has no particular significance to children's rights or interests.

Criminal law

Cybercrime overlaps with privacy, and given that crime and policing are a state-based law jurisdiction, there are also local state initiatives throughout Australia on promoting e-safety for children including privacy issues. These vary in their focus but are largely educational rather than involving the application of law.[2] Generally speaking the states defer to Commonwealth law and the Australian Federal Police in relation to cybersecurity and privacy related matters.

---

[1] Note that the OAIC also regulates Australia's FOI system, a function which regularly brings them in direct conflict with government. The OAIC has suffered significant underfunding over successive governments, most famously under the Abbott Coalition government when it came close to collapse.

[2] Eg in South Australia: https://parenting.sa.gov.au/easy-guides/cybersafety-parent-easy-guide.

One particular issue for the application of criminal law is doxxing, or the search for and publication of private or identifying information about a particular individual on the Internet, typically with malicious intent. It has a clear overlap with privacy protection, and it is also highly likely to be an offence. While doxxing is usually initiated and perpetrated by a 3rd party, the online source of the documents or images subject to a breach of privacy may also be considered responsible for facilitating the activity. Therefore the holders of people's information need to take care not to be caught up in such an event.

2. Adapting and responding to the rise of technology

New privacy threats have developed largely out of the exponential growth in computer and online technologies and the commercial incentives to buy and sell consumer data, and there has been a corresponding shift towards recognising privacy as a consumer protection issue. This has been highly significant due to the worthwhile partnership the OAIC has been able to form with the ACCC to bolster their regulatory enforcement role. The ACCC is a far larger and better resourced regulator than the OAIC, and its involvement in the sphere of privacy protection is a direct response to the rise in technology. Unlike its counterpart in the US (the Federal Trade Commission), the ACCC has not traditionally been involved in the privacy sphere and until recently did not take action against organisations in relation to misleading and deceptive conduct concerning the collection, use and disclosure of personal information. However the ACCC has recently shown a willingness to act on such matters, for example when it commenced proceedings against HealthEngine for misleading and deceptive conduct. In this case the ACCC alleged that the online booking platform unlawfully shared patient data, including names, phone numbers, email addresses and date of birth, with insurance brokers.

The ACCC has also brought a successful action to address alleged false and misleading representations to consumers about the personal location data that Google collects, holds and uses. The ACCC's case focuses on Google's representations in relation to two Google Account settings: the 'Location History' setting and the 'Web & App Activity' setting. Google is alleged to have misled consumers into believing that their location history was not being collected when the Location History setting was turned off. In fact, the Web & App Activity setting also had to be turned off in order to stop Google from collecting the consumer's location data. The ACCC also alleged that Google misrepresented the purposes for which the data would be used. According to the ACCC, on-screen messages did not disclose to the consumer that their data might be used by Google for purposes beyond the stated purpose (being the consumer's use of Google's services). In April 2021

the Federal Court dismissed the allegations about Google's statements on how to prevent the collection and use of the data, and on the purposes for which the data was being used, but found that Google had made a misrepresentation about the settings that was liable to mislead the public.

This action against Google was not unexpected following ongoing privacy-related investigations by the ACCC since 2017 (including in relation to Google) and in its Digital Platforms Inquiry, the *Final Report* of which was published in June 2019. In the *Final Report*, the ACCC recommended, amongst other things, that Australia's privacy laws should be amended to include stronger consent and notification requirements; increased penalties under the *Privacy Act* (in line with the *Australian Consumer Law*); and, relevantly for the Google case, a broader definition of 'personal information' that captures technical data (such as location data and IP addresses).

The second change due to the rise in technology has been the commensurate consumer and public demand for government to do more to protect and educate the public in relation to privacy issues. As a direct result of this demand, the work of the OAIC has also been bolstered by the relevant work of the Office of the eSafety Commissioner (OeC). The OeC's education and reporting role has a specific focus on children and young people and it provides information and advice on issues concerning digital footprints and the intersections of privacy, security and safety. It also works collaboratively with the OAIC on online privacy issues.

In 2019 the government published the *Online Safety Charter*, which is a statement of the Australian Government's expectations of online service providers, including that they:

1.8 Consider security-by-design, privacy-by-design and user safety considerations which are balanced when securing the ongoing confidentiality, integrity and availability of personal data and information.

- Where the service or product is likely to be accessed by children:
  - minimise the collection and disclosure of children's personal data and avoid its detrimental use;
  - uphold rules and behaviour standards, including age restrictions; and
  - provide accessible reporting tools and guidance for parental controls.

2.1 Provide technical measures and tools that adequately allow users to manage their own safety, and that are set to the most secure privacy and safety levels by default.

- Implement mechanisms, including parental controls and access controls that effectively protect children from online harms, such as grooming, exposure to sexually explicit or graphically violent content, abuse, threats or cyberbullying.
- Make information about online safety available at all relevant points in the supply chain, including point-of-purchase, registration, account creation, first use and when they are upgraded or updated.
- Invest in tools and features that provide users with control over what they share, who they share with, the content they see or experience, and who can contact them.

- Actively promote age-appropriate online safety resources to Australian users and signpost support services that are relevant to Australian users.

A strong policy focus on eSafety in recent times does not envisage changes to the *Privacy Act* itself, but it does interact with privacy provisions and regulation, particularly in relation to children and the risks posed by breaches of privacy by commercial operators. The Australian government policy on digital safety confirms that issues such as doxxing and grooming online have a strong interrelationship with the enforcement of commercial privacy provisions in relation to children.[3] These issues are a focus of the new *Online Safety Charter* and *Esafety Strategy* (discussed below) and are expected to be reflected in the new *Online Safety Act*. The overall regulatory framework in relation to privacy is therefore further bolstered by the online safety jurisdiction which, while adding a further layer of protection for children, also arguably adds further complexity to an already complex area of law.

3. Monitoring and enforcement

As set out above, compliance with privacy law in Australia is monitored and enforced by the OAIC. While the intervention of the ACCC into the privacy sphere is important, its actions are currently limited to cases where a privacy breach may be considered to invoke consumer laws, for example conduct amounting to misleading or deceptive conduct, or occurs in an industry subject to the CDR rules. The OeC has a reporting function, but it refers breaches directly to the OAIC.

The OAIC operates a direct privacy complaints system which functions like an independent tribunal, and the Commissioner can also initiate investigations into privacy breaches, even without a complaint. The OAIC has statutory powers to: make determinations on privacy complaints where conciliation has not resolved a matter; accept an enforceable undertaking from an entity where it has cooperated with an investigation or enquiry; or issue a report of a Commissioner-initiated investigation.

The OAIC is also empowered to make Privacy Assessments of entities. An assessment is a professional, independent and systematic appraisal of how well an entity (or discrete part of an entity) complies with all or part of its privacy obligations. The OAIC approaches these assessments as an educative process, and compliance with the *Privacy Act* is seen as part of good management practice. The assessment process is usually commenced by the OAIC identifying an agency of concern and the selecting a proposed focus.

[3] Department of Communications and Arts, *Online Safety Legislative Reform* Discussion Paper (December 2019) https://www.communications.gov.au/have-your-say/consultation-online-safety-reforms, p 23.

In addition to its specific regulatory functions the OAIC collaborates with other regulators, conducts regular industry-based privacy reviews, and participates in the international privacy network, the Global Privacy Enforcement Network (GPEN).

Like other government regulatory 'watchdogs', the OAIC relies heavily on information from the public as to potential breaches of privacy in the online commercial space, including systemic issues. Such information will influence the OAIC's focus and its allocation of resources.

4. Protecting the privacy of children online

Australian privacy law does not specifically mention children and offers no additional protection for them. This omission is a significant concern for human rights lawyers and a focus of calls for reform. The submission to the Attorney-General's Department review of the *Privacy Act* made by Witzleb, Paterson and Jones on behalf of the Castan Centre for Human Rights Law at Monash University explains that:

> As recognised internationally in the UN Convention on the Rights of the Child ('CRC') and the Council of Europe's Convention 108, children and young people may require special protections because of their potential vulnerability. The need for protection arises because children have diminished capacity to understand the importance of privacy, affecting their ability to consent and creating responsibilities for third parties, notably parents and guardians, in protecting their personal information. (p 31)

Where data processing requires consent, the ordinary principles relating to the capacity to give consent apply to children and young people. Yet Australian law also holds generally that young people have a reduced capacity for consent to things that may be against their interests, or cause them harm. A child's consent to information processing is valid only if he or she has the requisite capacity, which in turn requires that the child have sufficient understanding and maturity to understand what is being proposed. Legal capacity must generally be determined on the basis of individualised assessment. Giving weight to the age and maturity of the individual child in assessing capacity is consistent with the approach taken in article 12(1) of the UN Convention on the Rights of the Child, the key provision on children's participation in decision-making.

The APPs affirm the general proposition that APP entities need to determine 'on a case-by-case basis' whether an individual under the age of 18 has the capacity to consent and that capacity depends on 'whether they have sufficient understanding and maturity to understand what is being proposed'. However, the Guidelines also suggest that, if it is not practicable or reasonable for an APP entity to assess a child's capacity on a case-by-case basis, the entity may rely on two presumptions: first, that an individual aged 15 or over has capacity to consent, unless there is something to suggest

otherwise; and second, that a child under 15 does not have capacity to consent. In practice, there is very little information available on how Australian organisations handle children's personal data and how they conform with the requirements under the *Privacy Act*.

ACCC reform recommendations

In its 2019 *Digital Platforms Report*, the ACCC made a number of recommendations that relate to children's privacy, including expressly recognising that the risks associated with data collection and use are particularly acute for children (p 447) and that younger children may lack the technical, critical and social skills required to engage with the internet in a 'safe and beneficial' manner.

The ACCC Report made recommendations for the immediate reform of the *Privacy Act*, to strengthen notice and consent requirements in relation to children and to amend the notice obligations in APP5 (Recommendation 16(b)). The ACCC pointed out that APP5 requires notices to consumers to be 'concise, transparent, intelligible and easily accessible, written in clear and plain language, provided free of charge, and clearly set out how the APP entity will collect, use and disclose the consumer's personal information'. It recommended the further provision that:

> 'Where the personal information of children is collected, the notice should be written at a level that can be readily understood by the minimum age of the permitted digital platform user'. (p 461)

The Digital Platforms Report also suggested multi-layered privacy notices or the use of standardised wording for particular categories of data or categories of third parties to whom personal information may be disclosed.

The Report also recommends strengthening consent requirements and proconsumer defaults in the *Privacy Act* generally. Recommendation 16(c) seeks to expand the circumstances in which consumer consent is required to every collection, use or disclosure of personal information (with some exceptions such as unless the personal information is necessary for the performance of a contract with the consumer, or is required by law or otherwise necessary for an overriding public interest reason. This requirement would align the Australian law with the European GDPR as discussed below).

In recommendation 18 the ACCC proposes more targeted regulation of the data practices of digital platforms via an enforceable code of practice developed by the OAIC, in consultation with industry stakeholders. Such a code could balance privacy rights with children's desire for increased transparency, accessibility and flexibility in their dealings with online service providers. A key strength of this approach is that it would also reduce reliance on notice and consent requirements which remain problematic.

5. International models

The US and EU have established models of privacy law that go further in some ways to protect children's privacy. The most useful examples for Australian policy-makers and legislators are described and summarised below. Some other international jurisdictions such as the UK, Ireland and Canada are, like Australia, currently engaged in rigorous reform of their privacy laws. All of these international models are known to Australian law reform bodies and have been thoroughly canvassed in submissions to the AG's Review. In the ACCC's Digital Platforms Inquiry Report, the recommendations for reform were heavily based on the EU model, the General Data Protection Regulation ('GDPR'). Importantly however, none of the overseas models is without limitations and there is no consensus among privacy experts on a clear best practice pathway to protecting children online.

United States

Due to the immense share of the digital technology market that is based in the US, the US digital privacy law is well established and well known internationally. The US has a specific federal statute entitled the *Children's Online Privacy Protection Act* ('*COPPA*'), that was enacted in 1998 and came into effect in April 2000. The law has followed the rise of technology through the work of a large consumer regulator, the Federal Trade Commission (FTC). *COPPA* mandates and requires the FTC to promulgate regulations on the collection of children's personal information by operators of commercial websites, online services and mobile apps. The allocation of responsibility to the FTC places *COPPA* in the sphere of consumer protection rather than human rights.

The key regulation, colloquially known as the 'COPPA Rule', requires websites and other online services that collect personal information from children under the age of 13 to provide notice to parents and to obtain verifiable parental consent before collecting, using, or disclosing personal information from these children. The COPPA Rule also contains a right for parents to review personal information provided by a child, to object to the further use or future online collection of their child's personal information and to direct the online service provider to destroy personal information that has been collected so far. The rule also outlaws specified unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.[4]

COPPA imposes a rigid age limit of 13 years and requires companies producing content for children to establish whether a child is 13 years of age. In recommendations released in 2012 the FTC

[4] See 16 C.F.R. § 312.3. to 16 C.F.R. § 312.6.

encourages operators also to adopt age-appropriate protocols for personal information collected from teenagers aged 13 and over, (pp 29, 60) but there is no statutory requirement to do so within *COPPA*. There is also no statutory requirement for operators of general or adult audience websites to verify a user's age. There are many obvious limitations to this approach, some of which are usefully set out by the Castan Centre Submission:

> 'the imposition of a rigid 'age of digital consent' may have indirect consequences harmful to children. For example, business may decide to no longer offer services for young people under the relevant age limit and that young people choose to evade the age limits by deception. Indeed, many general audience social media companies provide in their terms of service that account holders must be 13 years of age or older. These limits are set to avoid the restrictions imposed by COPPA. However, there is some evidence to suggest that children lie about their age in order to access these websites or that they manipulate verification procedures.' (p 35)

California

As the home of Silicon Valley, the State of California also has its own comprehensive privacy law, the *Californian Consumer Privacy Act* ('*CCPA*'), which is a general data protection law to regulate the handling of the 'personal information' but it also contains specific provisions relating to children, including restrictions on the collection and handling of children's information. In particular the *CCPA* states that a business must not 'sell' a child's personal information if it has actual knowledge that the he or she is less than 16 years of age, unless he or she, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorised the sale of the consumer's personal information.[5] The *CCPA* deems a business that wilfully disregards the consumer's age to have had actual knowledge and includes the requirement to ask young users their age so that the business can determine its obligations in relation to the sale of that information and also trigger the collection limitation in the *COPPA* rule.

Perhaps the most important feature of the CCPA, however, is the provision of a qualified right for a consumer to request deletion of data.[6] Allowing individuals to erase volunteered personal information once it is no longer required is recognised as especially important to children, who may have volunteered their information without fully understanding the full implications of doing so, allowing them to gain control their digital footprint as they move into adulthood.

[5] California Civil Code § 1798.120(c).
[6] California Civil Code § 1798.105(a).

European Union

In the EU, the GDPR is a general privacy statute but refers specifically to children in several of its articles and recitals. Six of its provisions provide specifically for enhanced privacy protection for children:

- **Article 6(1)(f)** – provides that personal data may lawfully be processed where it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child.
- **Article 8** – specifies a cut off age of 16 for consent in respect of the provision of online services by entities such as online marketers, apps and online content providers directly to a child. This can be varied to a minimum of 13 years by individual member states but where a child is younger than 16 (or such lower age as is specified by a member country), consent is lawful only if, and to the extent that, consent is given or authorised by the holder of parental responsibility over the child.[7]
- **Article 12** – deals with transparency and requires data controllers to provide the information required in privacy notices 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language, **in particular for any information addressed specifically to a child**'. This Article is complemented by Recital 58 below.
- **Article 17** – concerning the right to erasure. This article permits individuals to request the erasure of their personal data in specified circumstances, including where that processing has been grounded on consent and they wish to withdraw that consent. This Article is supplemented by Recital 65 below.
- **Article 40** – requires member states and supervisory authorities to encourage the drawing up of codes of conduct to contribute to the proper application of the provisions in the GDPR, and makes specific reference to children. This requirement and that of Art 57 below are monitored by the European Data Protection Board (EDPB).
- **Article 57** – requires the supervisory authorities that provide oversight over data protection in individual member states to give specific attention to public awareness activities that are addressed specifically to children.

[7] The Castan Centre noted a lack of uniformity among member states – Germany and Ireland adopt 16 years but most others have adopted between 13-15 as relevant age. See Castan Centre Submission, p 37.

These GDPR articles set out the binding legal requirements that must be followed and are supplemented by recitals, which serve as a similar type of function to the Explanatory Memorandum for an Australian Act. The relevant Recitals are:

- **Recital 38** explains that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. It also emphasises that this protection should apply in three situations, in particular:
    1. the use of children's personal data for the purposes of marketing;
    2. the use of children's personal data for the purposes of profiling them;
    3. the collection of children's personal data when they are using services offered directly to a child.
- **Recital 58** emphasises that 'any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand'.
- **Recital 65** emphasises that the right of erasure is particularly relevant where consent to processing was given while the data subject was still a child and not fully aware of the risks involved, and later wants to remove this personal data. It also stresses that this is especially important where the data is located on the internet.
- **Recital 75** lists risks to the rights and freedoms of natural persons that may result from personal data processing and lead to physical, material or nonmaterial damage. That list specifically refers to the 'processing of personal data of vulnerable natural persons, in particular of children'.

6. Challenges and risks

Many of the privacy related legal challenges and risks associated with children's online engagement with commercial interests have been previously outlined above in this paper and they include issues concerning the digital age of consent and the existence or otherwise of a right of erasure.

Social research also suggests a significant challenge associated with parents or guardians consenting to share children's information. In a community where there are not well-established and understood norms as to the importance of protecting children's privacy, many parents and guardians are not equipped to undertake this responsibility in a way that preserves their children's rights. If it were accepted that this is beyond the capacity of most caregivers, arguably the public interest would lie in reducing the importance of parental consent in privacy law and enhancing the

emphasis on safety by design. The other key challenge is that of children readily accessing sites that are not designated as child-oriented, as there will be lower consent and privacy alerts required for adult-oriented services.

Due to these challenges, when children engage online with commercial interests there is a direct and relatively high known risk of a breach of their privacy.

Another set of challenges arises from the fact that business or individuals who own the app or site, and who bear responsibility for compliance with privacy law in Australia, are likely to be based overseas. Australian law will generally have limited control over the actions of an international entity for a breach of privacy, and if the entity is able to escape the effects of regulation, there is a question whether Australian privacy law has 'teeth' when breaches occur. That said, where products produced by international companies are readily available in Australia and are found to be in breach of Australian legal standards, it is still possible to notify Australian authorities and invoke the powers of Australian regulators (OAIC, ACCC). While the Australian regulators may not necessarily have powers to impose sanctions international companies themselves for privacy breaches, they are able to issue notices, inform other international regulators and in serious cases take legal action to reduce the company's access to Australian markets.

7. Risks of covert tracking of children

Whether the covert tracking of children under the digital age of consent is unlawful would depend in most jurisdictions on whether the company was collecting 'personal information' about the child, whether a parent consented to this and whether any breach of privacy would be likely to cause 'serious harm'.

In a 2015 'Privacy Sweep', OAIC joined with 28 other international privacy enforcement authorities to examine 38 free websites and mobile apps targeted at children aged 12 and under. Globally, participating privacy enforcement authorities examined 1,494 websites and apps targeted at, or popular among, children. Sweep participants looked at whether the website or app collected children's personal information, and if so, whether protective controls existed to limit that collection. The then Acting Australian Information Commissioner, Timothy Pilgrim, stated that while covert tracking is limited in entertainment apps targeted at children, 'many of the most popular apps and websites used by children are not specifically designed for children and as such do not incorporate child-appropriate privacy measures'. Even the finding of limited covert tracking in children's apps is now subject to question following research released in 2018 by the International Computer Science Institute at the University of California, Berkeley. The research consisted of an

automated analysis of 5,855 of the most popular free children's apps and found that a majority were potentially in violation of *COPPA*, because they did not disable tracking or behavioural advertising.

8. The potential harm to children

Breaches of privacy raise a number of general risks, not just to children: for example, personal information can be used in identity theft or to target people with scams; or to discriminate against people and exclude them. The information that might be collected is not just demographic in nature (for example addresses and place of birth) but it might include psychographic information (for example attitudes and beliefs), which can be used to manipulate users with commercial and other messages.

These concerns are heightened when the information relates to a child. Children are more prone to things like manipulation or adverse effects from exclusion when their data are collected and misused. They are also more vulnerable to cyberbullying and grooming, which becomes a risk if location information is gathered. Similarly with advertising and the creation of desire for products that are not in their interests. Children are also at heightened risk of data collected influencing later opportunities for study or employment, if only because they have more of life ahead of them.

These known harms can be difficult to quantify in terms that may invoke the current 'serious harm' criterion of Australian privacy law (discussed above). This is perhaps why the consumer law aspect, where companies are engaged in misleading conduct that also constitutes a breach of privacy, is easier for regulators to pursue than a privacy law breach: the misleading conduct is unlawful in and of itself, and there is no need to demonstrate a particular level of harm. That is not to say that real and serious harm does not occur as a result of privacy breaches, but more research into the digital footprint over time is needed to be able to demonstrate this.

9. Law reform activities

At the time of writing (early 2021), there are ongoing law reform and regulatory activities that consider the effect of the *Privacy Act* in Australia and are relevant to children's interaction with online commercial entertainment media. A great deal of expertise and research is being directed to children's privacy in Australia through these activities.

The most significant of the activities is the Attorney-General's Department review of the *Privacy Act*. This was announced in November 2019 as part of the Commonwealth government's response to the ACCC's Digital Platforms Inquiry. The Terms of Reference cover:

- scope and application of the Privacy Act
- whether the Privacy Act effectively protects personal information and provides a practical and proportionate framework for promoting good privacy practices
- whether individuals should have direct rights of action to enforce privacy obligations under the Privacy Act
- whether a statutory tort for serious invasions of privacy should be introduced into Australian law
- the impact of the notifiable data breach scheme and its effectiveness in meeting its objectives
- the effectiveness of enforcement powers and mechanisms under the Privacy Act and how they interact with other Commonwealth regulatory frameworks
- the desirability and feasibility of an independent certification scheme to monitor and demonstrate compliance with Australian privacy laws.

While these make no reference to children's needs or rights, the Issues Paper released in October 2020 included, as one of its specific questions, 'Should specific requirements be introduced in relation to how entities seek consent from children?' Submissions in response to the Issues Paper were received from a broad range of stakeholders. There will be a further Discussion Paper, consultations and a final Report and recommendations.

Running parallel to this review, the Commonwealth is also working on reforms to the online safety legislative framework. This is focussed on offensive and harmful content and conduct rather than privacy, but it is relevant to the issue of children's interaction with online businesses and can therefore affect privacy regulation indirectly. Importantly, the eSafety review has an explicit focus on children, and appears to more clearly articulate potential harms for children in the digital media environment, some of which may be privacy related.

The Discussion Paper for the reform states that:

> The Government has committed to working with online service providers to make online apps, games and services marketed to children default to the most restrictive privacy and safety settings at initial use or set-up. While many services currently provide the option of privacy and safety settings (for example Microsoft Family or Apple operating systems), information on what is available for consumers is not always transparent and accessible. The Government is looking for industry to ensure that products marketed to children default to the highest level of privacy and safety at the outset, and to enable consumers to set and adjust these controls as they wish. It would be preferable to have these enhanced safety features developed and implemented voluntarily through an industry wide commitment to safety, consistent with the SbD *(safety by design)* principles and basic online safety expectations. However, in the event that a sector of the industry or particular service providers don't adopt this as a standard practice, the Government will consider the merits of empowering the eSafety Commissioner to specify, by legislative instrument, that particular types of service, or individual service providers with services marketed to children, default to the most restrictive privacy and safety settings. (p 23)

The government is running a public consultation on consolidating existing legislation into the form of a new *Online Safety Bill*. The Bill is expected to incorporate the previously published *Online Safety Charter* (see above).

It appears likely that the OeC will need to collaborate with the OAIC in order to enforce these standards.

Australia's *Cyber Security Strategy 2020* is another ongoing general policy and law reform activity that touches on privacy. While it does not have any particular focus on children's data, this strategy does emphasise the connection between identity theft and cybercrime.

Finally, the UN Committee on the Rights of the Child has recently adopted General Comment 25 (GC25) on children's digital rights, which includes a clarification of their right to privacy. A detailed discussion of the impact of this on law reform is beyond the scope of this paper, but as a signatory to the CRC, the Australian Government is required to consider the implications for law reform, and the General Comment should feature in the above domestic law reform activities. The discussion at the UN Committee level concerning encouraging the use of end-to-end encryption to manage children's data is an important reflection of the complexity of privacy law and its interaction with criminal law enforcement. In its submission to the CRC on GC25, Australia expressed reservations about end-to-end encryption, on the basis that 'predators and grooming groups … may use end to end encryption and other technology to carry out and conceal their illegal and harmful activities'. The submission also qualified Australia's support for children's right to privacy to 'arbitrary or unlawful' breaches.

10. Getting involved

The most effective way for parents and guardians to engage with these issues is to respond to and participate in all calls by the regulators (OAIC, ACCC, OeC) for public contributions to discussion, and to supply information to any or all of the regulators about interactions and experiences with any privacy issues their children experience online, either good or bad. There are links in the text above to websites inviting comment from the public.

The OAIC suggests that individual notifications of both good and bad examples of privacy practices by apps and online games are highly useful to their work, and invites parents/guardians to notify the OAIC or OeC via their websites as to any concerns or observations. The OAIC's results and the global results from the GPEN Privacy Sweep have identified the following examples of good and bad privacy practices on websites and apps targeted at children that parents/guardians should bring to their attention:

Examples of good privacy practices on websites/apps targeted at children

- Providing users with pre-created avatars to use when navigating the site, removing the need for children to create their own avatars and to use their own information.
- Warning children not to use their real names when setting up an account.
- Having a chat function that allows users only to select words and phrases from a pre-approved list, instead of typing freely, so that children could not disclose their personal information inadvertently.
- Automatically offering children under a specified age an alternative version of the app: child-centric alternatives appear to collect and share less personal information compared to the adult-version of the app.
- Tailoring protective communications to children by writing in plain, age-appropriate language or delivering their messages in some other child-friendly way.
- Having an age verification or gating to bar younger children from accessing the site or app.
- Encouraging parental involvement.

Examples of bad privacy practices on websites/apps targeted at children

- Inadequate or non-existent privacy policies, or lengthy and complex privacy policies.
- Over-collection of personal information, for example, collection of exact date of birth instead of simply the year/month of birth to verify a user's age.
- Failure to use simple language, or failure to present warnings that children can easily read and understand.
- The potential to be redirected to another website via advertisements, for example via an advertisement or contest which has the appearance of being part of the original site.
- Unclear or generic privacy policies that provide little information about why a particular site or app is collecting personal information.
- Ineffective age verification or gating tools, for example, controls that do not function (e.g., a child indicating she was 10 years old can still access the site) and others are only passive (e.g., a pop-up indicating that a child below a specified age should not access the site).
- No accessible means of deleting account information.

Reporting bad practices would assist the OAIC to track these providers and consider further action to require their improved compliance. Reports can also encourage good practice and, through the OeC, use levers of good publicity to enhance community expectations and values as to privacy standards.

****

The LAW FOUNDATION of SA Incorporated

ACCM acknowledges the support of the Law Foundation of SA which funded the research for, and publication of, this document.