# Children's digital privacy – what are the risks?

## INTRODUCTION

### *Australian children online*

Being online has become an integrated part of family life for most Australian children. Nearly half of children aged over six use a device of their own, and by the age of thirteen, the majority own a mobile phone. Technology, intelligent devices and connectivity are part of how we socialise, how we have fun, and how we learn new things. The development of intelligent and intuitive devices, in particular touch screens and voice activated technology, means that even very young children can navigate and enjoy interacting playfully with online technology. For Australian teenagers, online connectivity is a tool not just for education, but for building social networks and expressing creativity and identity.

Today's parents did not experience this kind of internet-integrated childhood, even those younger generation parents who might consider themselves to be "digital natives". The infiltration of online technology into family homes and family life is growing incredibly fast, with no clear blueprint on how to navigate the risks. Parents are uncomfortably aware that despite the benefits of online connectivity, there are safety issues. Many feel overwhelmed and ill-equipped to protect and educate their children about online risks.

### *Privacy is a Safety Issue*

Common safety concerns that parents identify are:

- inappropriate content;
- online predators;
- digital addiction; and
- cyber-bullying.

Parents also identify risks to our privacy, and the commercialisation of personal information, as genuine concerns. Most parents feel that protecting their children's information is an important issue and are even more concerned about their children's privacy than their own.

The exponential growth of apps, many of which are free and offer benefits such as communication tools, social networking, games, education and entertainment, comes at a price: our personal information. *Data mining* (collecting personal information from consumers) is far more extensive and intrusive than most people realise. Through the apps that we have on our devices, and the 'smart' technology in our houses (appliances, toys and technology in your home that are connected to the internet) **our locations are being tracked, our behaviour monitored, and our voices listened to**. Surveillance is being covertly embedded into our homes and family life.

### *My Digital Footprint Belongs to Me*

Each one of us has a digital footprint. It is a collection of accumulated pieces of information about our lives, stored online. The more time we spend engaging online, the more personal and detailed our digital footprint becomes. Parents and caregivers need not only to take responsibility for their own digital footprint, but also to be the caretakers of their children's. Children and adolescents do not have the developmental capability to understand fully how and why their personal information is valuable, or why it might be exploited as a commodity. These are complex concepts, and that is why consent needs to be guided by parents.

Nevertheless, children can be taught that their personal information, their *digital footprint*, has value. In developmentally appropriate ways at different ages, parents, caregivers and educators can help children to take responsibility and ownership of their online information. They can help to teach them safe practices and ways of mitigating the risk of their personal information being used in harmful ways. *Children can understand that they have a right to privacy and develop the skills to protect it.*

## WHAT ARE THE RISKS FOR CHILDREN'S DIGITAL PRIVACY?

The apps that children download are gathering information. While some children's apps collect only the information required for using, updating and improving the product, many will 'mine' children's data in order to monetise or increase their profits by selling on this information to third parties. *Third-party trackers* are small pieces of code that are embedded into an app to give other companies (not just the app developer) access to the information on the device. Several studies have discovered that apps targeted towards children have a very high rate of third-party trackers in comparison to apps for adults. Many of these apps do not seek adequate parental consent for the information they collect and have been found to breach privacy regulations for children.

### *What information do apps collect?*

There are lots of ways that apps use devices to collect information, but these are some of the most common methods:

**Personal information**
Also understood as *personally identifiable information* (PII), personal information is basic information such as name, date of birth, gender, email, and address. Any app that requires signing up for an account is usually collecting personal information. Checking the app distributor's privacy policy may help to understand why and how that information will be used.

**Advertising ID**
This is the most common piece of information collected by apps. It is an identifier which gathers data about how you use your device or your activity within an app, for example, the posts you 'like' or 'share' on Facebook, the tweets you 'retweet' on twitter, or the items you search for on eBay. This creates a profile about your behaviour that is useful for advertisers. Data can even be used to identify and establish your vulnerabilities in real time (such as feelings of low self-esteem or loneliness) for exploitation by advertisers.

**Voice and Audio Information**
When you download an app that requests access to your device's microphone, it is possible that you are allowing the app to listen and record your conversations through your device. This may be limited to the time when you are using the app, but some may request 24-hour access to your microphone and so can continue to listen even when you are not running the app. This technology can then identify and target you with topics or ads for products that might interest you.

**Location**
It is very common for apps to request to use location data. This can either be general (sometimes described as 'coarse') or precise. Devices usually have geo-location software inbuilt and the app can access this information. Sometimes location information is accessed by requesting your wi-fi, network, router or IP details. The purpose of this is usually to target advertising that is relevant to where the user lives.

**Gameplay**
Some game apps will request to record gameplay behaviour. This helps developers to identify what keeps people playing the longest, and what keeps them coming back for more. Many psychological tools are used to keep people in gaming environments for as long as possible, for example, advertising revenue and in app purchases require users to be at the screen as much as possible to maximise profits. Collecting gameplay data is useful for proving what works and what doesn't.

**Camera and Photos**
Apps that request the use of your camera or phone are usually using it to enable the functioning of the app, for example, being able to edit photos or make collages, or

for posting photos on social media. However, in gaining access to your camera it can use the camera to watch you, sometimes even when the app is not open. When you grant access to your photos, apps can have access to your entire photo library, not just the ones you choose to share or use when the app is open.

**Contacts**
Some apps will request access to your contacts list on your device, or your friends on social media. Some apps need this information to work well, but others will use it to gather information on your networks and for selling to third-party advertisers.

## *What are the risks for children?*

There are many reasons to be concerned about the invasion of children's privacy. Some of these reasons are easy to understand as they have an obvious negative impact on our lives. Others are more abstract and don't seem to pose any immediate threat. However, they are still problematic and need to be considered. Here are some of the risks associated with tracking and collecting children's information:

**Persuasive Design and Digital Addiction**
Most information collected via tracking in apps is, at the present moment, used for the purposes of making advertising more persuasive and more relevant to the user.

'Persuasive design' uses knowledge of psychology and human behaviour to influence people's decision making and actions. Persuasive design practices are used widely in online advertising, and they become even more influential and powerful when combined with targeted advertising. Persuasive design also plays a large part in both online gaming and social media platforms. Information collected on gaming behaviour and social media activity can be used to make these activities 'stickier' on an individual level. In fact, senior executives from big tech companies have openly stated that the products are designed to be 'addictive' or to get users 'hooked'. Keeping people engaged within the platform for as long as possible translates into money for the distributor, so getting children dependent on games and social media is good for business. Children are highly vulnerable to these psychological tactics and there are substantial risks and consequences to developing digital addiction. Digital addiction in children has been linked to a range of negative outcomes including poor academic performance, substance addiction, obesity, muscular-skeletal and optical problems, low self-esteem, anxiety, stress and depression.

**Psychological Exploitation**
Children, in particular those under the age of 12, do not have the developmental ability to understand the biased and persuasive intent of advertising and so are more vulnerable to psychological coercion and manipulation from advertisers than adults are. Children have difficulty resisting the pressure to spend money online as the result of persuasive advertising.

**Identity Theft and Fraud**
Making a lot of personal information available to unknown third parties leaves children more vulnerable to identity theft and fraud as they grow older. Although many apps claim that the information they collect has been 'de-identified', anonymity is rarely guaranteed and there is a high chance of privacy violations. The capability of organisations to handle and store personal information safely is not uniform and data breaches are common.

**Online Predators**
Allowing detailed information about your children to be accessed on the internet, such as photos of them, where they live, and where they go to school, could increase

their risk of being targeted by online predators, thereby posing a physical threat to their safety.

**Intrusive Surveillance – Becoming Desensitised**
The cost we pay for the convenience and benefit of a 'connected life' is to live in a state of surveillance. Because this surveillance is mostly invisible, it is easy to ignore and tolerate. Having a complacent and tolerant attitude towards digital surveillance could be demonstrating to our children that it is a completely normal and acceptable part of life. Whilst it may be difficult to see this as a threat now, we don't have any control over how information will be collected or regulated in the future. Teaching our children to think critically and to value and protect their privacy will benefit them now and in the future.

**Children's digital footprints may define their future**
Digital footprints are growing more and more accurate and detailed over time. Tech platforms have a staggering amount of information already connected to Australian children, which may include information such as: their likes and dislikes, the sports they play; the books and media that they love; the socio-economic status of their parents and the schools they attend, even details of health conditions that run in their families. The list goes on. In the current climate, it's hard to imagine why this information would matter. If it is only used to advertise things to them, it may not feel like a serious risk. However, we must consider the possibility that over their lifetime, information could be used in ways that we have not anticipated. It could even be used to define and shape their future – for example, to determine acceptance into University courses, which health insurance they could access or which applicants get scarce jobs. Teaching children now, to think critically and to value and protect their privacy, will better protect them from arbitrary discrimination in the future.

### *Are there laws that protect my children's privacy?*

At the moment, there are no privacy laws in Australia specifically mentioning the privacy of children, and therefore there is no special protection. Children are considered to be under the supervision of their parents up the age of 18 and are afforded the existing privacy rights given to all Australians.

However, the United Nations Convention on the Rights of the Child says children have a right to privacy (Article 16) and recognises that children need special protections because they are more vulnerable than adults. Their ability to give consent is compromised by the fact that they don't fully understand the importance of privacy. This highlights a need for reform in our privacy laws.

Many parents know that privacy laws exist for Australians, but don't know enough about them to know if they are adequately protecting the privacy of their children. If you would like more information about how you and your child's privacy is protected in Australia, or if you'd like to know how you can advocate for stronger and better legal protection for children's privacy, you can find out more here: https://childrenandmedia.org.au/resources/australian-privacy-law-is-it-protecting-our-children-when-online

## WHAT OTHER TRAPS WITH APPS ARE THERE?

In addition to risks involved with children's digital privacy, there are other traps with apps which, while not necessarily invading children's privacy, also place them at risk.

Here are some examples of common traps with apps:

**In-app purchasing**
Many apps are purposely frustrating if you are unable to buy extra items to play with, extra levels, in-game currency, or extra content. In some games you need to make

purchases to progress in the game. Parents need to take great caution that their children are unable to make payments on their device without parent permission. The simplest way to avoid a hefty bill is setting up a password for purchases. The pressure for in-app purchasing is most common in apps that are free to download, so you might also consider it worthwhile to pay a small amount to buy an app instead.

**Simulated gambling activity**
Many children's apps contain psychological strategies that are used in the gambling industry. Children are encouraged to risk something of value, such as in-game currency, and 'gamble' on getting something even more valuable in exchange. A common example of this strategy is a 'loot box', which is found in many games and apps. Not only do these tactics keep children addicted and hooked in, but they also increase the likelihood of a young person developing an actual gambling problem.

ACCM provides reviews of popular children's apps which are specifically designed to capture these common risks as well as let you know about inappropriate content. You can find them on our website:

https://childrenandmedia.org.au/app-reviews/

## TIME TO ACT?

Recognising that your children's privacy is worth protecting is fundamental, but what can we do to safeguard their privacy until they are old enough to take it on independently? How can we teach them the skills to manage their own privacy? It is easy to feel overwhelmed, but with some simple strategies, parents can reduce the risks and help their children to learn.

For some practical tips and advice, read our guide, *Steps parents can take to protect their children's digital privacy*:

https://childrenandmedia.org.au/app-reviews/apps-can-trap-tracking

**********

MACQUARIE University
Produced in partnership with the Macquarie University Department of Psychology.

accan
ACCM acknowledges the support of the Australian Communications Consumer Action Network (ACCAN) which funded the research for, and publication of, this document.