Young Children's Safety in an Online Environment

Policy Brief

This briefing is in response to the proposed Office of the Australian Information Commissioner (OAIC) Children's Online Privacy Code (The Code). The briefing leverages the expertise of Curtin University's Early Childhood Education Research Group and Curtin University's Education Researchers from the Australian Research Council's (ARC) Centre of Excellence for the Digital Child, to inform the OAIC and the wider community about the current challenges, recommendations, and opportunities concerning young children's online privacy.

Context and Rationale

The United Nations Conventions on the Rights of the Child General Comment No. 25 (2021) foregrounds the importance of digital technologies for all children, including the very young. Digital technologies are increasingly central in fostering children's active participation, including in social, education and access to government services. The scope of digital technologies is evolving at a rapid pace such as expansion of AI, with this requiring frequent expansion of digital literacy. Constant attention is required to ensure the child's digital citizenship, dignity and safety is maintained when engaging with digital technologies.

A child is surrounded by many 'systems' or spheres of influence (Bronfenbrenner,1979) which impact on their growth and development. Parents, caregivers, educators, siblings, and AI in the child's spheres of influence become 'enablers' of the child's access to digital technologies, often providing consent on behalf of the child. However, the provision of informed consent is questioned. Several enablers have a lack of digital literacy themselves. Further, the child is frequently not afforded opportunity to provide assent as part of informed consent processes. Many children already have a substantial digital footprint that they are unaware of and/or has been created without true informed consent.

In response to the proposed OAIC Children's Online Privacy Code (The Code), the following challenges, recommendations, and opportunities are presented.

Key Challenges

1. **Parents/ caregivers and educators providing informed consent –** For young children's online data and privacy.
2. **Young children providing informed assent –** To their online presence.
3. **Identifying all enablers for a young child's access –** To online environments, including the role of AI as an enabler.
4. **An identified lack of digital literacy in parents/ caregivers and educators –** Particularly concerning online data, privacy, and storage.
5. **Potential commercialisation of children's data –** By technology companies.

Recommendations

1. **Enhanced readability and accessibility –** Of privacy statements, data agreements, and The Code for parents/ caregivers and educators.
2. **Enforced translation of key documents –** Such as privacy statements, data agreements, and The Code, specifically for young children through age-appropriate language and multimodal translations of information (e.g. cartoons, videos, storybooks).
3. **Use of AI technology and facial recognition software –** To prevent young children's access to online environments, as required by The Code.
4. **Prohibiting commercialisation of children's data –** Through the introduction of new targeted regulatory requirements.

Opportunities

1. **Development of a research derived checklist –** In partnership with Universities and children, of the major considerations required that parents, caregivers, and educators, must indicate agreement to before they provide informed consent.
2. **University facilitated outreach programs –** With parents, caregivers, and educators, to provide research informed opportunities for their development of digital literacy in a meaningful and connected way.
3. **Build AI literacy into initial teacher education courses –** Specifically focusing on early childhood education and including the ethical and critical thinking skills required to be informed and keep our children safe online.