le.committee@aph.gov.au
Commonwealth Parliament of Australia
Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600
Phone: +61 2 6277 3419
le.committee@aph.gov.au

9th March 2023

Dear Honorable Committee Members of the Parliamentary Inquiry into Law Enforcement Capabilities in relation to Child Exploitation,

Further to our original submission. I am writing more detail on a growing concern regarding child exploitation on the popular online gaming platform Roblox and also daycare and early primary school journaling apps.

Roblox

Roblox is an interactive, multi-player, user-generated 3D world with over 43 million daily active users, exactly half of whom are aged under thirteen years. Despite the current recommended age rating for Roblox being 12+ on both the Apple store and Google Play stores, the game is downloadable on all smartphones, tablets, devices, desktop computers, Xbox, and Nintendo Switch. There is no age verification beyond the age recommendation guideline of 13+ in the Terms and Conditions of use.

My team at Safe on Social has received numerous reports from children under 13 during every single session we conduct, where they have been asked to be someone's boyfriend or girlfriend in the game while playing Roblox. Some children have been asked to be the Mum or Dad in role-playing games in exchange for free Robux, the in-game currency, to be "adopted" or to lay down on top of someone else's avatar. Parents have reported that their children have seen nude or semi-nude avatars within the platform, simulated sex and sexual acts between avatars within certain role-playing games, and are often asked to date, other players. Sexualised and crude language is also frequently observed, which would usually be blocked or restricted by Roblox child safety filters but has somehow been bypassed. Parents are often too scared to speak up to law enforcement or government agencies for fear that they may be shamed for being bad parents for letting their child use apps under 13yrs.

Australian children using Roblox are being exposed to online grooming and predators, and law enforcement agencies must take action to address this issue. As mentioned in our original submission, in a recent disclosure, a little girl aged 11 years old disclosed that her in-game character was sexually assaulted. She described the incident in detail and referred to her in-game character as "me". Little ones create these avatars as an extension of themselves; therefore, the trauma can be as if it has happened in the physical realm. Predators are using this

to normalise predatory behaviours towards children. There is no central body to report these disclosures so law enforcement training in cyber safety can keep up to date. Unfortunately, they will always be lagging due to the fear of disclosing this kind of information to a police officer presenting at a school. As we are a private organisation, we get told a lot but have nowhere to report things that are not mandatory but are certainly triggering predatory trends and could be used as a preventative training measure.

I urge the parliamentary inquiry to take this matter seriously and consider implementing stricter measures to protect young children on Roblox and other online gaming platforms. We must proactively safeguard our children's online experiences and prevent child exploitation.

Childcare and early primary school apps

While the internet provides immense benefits, it also poses significant risks, particularly for children. Child exploitation and privacy risks associated with digital technology have become a growing concern, as predators have found ways to exploit the anonymity of the internet to target children. As such, it is crucial to take a proactive approach to child safety online to protect children and create a safer and brighter future for all.

Online child exploitation has become a significant concern, with predators using online gaming platforms and social media to engage in inappropriate behaviour with children. For example, on Roblox, an online gaming platform, predators can offer children money (usually in-game currency) for sexual acts, engage in role-play games that involve sexual activity, and move conversations to other platforms such as TikTok, where children can be groomed, sextorted, and threatened.

It is essential to invest in up to date education in training for educators, staff and parents to track and analyse online activity, particularly on social media and messaging apps, where predators often move their activities. Law enforcement must also have the necessary resources and expertise to identify and apprehend predators, including working closely with companies operating online platforms to identify and report suspected abuse.

Local community social media groups frequently feature callouts from parents asking for recommendations for the best childcare centre, or sometimes advice on which ones to avoid. Many centres and schools are recommended based on the use of their centre App, and how engaged the service is, with the App keeping you up to date on everything your child is doing during the day.

The App, you will be told, makes life so much easier. You'll be sold on how much information is put into it. General newsletters, the weekly menu, photos of your child, observations, and reflections, you'll know just how much they slept and ate and all about their toilet habits.

App and software developers have seen the benefit of creating childcare (and school) Apps. The industry is lucrative and seemingly has an infinite future supply of user accounts.

When we as adults download an App, we consent to the Terms and Conditions, whether we read them or not, and honestly, how many people really read the fine print?

By simply downloading and ticking that little 'I agree' box, we are consenting for our own data to be used by the App as well as consenting to permissions such as accessing our photos, comments, phone contacts, and sometimes even our location. We understand that we are adding to our own digital footprint, and for the most part, that's fine, we're adults, and we get to make that decision. But what happens to the rights of our children? What data are the apps collecting, and who can see it? How will the data these apps collect affect them in the future?

These are the questions we raise regarding the Apps that most childcare centres enforce for communication purposes when a child first attends their centre or when the Centre chooses to introduce one.

The list is quite exhaustive, with new Apps popping up all the time; however, some of the most popular Apps that childcare providers are currently using include (but are not limited to):

· Xplor
· OWNA
· HiMama
· Brightwheel
· KidKare
· Sandbox
· Kidsoft

Primary and Secondary Schools are also mandating the use of Apps, including Sentral, SeeSaw, School Stream, Skool Loop, and SkoolBag, to name a few.

The use of Apps in a childcare and school setting is very commonplace but what many don't realise, is that when we as parents and/or carers agree to these Apps on behalf of our children, we are aiding in the creation and building of their digital footprint, a footprint that they have no control over, and this footprint can be very sensitive. Arguably, your childcare service provider does not have control over this footprint either. Nor do their staff completely understand the crossover with Cyber Security and Cyber Safety and the issues caused for a child's future and safety.

When a childcare service provider or school enters into an agreement with an App provider, the contract of service is between the service provider and the App provider. The parent or guardian is merely a user, not a party to the contract. In basic legal terms, if you are not a party to a contract, you cannot enforce it or seek a remedy for any breach or damage.

When a parent submits the completed enrolment forms, the service provider enters the personal details of parents/guardians in the administrators' side of the App. A child's data is also entered into the App, including sensitive medical information, insurance, any medical providers, and medical reports.

The provider then uses the App to upload daily routines, toileting data, sleep data, feeding data, photos, observations, stories, and incident reports, including behavioural notes and

other tailored reports. Likely a parent/guardian can comment on the entries made. Sometimes other children will be included in these entries. And yes, mistakes can be made with a simple click on the wrong child or parent, seeing your child's photo, sensitive information, being shared with other families. The enormous amount of information shared on every child every day is also a distraction for the Teacher or Childcare staff member taking away from their actual job of educating a child and keeping children safe while onsite at the service provider.

Many Apps allow 'family' to view a child's journal, which also includes other children if they are featured in a child's account (which is highly likely). There is no vetting of who can get these invitations; it's on the user to invite others. This could be an aunt, an uncle, the grandparents, or even the man who lives next door, 'just in case.' This means that someone else is seeing a child, someone a parent hasn't consented to. You do not get to approve additional users who are added or given access by other parents, only those you choose to provide access to yourself.

Additionally, there is rarely two-factor authentication in these Apps to protect login details and to track that people are who they say they are. Let's not forget it's common to practise to share login details with family than have them set up their profiles, so commentary, viewership, and communications can be from someone who is not the intended user.

Mandating the use of Apps is becoming standard for the convenience of childcare providers. Recently, we have been made aware of more and more After School Care services mandating the use of Apps. In some cases, even including that, the service provider can only be notified of absences in the app. Otherwise, an 'administration fee' will apply. This is also applicable to many primary and secondary schools.

What's the problem with using a childcare App if, seemingly, every other industry has one? Very little research has been conducted into the childcare App market. It doesn't even raise eyebrows as these Apps are seen as convenient and a timesaver for the provider and a key engagement driver for parents. And the Apps aren't silly; some are designed with the whole mummy/daddy guilt in mind, played on by the developers, so parents feel that they *can't* sign up without suffering from major FOMO and a massive case of the guilts.

A Privacy and Security Analysis of Mobile Child Care Apps is a study that was released in March 2022. The study looked at 42 Apps and found a direct threat to privacy by tracking mechanisms embedded in the applications. Another risk it noted was information leakage.

We forget that children cannot consent to their data being stored. That in itself raises privacy issues. As the authors of this study state, it is the job of the parents and educators to act with caution. **Always remember** that we are the product if something is free to use**.** If a child's daycare centre or school is using a free App to keep parents up to date with what a child is doing, that means that they could be paying with external access to all the data stored within it.

Serious questions need to be considered about the mandatory use of these Apps when considering anti-discrimination laws and the privacy rights of a child. There appears to be a giant black hole, and these two do not meet.

On a cursory glance, forcing an individual or family to use an App for convenience appears to be nothing short of indirect discrimination against those exercising their rights to keep their lives offline.

The Human Rights Commission defines indirect discrimination as:
"*where an unreasonable rule or policy that is the same for everyone but has an unfair effect on people who share a particular attribute."*

Yet, for many, they will not satisfy the protected attributes required under our discrimination laws, such as gender, disability, or race (amongst others). Some will, however, for example, the vision impaired who may not be able to utilise these apps or perhaps families who are not from an English-speaking background. Those of us who have, for want of a better expression, a 'conscientious objection' to putting our children's data online have no protection.

Interestingly, Article 16 of the Convention of the Rights of the Child states that:

" 1. *No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour or reputation, and*
2. The child has the right to the protection of the law against such interference or attacks"

These Apps that have been designed for convenience do not seem to consider either of these aspects, and there is a gaping hole. How we can protect our children from storage and usage of their data?

The concerns with this are many, including that most services do not consult or are not consulting with parents/guardians about using an App, moving to an App, or in the case of new families to a service, even providing them with an option to use the App or to inform them that one is being used.

Some families have no choice due to vacancy rates for centres in specific geographical locations. At best, you'll be presented with a Privacy Policy or referred to the Centre's Privacy Policy on their website that concerns the Centre itself and how it handles your and your child's personal information. In one instance that has been observed, the Centre's Privacy Policy is very vague, stating "… *realises the importance of privacy to families/guardians and as such does not release any information of records stored to a third party for their use without the account holders' authority unless required by law".*

Arguably, the transmission of personal information is not being 'used' by the third party. Still, this Privacy Policy makes no mention that the service utilises an App and that, as part

of the Terms of Use of the service, personal details will be disclosed. You also need to agree to the Apps' Terms and Conditions and their Privacy Policy.

One service provider states in their Terms and Conditions that whilst they take care to provide services and ensure that the App and website is free of any virus or malware, they are not responsible for damage caused, and that you indemnify the developer from all liabilities, costs and expenses. In relation to privacy, it states that whilst it aims to take due care, they do not warrant and cannot ensure the security of any information which is provided, and information is transmitted solely at your risk.

The first generation of social media users are now parents, and they are the target market for these Apps. This generation had little or no guidance about the risks of what they were using when they were in school in the early 2000s, and now they are becoming parents; many don't know the questions that they should be asking because it all just feels like 'the way it is'.

However, the problem with some of these apps, especially for those who are not tech savvy, is that you may not know what questions to ask regarding what vulnerabilities these Apps may have, what trackers are in place for analytics, or how they are used. We also don't know how our data is used to 'better the product,' how secure the cloud storage is, and what country it is located in (many Apps state that data is 'stored in an external data storage facility.'

And what happens to photographs and videos uploaded of our children? Who can download them, and who is taking screenshots? Who are the other parents, grandparents, siblings, aunties, or uncles who now have access to photos of your children through the App? For parents with no choice as to providers, their children's data, along with their own, is being held for ransom because the use of the App is mandated by using the service.

On top of all this, we have no idea what this data will look like for our children in the future. Already, some life insurers are using the reason a person has accessed mental health services, including youth mental health services, even without a formal diagnosis of a mental health condition, to decline or heavily restrict offering insurance coverage to an individual. This has been identified in various complaints to State Anti-Discrimination Tribunals and highlighted in a 2021 report by the Australian Public Interest Advisory Centre.

Whilst there is clear discrimination here, some insurers are finding their way around the Anti-Discrimination laws. Often, consumers do not know or understand their rights to challenge the decisions made. In addition to these reports, Safe on Social has been informed of cases where individuals are being declined insurance coverage for having had episodes of anxiety, including young adults.

What about the possible impact of this data being released or otherwise located by our children's potential employers down the track? How will the possible disclosure of this information impact their job-seeking? Already we know that employers are searching for prospective employees, with many scrutinising their social media presence, and the

perceived reality of a candidate is an influencing factor for some employers. Adding an extra layer of sensitive information could be devastatingly adverse for some individuals.

There is no suggestion that these Apps or the data collected is being misused at present, but any data collection is open to exploitation. Data such as sleep patterns, toileting, and what our children eat during the day is essential for some parents, but does it need to be collected and stored, especially when we don't know who the App developers may share the data with? or sell it to?

Photographs of our children are lovely, but do they need to be stored in a third-party Application that cannot guarantee our children's privacy? Who monitors or vets who are allowed to use the App, and what invitations can be sent to what family members or friends?

Other issues are more subtle but of equal importance. For starters, forcing a parent to utilise an App may disadvantage some members of our society (the vision impaired or other language speakers), potentially resulting in some form of indirect discrimination. It may even go further to discriminate against parents with family responsibilities who feel they have no choice but to remove their children from services because of a desire to protect their privacy. Those parents are forced to choose between work or placing their child in the care of a service provider who mandates storing their child's data and who has no control over disclosing that data.

We all sign Permission to Publish forms for our children, and there used to be a choice. If you opted out, you would be emailed the photo or given a printed copy. But lately, Safe on Social has been contacted more and more by parents that feel discriminated against. For example, a parent contacted us who was very upset that she had to pull her child from an early childhood after-school activity because she didn't agree to photos of her child being published online. She had escaped domestic violence and did not want photos of her child online. She was told that her child could not participate if they could not be photographed and published on the business's social media pages.

Newer parents are learning from older parents and are indeed becoming wiser. New parents are making conscious choices to keep their children's data offline; they're not posting photos and are thankfully starting to be more cyber-street smart. But are they thinking about the Apps they use to keep track of their children's activities during the day in childcare or just not sharing them on the major social media platforms?

We teach our children about being safe online, and generally, we are now becoming more cautious about when we allow them online and what we allow them to do. These Applications and mandating their use of them take that control away from parents who cannot make informed decisions about what or how their data and their children's is being used. Isn't it time we had a conversation about how best to manage the delicate balance between convenience and our children's privacy?

For more information on an ever-changing area please do not hesitate to contact me. Thank you for your attention to these matters.

Sincerely,

Kirrily (Kirra) Pendergast

Founder
Safe on Social Media Pty Ltd
The eSafety Training Company Pty Ltd

Kirra is a renowned cyber safety expert, with over 30 years of experience in the fields of cyber security, IT Business consulting, and Cyber Safety. She is also passionate about working with children and has dedicated the last 15 years of her career to educating and training people on cyber safety ranging in age from 5yrs - 75+. In 2021 she spoke to more than 106,000 young people in Schools across Australia.

As the Founder of Safe on Social, Kirra splits her time between the Asia Pacific Headquarters in Byron Bay, Australia, Safe on Social's UK, and European Headquarters in London, England, and Florence, Italy. Her experience of enduring online bullying and abuse inspired her to create Safe on Social, which has now become the largest and most trusted cyber safety education and training group of companies globally.

Kirra is a global thought leader in cyber safety, providing organisations of all sizes with cyber safety and social media risk management awareness training on an international scale. She is a dynamic and engaging public speaker and media commentator, having written for numerous media organizations and appeared on major international news channels. She is also a regular guest on podcasts across the world.

Kirra's straightforward, no-nonsense approach empowers people with knowledge, giving them the skills to consume technology positively rather than have their lives consumed by technology. Her extensive experience advising governments and organisations of all sizes for 18 years before founding Safe on Social has powered the training programs provided by the company.

In 2020, Kirra appointed a first-of-its-kind advisory committee of young people to help guide Safe on Social's work. She is known for her dedication to the cyber safety cause and expertise in every aspect of the sector, making her a highly sought-after speaker and commentator.

More information about Kirra and the Safe on Social team can be found on their website www.safeonsocial.com