CHILDREN & MEDIA AUSTRALIA

Thriving in a digital world

SUMMARY of pilot *Apps can track* project 2021-2022

***Background*:** Children and Media Australia (formerly known as the Australian Council on Children and the Media) has been providing child-development-based reviews of current and selected older movies since 2002. In 2014, CMA was commissioned by the SA Govt (who had been funding these movie reviews for several years) to provide a service similar to the movie reviews, but for apps, and to include an assessment of whether apps included simulated gambling behaviour.

CMA has been providing these reviews as a free service to parents who want more detailed information about the age-appropriateness and content of movies and apps for their children under the age of 15 years. CMA is motivated to do this because the National Classification Scheme (NCS) lacks recommendations about age-appropriateness for children under 15. CMA has also endeavoured to include in its app reviews, other information not covered in the NCS, about new traps in apps for the unwary (incl. loot boxes, in-app purchasing).

There are now over 1500 movie reviews and 990 app reviews on CMA's website.

CMA's awareness of the extent and covert nature of much of the tracking activity in apps, was heightened in 2018, when Hon CEO Barbara Biggins attended a conference in New York at which Dr Serge Egelman presented his research and findings on his system of determining the tracking activity of children's Android apps.

> *We identified several concerning violations and trends: clear violations when apps share location or contact information without consent (4.8%), sharing of personal information without applying reasonable security measures (40.0%), potential non-compliance by sharing persistent identifiers with third parties for prohibited purposes (18.8%), and ignorance or disregard for contractual obligations aimed at protecting children's privacy (39.0%). Overall, roughly 57% of the 5,855 child-directed apps that we analyzed are potentially violating COPPA.*

CMA was motivated to act by the risks to children from such tracking, which include the formation of an extensive digital footprint that can be used by predators and marketers, and may jeopardise prospects later in life such as jobs, university places, health insurance and more. CMA wanted to support parents who may not be aware of the risks in apps their children play, nor be able to detect or prevent them. Furthermore, Australia has no regulation in place to protect children's rights to online privacy. Big Tech's business model is to gather users' data to sell them things, and will not be easily budged from this stance.

CMA invited Dr Egelman to speak at a conference in Australia in 2019, and introduced him to government agencies working in the field of digital privacy.

Children and Media Australia
PO Box 1240, Glenelg South SA 5045
61 8 83762111 61 8 83762122
info@childrenandmedia.org.au
www.childrenandmedia.org.au

The Project:

In 2020, CMA gained a grant from the Australian Communications Consumer Action Network (ACCAN) for an 18 month project to incorporate tracking analyses (produced by Dr Egelman's research company, AppCensus) into CMA reviews; to explain how to interpret the analyses; and to develop a package of privacy resources for parents.

The new service was launched in June 2021. CMA has added a total of 208 app reviews, with AppCensus checks, to its website.

NOTES:

The analyses produced by Appcensus are by their nature very technical. CMA has worked hard to produce a more parent-friendly format for these. If further funding can be gained, CMA aims to produce a version of the checks that highlights the level of risk found in each app.

Users need to know that [more at our guide to the system]:

- The most risky apps are those with insecure data transfer, and those where either both Android Advertising identifier (AAID) and Android ID (AID) are transferred, or IMEI (International Mobile Equipment Identifier) and AID, are utilised.
  AAID can be reset by modifying phone settings. Both AID and IMEI are globally unique identifiers that could be used to track users over time and across apps. AID requires a factory reset, but IMEI cannot be reset. Such apps are risky as these identifiers can be used to circumvent privacy controls.
- Many developers will say they do not use the collected data, but the question is, why collect it?

Our Findings:

Of the 208 apps we checked over the 9 months, 22 were school-home or parent-child communication apps (analysed to see how safe these were).

At the time of checking, the following results were found for the 186 popular game apps (Note companies may have changed the app since then).

Risky entertainment apps

Very risky (any app that transfers data in an insecure manner)

7 apps (3.8%) transferred personal IDs to one or more ad-linked companies in an insecure manner. eg *Starwars Pinball 7* *v7.0* - it also collects email addresses automatically and insecurely.

Risky (any app that transfers both AID and AAID, or IMEI and AID, to ad-linked companies)

54 apps (29%) transferred both AID and AAID to between 1 and 6 ad-linked companies. eg *Dr Panda's swimming pool* *v1.01*– collects IMEI and AID.

Need caution (any app that transfers AAID to ad-linked companies)

A further 40 apps (26%) transferred the identifier AAID to at least one ad-linked company eg *Icecream cone cupcake baking maker* *v1.0.9*– collects AAID and sends to 5 ad-linked companies.

All up, a total of 59% of apps reviewed had some level of problematic data collection behaviour at the time of checking.

Parents can search in CMA's database of over 200 app reviews (that include these tracking checks), for titles that their children want to play. CMA will continue to add to this database if funding is found.

What CMA hopes to achieve from this pilot:

To raise parents, general community and policy-makers' awareness of

- the importance of privacy issues, and lack of protections for children.
- the hidden nature of the tracking and the difficulty in stopping it happening, despite following the usual advice.
- The urgent need for effective regulatory protections.
- The need for more responsibility by industry: to use child-centred safety by design, and to stop their targeted manipulation of children.
- To be able to get funding to continue these reviews (and further highlight the levels of risk) until all the above is in place.

To share Dr Egelman's aims:

> *End-users can examine our results to understand the privacy behaviors of the apps they use (or plan to use).*
> *Developers can use our testing infrastructure to assess how well their apps comply with their privacy policies and regulatory requirements, prior to releasing those apps to the public.*
> *Finally, regulators can use it to detect deceptive and suspicious activities in the marketplace as part of investigations.*