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

16th February 2023

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

My name is Kirra Pendergast I am the Founder of Safe on Social Media Pty Ltd.
I am writing to draw your attention to two pressing issues related to child exploitation: the prevalence of child grooming and sexual abuse on online gaming platforms, specifically Roblox, and the privacy and security risks associated with the often mandatory use of mobile applications (Apps) in childcare centres and schools in Australia.

As you are aware, the internet is constantly creating new opportunities for predators to target children and engage in grooming and sexual abuse.

The specific issue is how such behaviour happens on Roblox. Predators on Roblox use a range of tactics, including offering children money (the in-game economy is called Robux) for sexual acts, engaging in role-play games that involve sexual activity and moving conversations to other platforms such as TikTok, which may open up a video message function where children may be groomed, sextorted and threatened.

In one of many disclosures, in May 2022 I spoke at a school and an 11yr old girl presented to me after the session. She graphically described whilst she was shaking a sexual assault of her in game character on Roblox. She kept saying “it happened to me” children no longer see the world as online and off. To them it is just life. The Principal and I decided that even though it was online, it was a mandatory report. The Principal notified the parents and the authorities. I am unaware of the outcome.

To combat this problem, law enforcement must have the necessary resources and expertise to identify and apprehend these predators. This may involve working closely with companies operating online gaming platforms like Roblox to identify and report suspected abuse. It may also require investment in advanced technologies and training to track and analyse online activity, particularly on social media and messaging apps where predators often move their activities.

Additionally, we would like to raise concerns about the privacy and security risks associated with the mandatory use of Apps in childcare centres and schools. While these Apps can be convenient for parents and educators to communicate and share information, they can also pose enormous risks to children's privacy and security. We must address that childcare centres, schools, after-school care, and after-school activity providers such as dance and gym classes cannot mandate these apps to parents or guilt them into using them.

When parents or guardians sign up for the service provider's App on behalf of their child (often being told that if they don't, they will miss out), they are also aiding in the creation and building of their child's digital footprint, which the child has no control over. Sensitive information, including medical records, is also entered into the App, which third parties can access if the App's security measures are not adequate.

Moreover, many apps allow users to invite "family" to view the child's journal, which includes other children if they are featured in the child's account. More often than not, someone else is seeing the child, someone the parent or guardian has not consented to, and the child they have permission to view. This may be a significant security issue when someone who may be a predator is invited into these photographs of children going about their day at day care, primary school, after-school care, and after-school activities such as dance classes.

As we all know, predators are not looking for photos of naked children; they are just looking for children.

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 got us 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 pictures 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. This must stop.

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 are being used.

Questions that need to be asked;

1. Is the App paid for by the service provider, or are they using a free version? (Remember, your data becomes the product if something is free to use. If it is paid for by the parent, the use of the data may have further protection by the Australian Information Commissioners Office.)

2. Who has access to the App and its data? Where is it stored, and can it be deleted if you or your child want it all deleted in the future?

3. How are the people accessing your and your child's data vetted?

4. Are the photos able to be saved/screenshots?

5. Is there a Social Media Policy in place that advises parents not to share photos from within the App on their personal Facebook pages if other children are in the image?

6. Does the service provider have a way to email photos to the parents if they choose not to allow their child to be published on the service provider's Facebook/Instagram, and why?

7. If an opt-out is allowed, do they take photos and blur the child's face out of things they publish online or exclude them completely? (This way, a child can still feel included, and their parents can be emailed the photo, but if blurred out, they cannot be identified online.)

8. What happens to the photos and the data when a child leaves the service provider?

9. Can a parent ask for all data to be destroyed, and if so, how does that happen and when?

10. Is the use of the App mandatory? Is there another way you and your service provider can communicate and share information without using a third-party App?

Serious questions need to be asked about the legality of the compulsory use of these Apps.

We also recommend that the government invest in ensuring that these Apps are secure and that parents and educators are adequately trained in their use.

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