Children's online privacy v online safety: Australia stepping up its regulation

The Privacy Reform Implementation and Social Media Taskforce (**PRISM**) of the Office of the Australian Information Commissioner (**OAIC**) is hard at work developing the Children's Online Privacy Code (**Code**). Consultations with parents and children are underway and other stakeholders will have their say later this year. Expected at the end of 2025, the draft Code will likely take inspiration from similar regimes in the UK, Ireland and California.

Once issued and registered, likely in 2026, the Code will have the force of law. It will add another layer of protection for children online alongside existing criminal and online safety laws. Each of the three regimes grapples with different aspects of online risk which may result in cyberbullying, grooming, child abuse, sextortion, harassment, emotional harm, self-harm, suicide, exposure to age-inappropriate or violent content, misinformation, disinformation, indoctrination, fraud, screen addiction and other harms.

The Code will strike where harmful data practices such as profiling, recommender systems, and commercialisation of children's data fail to put the best interest of the child first. The Code might provide fresh interpretation and reaffirm certain rooted privacy concepts where the historic interpretation of the Australian Privacy Principles (**APP**) fails to do so. Acting in the best interest of the child will often mean doing right by the individual over the business.

Criminal law not coming to the rescue …

The reach of criminal law is limited if a cyber criminal's harmful conduct falls short of constituting a criminal offence or if he/she evades detection in the real world.

The range of criminal offences concerning child abuse and the handling of child abuse materials[1] are expanded by the recent criminal law reform criminalising sextortion (blackmail with intimate images), explicit deepfakes, non-consensual intimate image sharing,[2] and doxxing (publishing one's details for online harassment).[3]

Setting the benchmark by defining new digital criminal offences concerning children is important. However, in practice, law enforcement will struggle with limited resources, digital skills, perpetrators outside jurisdiction, platform resistance to give access to evidence and a high burden of proof. The resulting focus on the most serious cases leaves much harmful conduct unchecked.

Nevertheless, criminal liability could arise if organisations fail to implement a culture of compliance,[4] and are suspected of:

- administering or encouraging the use of a digital platform to deal with child abuse material[5] or abhorrent violent material;[6]
- disseminating or possessing child abuse material;[7]
- providing information about avoiding detection;[8]
- failing to report child abuse;[9] or
- distributing child abuse material outside Australia.[10]

[1] For example, section 66EB grooming; section 66EA Persistent sexual abuse of a child or section *66DF Sexual act for production of child abuse material under of Crimes Act 1900* (NSW) or section 51C *Producing child abuse material under Crimes Act 1958* (Vic).
[2] The Criminal Code Amendment (Deepfake Sexual Material) Bill 2024.
[3] Proposed new section 474.17C and 474.17D under the Privacy and Other Legislation Amendment Bill 2024.
[4] Part 2.5,*Criminal Code Act 1995* (Cth).
[5] 91HAA and 91HAB *Crimes Act 1900* (NSW).
[6] Subdivision H — Offences relating to use of carriage service for sharing of abhorrent violent material; *Criminal Code Act 1995* (Cth).
[7] 91H *Crimes Act 1900* (NSW).
[8] 91HAC *Crimes Act 1900* (NSW).
[9] Section 316A *Concealing child abuse offence of Crimes Act 1900* (NSW).
[10] Section 273.6 Criminal Code Act 1995 (Cth).

Understanding potential criminal liability and available defences[11,12,13] is critical in formulating corporate risk mitigation strategies for digital services.

eSafety laws starting to bite

Australia's *Online Safety Act 2021*(Cth) (**OSA**) came earlier than its counterparts around the world.[14] eSafety laws place accountability on digital platforms which have greater visibility of user activity and therefore should be best placed to understand user risks and implement safety measures.

The OSA regulates seriously threatening, menacing, intimidating, harassing, humiliating, abhorrent[15] and otherwise offensive content. It is not directly concerned with copyright infringement, defamation, racism, discrimination, cybercrime or privacy, but there are overlaps. For example, intimate image sharing will likely be a privacy as well as eSafety matter. The Commissioner's role is limited to online content, and does not extend to police matters,[16] such as child sexual exploitation, fraud or bodily harm. However, the Commissioner may disclose information, for example, to law enforcement or a teacher at school in the context of a cyber-bullying complaint.

The OSA applies to online services including social media, communication services, app stores, search engines and other designated services. Under OSA online service providers must:

- implement a clear complaints procedure for end-users;
- implement the basic safety expectations,[17] including proactively ensure safety of service,[18] identify and mitigate risks of AI and recommender systems, consult the Commissioner, uphold the best interest of the child, and handle complaints promptly; and
- provide reports about compliance upon Commissioner's notice.

The eSafety Commissioner can issue removal notices, alert to the presence of abhorrent violent materials, and initiate a criminal prosecution.[19] Indeed, any awareness of unlawful content will defeat the 'hosting exemption' under section 235 of OSA. The Commissioner can ask an end-user to cease offensive activity and apologise to the victim.[20]

The eSafety Commissioner's powers are limited to content available in Australia. In *eSafety Commissioner v X Corp*,[21] the court held that X had effectively complied with a removal notice by geo-blocking the content and not removing it globally.

The data privacy angle

The Code must be completed by December 2026. It will likely attempt to capture all information about children, whether known, observed or inferred. The Code will strengthen the interpretation of the APPs but not create entirely new prohibitions or principles.

It will apply to businesses or organisations covered by the *Privacy Act 1988* (Cth), excluding small business operators, if they are a provider of a social media service, a relevant electronic service or designated internet service, and the service is likely to be accessed by children. For example, the Code

---

[11] Updating content filtering technology in accordance with the law (Section 273.9 *Criminal Code Act 1995* (Cth).
[12] Disseminating child abuse materials in the context of machine learning under a research exemption (9HA(8) *Crimes Act 1900* (NSW).
[13] Assisting the eSafety Commissioner (Section 273.9(5) *Criminal Code Act 1995* (Cth).
[14] Singapore's Online Safety (Miscellaneous Amendments) Act 2022; Irish Online Safety and Media Regulation Act 2022; UK's Online Harms Act 2023 or EU's Digital Services Act passed in October 2022.
[15] Depicting murder, torture, rape, kidnaping or a terrorist act (Criminal Code, 474.32).
[16] Albeit the Commissioner plays a role in relation to notices of abhorrent violent content under the Criminal Code Act 1995 (Cth).
[17] Online Safety (Basic Online Safety Expectations) Determination 2022 amended on 31 May 2024 (link).
[18] Reasonable steps to provide a safe service, prevent children's access to X-rated materials and minimise its presence, proactively minimise unlawful or harmful material or activity, and make available appropriate user controls for safe online interactions;
[19] Subdivision H — Offences relating to use of carriage service for sharing of abhorrent violent material; *Criminal Code Act* 1995 introduced by the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act* (Cth) 2019.
[20] *eSafety Commissioner v Rotondo* [2023] FCA 1296 QUD 451.
[21] [2024] FCA 499.

may specify that it applies to smart toys or edtech used in and out of schools. It will not apply to health service providers.

The Code will not directly regulate online content but rather focus on minimising risks of the collection, use and disclosure of personal information. The Code may impose express APP-consistent requirements in relation to, among other topics:

- the best interest of children to prevail over inconsistent commercial interest;
- appropriate policies, systems and controls to be implemented;
- understanding user age-groups, the changing cognitive needs of children and the underlying privacy risks;
- data privacy impact assessments to dictate the necessary mitigation strategies;
- privacy by design with children in mind to be adopted in developing user interfaces and backend processes;
- transparency notices to provide clear and age-appropriate information;
- meaningful choices to be offered and nudge techniques and dark patterns avoided;
- parental consent to be required where young children cannot fairly be expected to make informed choices;
- data minimisation to limit data handling to what is strictly necessary to provide child-friendly services; and
- data use for direct marketing and profiling to be appropriately limited and not to exploit children's curiosity and gullibility.

Conclusion

Australia's online harms regime is becoming more complex with various regulators such as the Australian Communications and Media Authority (**ACMA**), the OAIC, the eSafety Commissioner and the Australian Competition & Consumer Commission (**ACCC**), overseeing this area of compliance.

Developing digital services for children comes with an increased compliance risk. Adherence to developing requirements will not be possible without a governance framework underpinned by assigned responsibilities, risk assessments, staff training, policies and procedures and record keeping.

In terms of privacy risk, a simplified approach to legal compliance could consist of the following steps:

Step 1 – Are children likely to access your service? It will likely not suffice to just say that your service is not intended for children if it is in fact used by children or relying on user-declared age.

Step 2 – What are the specific risks to children in the context of your service? It will be important to understand all service use cases (and misuse scenarios) to advise on the likely risks for each age group.

Step 3 – How can risks be mitigated in a compliant way while achieving business objectives? Various third party child safety tools could help achieve compliance without unduly restricting user activity. Blanket bans or broad restrictions will likely not be in the best interest of children, which have the right "*to rest and leisure, to engage in play and recreational activities appropriate to the age of the child and to participate freely in cultural life and the arts*" under the Convention on the Rights of the Child (1989).

Necessary measures may include age assurance, age verification, content moderation, preventing anonymous accounts, user reporting and complaints, privacy-protective default user settings, restricted service features, seeking explicit consent and parental consent, enforcement of terms and community guidelines and others.

KHQ can share experiences with online safety regimes in other jurisdictions and contribute to governance, assessment and mitigation efforts and generally navigating the complex online harms regulatory landscape.

Alexander Dittel is Principal at KHQ Lawyers