Is children's privacy protected under Australian law when they use online game apps?

Short answer: **No**

Longer answer: Australian privacy law is really complex, so strap in for an explanation.

1. What do we mean by privacy?

For a lot of people, the idea of 'privacy' is about being able to do things without other people looking. You might hear about paparazzi taking photos of celebrities over the fence and think: that's an invasion of privacy. But when we talk about children's online privacy, we are usually referring to the way that websites and apps (online providers) collect information about them, and how that information is then used. The information might be demographic (like an address or date of birth) or psychographic (like the user's likes, dislikes, attitudes and beliefs). It also includes 'inferred' information, for example an online provider might know from geolocation that you have attended some kind of medical clinic, and work out (or presume) that you have a particular kind of health condition.

Privacy issues also arise when online providers have access to communications functions on our devices; or to sound and vision from wherever the user is (including at home). However Australian law has so far focussed mainly on the question of what information people can collect from us, and what they can then do with the information.

2. What is the harm if children's privacy is not respected?

There are a number of general potential harms from privacy breaches, 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. Psychographic information (see above) can be used to manipulate users, for example to make an online experience 'stickier' so the user stays engaged for longer.

As mentioned, these are concerns for everyone, but the concern is 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. Also there are all the possible future uses of information that could affect the child's life into adulthood. This is troubling even if consent has been given, but all the more so where it has not.

3. What laws and procedures are there to protect the privacy of online app users?

The most important law, the Commonwealth *Privacy Act 1988*, sets up the 13 Australian Privacy Principles, or APPs for short. These guide the actions of bodies called 'APP entities', which include all

government agencies, all businesses, all not-for-profit organisations with a turnover of more than $3 million a year, all health service providers and all organisations that trade in personal information. You can download a document with all the APPs here, or a simplified version can be found here. They cover:

1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use or disclosure of personal information
7. Direct marketing
8. Cross-border disclosure of personal information
9. Adoption, use or disclosure of government related identifiers
10. Quality of personal information
11. Security of personal information
12. Access to personal information
13. Correction of personal information

Some kinds of information have stronger protection because they are seen as especially sensitive. These include medical and financial information, but not children's information as such. There is no special protection for children in the APPs.

The APPs are enforced by a Commonwealth agency called the Office of the Australian Information Commissioner (OAIC). This body is also responsible for enforcing other laws, for example the *Freedom of Information Act*.

The OAIC receives complaints from individuals about the handling of their personal information by APP entities, and it also has quite broad powers to regulate those entities directly.

The OAIC also gives information and advice on privacy to individuals, businesses and agencies; and occasionally it brings court cases against entities that appear to have breached the APPs. In 2020 it brought its first ever action, against Facebook for serious and/or repeated interferences with privacy.

The APPs cover things that entities do on purpose, but the OAIC also has a role when an entity holds information and somebody else accesses it without authorisation. When this happens, it is called a data breach, and if it is likely to result in serious harm, the entity has to inform the OAIC.

Serious harm means more than making someone upset or distressed, rather it means serious physical, psychological, emotional, economic or financial harm, as well as serious harm to reputation.

If a child's personal information were accessed during a data breach, it's unlikely that the potential harm would be considered serious just because the information related to a child. The age of the people whose information was accessed might be a relevant consideration in deciding seriousness, but not enough in itself to make the harm serious.

Privacy law also intersects with consumer protection law, or the law that governs our rights when we buy something for our own use. Concepts like 'misleading and deceptive conduct' and 'fit for purpose' come from consumer law, and it is quite a powerful tool for protecting those who need it.

It is administered by the Australian Competition and Consumer Commission (ACCC), which is a powerful and well-resourced regulator, but the law it administers applies only to bodies engaged in commercial transactions.

The ACCC has applied traditional consumer protection rules, like the one against misleading and deceptive conduct, to online providers for the way they manage personal information. At the time of writing, it had recently won a case in the Federal Court against Google, which was found to have misled users about how to prevent the tech company from keeping or using information about their location. Because of its size and powers, the ACCC is potentially an important actor in this field.

Another government body with a role to play is the Office of the eSafety Commissioner. It collaborates with the OAIC in privacy matters as well as publishing information and advice on issues such as digital footprints and the intersection between privacy, security and safety.

4. What are the special issues for children in privacy protection?

The *Privacy Act* doesn't have any special provisions for children, but the APPs do address consent to the collection and use of personal information, which is a significant issue for children. Because Australian law generally recognises that children have less capacity than adults to give consent to things that might harm them, it's necessary to look at individual children to see whether they have the maturity to understand what they are being asked to agree to. The APPs support this approach, but they also recognise it won't always be possible for an online entity to judge an individual child's capacity. In those cases, they are allowed to presume that anybody over 15 has the capacity to consent, unless there is reason to think otherwise, and that anybody under 15 does not have the capacity.

Many online providers have an age cut-off of 13 to have an account or a profile. This is due to US legislation, which aims to protect children's privacy. And yet we know that as a result many children lie about their age in order to get access to popular sites. When this happens, the child doesn't get any age-appropriate privacy protection from the site, rather the site will approach matters of consent and disclosure as it would for an older person.

When an online provider (such as an app, or a social media site) collects personal information it is likely to want to use the information to its advantage (for example by sending the person marketing messages), or to sell it on to somebody else who wants to use it for similar purposes. This can include 'online profiling', or putting together a picture of a person's likes, insecurities etc based on their online activities. The profile is then used to target advertising, but it could be used in other ways as well. Research by the ACCC, and by a team at the University of California, Berkeley, shows that many websites and apps not only collect children's data but track children without them knowing ('covertly').

While there is a general problem for everybody in having our information used in ways we didn't choose, it becomes greater when the information is about a child because the uses to which it is put might be simply inappropriate for children, even with consent. For example, they might be targeted with advertising for inappropriate products, or that might be misleading to them (even though an adult might understand it properly).

Another issue is when a provider directs users to other websites. A parent might give a child permission to play on one site because it seems appropriate but then the child clicks a link and ends up somewhere very different, including having different standards and practices for users' privacy.

The Commonwealth government is bound by the requirements of the United Nations Convention on the Rights of the Child. These give it a delicate balancing act to perform between allowing children freedom to use the internet, as a source of information for example, and protecting their privacy while they are doing so – both rights that are listed in the Convention. The UN Committee that looks after the Convention has recently released a statement about children's rights in the digital environment and this should be helpful in starting a conversation about how to get that balance right.

5. What more could the law do for children?

The ACCC put out a report in 2019 recommending some ways of strengthening privacy law to protect children better, at least on digital platforms like search engines, social media platforms and content aggregation platforms (like Google News). Some of the improvements they suggested are:

- making it harder to collect, use or disclose children's personal information for targeted advertising or online profiling
- minimising the amount of information about children that is collected, used and disclosed
- setting a minimum age below which children can't legally consent to collection of their data, and strengthening requirements about parental consent
- simplifying privacy notices so that children can understand them
- generally making privacy notices easier for everyone to understand
- generally expanding the situations in which consent is required, to include any collection, use or disclosure of personal information, with only specific exceptions

The government is not required to accept any of these recommendations.

6. How are the laws enforced?

We mentioned earlier that the ACCC can take action in court against companies that it thinks have breached consumer law. The OAIC can also bring court actions, but it has done so only once. Mostly it conducts its own investigations (including on data breach incidents, see above) and issues reports on those; and acts on complaints by members of the public. If a complaint is not resolved by conciliation, the OAIC can make its own determinations and accept an enforceable undertaking from an entity. This is a promise to do or not do certain things, and if it's broken the entity can be taken to court. So an entity that breaches somebody's privacy gets a chance to mend its ways before there is any kind of legal penalty.

7. How does all this apply to children who use gaming apps?

A child who wants to play a game on an app might be asked or even required to hand over some kind of personal information, for example an email address or a date of birth, or to give the app permission to access other things on the device being used, for example contacts or location. When this happens, some questions need to asked:

- Is it really necessary for the app to have that information?
- Should the app be seeking the child's parent's consent instead? If so, how should it go about that?

- How informed is the consent? Does the app provide clear and understandable information about what the child or parent is consenting to?
- How is the information used? And especially, what uses are there outside of the actual game-play, for example to target the user for advertising? Is the user given enough information about this before consenting?

The law has the potential to help at every stage of this process: whether the app is allowed to ask for information, how it should ask for and get consent to collect and use information (including the information it should provide) and how information can be used. But there aren't any rules in place about these things at the moment.

Conclusion

There is evidence of widespread collection and use of children's data when they play on apps, often done covertly. Yet despite children's extra vulnerability to having their privacy compromised, and to special risks of harm when that happens, Australian privacy law doesn't provide them with any special protections. Their information is not treated as especially sensitive, and there are no requirements about getting parental consent to share the information. It remains to be seen what, if anything, the government will do in response to the ACCC's 2019 recommendations, but meanwhile parents and carers can help keep children's information safe by always asking questions about any app a child might want to play.

If you'd like more information, including information about other reform proposals, you can read our more detailed report https://childrenandmedia.org.au/assets/files/resources/reportaccmprivacyresearchproject.pdf.

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.