How Encryption Helps Build a Safer Internet for Young People Globally Webinar

Wednesday, February 12, 2025 - 2 - 3:30am AEDT

Remarks by Peter Leonard, Principal and Director, Data Synergies, Australia

Firstly, an apology that I am not joining you live for today's session, which is being held at about 3am Sydney time. Given my customary incoherence at 3am, it is probably better that I record my remarks!

Second, I should observe that today's topic addresses two of the more contentious areas in regulation of digital services in Australia, being:

- protection of under-18s from harmful content and mental health and other personal safety issues associated with certain online interactions, and
- how to get the balance right between (1) privacy and information security, and (2) safety, in relation to end-to-end encrypted online interactions.

Australian parliamentarians and regulators have recognised that there is a legitimate place for end-to-end encryption.

The so-called TOLA amendments of 2018 substantially broadened the legal right of law enforcement and intelligence agencies to compel providers of apps and online services and communications intermediaries to provide assistance in accessing encrypted communications. However, the TOLA provisions did not require these providers and intermediaries to introduce or maintain any systemic weakness or systemic vulnerability in end-to-end encryption.

A 2021 parliamentary review of the TOLA provisions recommended significant changes, but endorsed the exception allowing effective end-to-end encryption. Submitters to that review noted that encrypted communications:

- are critical to security of banking and identity data and thereby guard against certain online harms such as identity theft, and
- also protect the privacy of a range of vulnerable people, including victims of domestic violence, whistle-blowers and other journalists' sources, political dissidents, and children that may be exposed to sexploitation or other abuse.

Other submitters to the TOLA review, including law enforcement agencies and the eSafety Commissioner, observed that encryption may also facilitate children being exposed to sexploitation or other abuse as a result of the substantial impediment that end-to-end encryption creates to detection of criminal activity.

Particularly over the last two years, there has been a shift in perceptions of many Australians as to how that balance should be maintained between (1) privacy and information security, and (2) safety, in relation to end-to-end encrypted online interactions.

That shift in perceptions is at least partly due to community concern as to end-to-end encryption facilitating criminal activities including sexploitation, grooming of children, child abuse, hate crimes and terrorism.

This has in turn led to a new focus upon alternative technological, operational and cultural means to detect and deter such activities, including improved digital ID and alternative attribute verification or assurance measures to improve detection of would-be bad actors.

Improved capabilities of AI and other advanced analytics techniques to assist detection of would-be bad actors has in turn led regulators to propose that service providers and other digital intermediaries that facilitate provision and use of end-to-end encrypted services should be legally obliged to take proactive measures to implement these alternative capabilities.

The current Australian government, and many other Australian parliamentarians, have picked up upon these regular proposals, now proposing that the Online Safety Act 2021 should be amended to include **a general, overarching duty of care of online service providers in relation to services that they provide**.

What would this brave new world for regulation to facilitate online safety look like, and would children and other vulnerable people be able to continue to use end-to-end encrypted services?

It is important to note at this point the broad consensus in the Australian parliament as to the social media minimum age amendments as passed in late 2024 and coming into operation in late 2025.

Under this new law, age-restricted social media platforms - likely including Tik Tok, Facebook, Snapchat, Reddit, Instagram and X - will be obliged to implement appropriate systems to prevent children under 16 from creating accounts on their platforms.

Note that this statutory prohibition cannot be overridden by consent or approval of a parent or guardian: a child under 16 will not be permitted to establish or maintain a relevant account, regardless of what any parent or other adult may purport to permit.

An evaluative trial of age verification or age assurance measures is now underway. This trial will likely lead to approval of a range of alternative measures as appropriate to particular online services and provider capabilities. Although the trial is focussed upon determining whether a person creating or operating an account is likely to be a child under 16, the relevant technical or operational measures may include use of digital ID or other verification or assurance in relation to other accounts: this may assist detection of adult would-be bad actors seeking to engage with vulnerable people, including children.

The Online Safety Act 2021 was subject to an independent statutory review during 2024. The 200-plus pages report of the independent reviewer was released by the Minister for Communications on 4 February, just last week.

That report includes, as *Chapter 8 – Wicked Problems*, discussion of the complex issue of targeted technology facilitated abuse and the increasing use of end-to-end encryption and its encryption impeding prevention and detection of child sexual exploitation and abuse material and other illegal material, and sextortion. The report notes that in the Australian Federal Police's submission to the review, the AFP stated that in 2022-2023, about 96% of content the AFP lawfully intercepted was unintelligible due to encryption. The AFP suggested that encryption also prevents communications service providers from identifying illegal content on their own platforms and reporting it to law enforcement agencies.

The Report then went on to note that legally enforceable codes approved by the eSafety Commissioner work around end-to-end encryption and take an outcomes-based approach, requiring relevant service providers to:

> "implement appropriate systems, processes and technologies to detect and remove known child sexual abuse and pro-terror material where it is technically feasible and reasonably practicable to do",

while also stating the qualification:

> "Providers will not be required to implement systems or technology to detect and remove material where doing so would require the provider to implement or build a systemic weakness, or a systemic vulnerability, into the service or where it would require an end-to-end encrypted service to implement or build a new decryption capability or render methods of encryption used in the service less effective."

The Report proposed the new overarching duty of care of online service providers. That proposal has now been endorsed by the Minister for Communications, and which is expected to be the subject of a bill to be introduced into the Australian Parliament early in 2025.

If the bill reflects the recommendation in the Report, that duty:

- will be expressed in general terms that will oblige providers to take reasonable steps to develop and implement processes to detect and address material or activity on the service that is unlawful or harmful, but
- will not be stated in terms which expressly prevent provision of end-to-end encrypted services or require introduction of systemic weakness or systemic vulnerability into encrypted communications to the benefit of law enforcement agencies.

That noted, we may expect lively debate as to what is, or is not, a systemic weakness or vulnerability.

Finally, I would observe that Australia is likely to continue to take a distinctive approach to regulation of online safety, while also drawing significantly on, in particular, parallel initiatives in the United Kingdom. The UK Online Safety Act gives Ofcom the power to require that a company use 'accredited technology', or "make best efforts to develop technology", to tackle child sexual exploitation and abuse on any part of its service including public and private channels. However, it is yet to be determined what this technology will be. It may be that Australia, and the UK, adopt analogous approaches in determining reasonable technological means for providers to implement to work around 'the wicked problems' presented by end-to-end encryption. But Australia may act alone, and adopt a distinctive 'Australian way' solution: it is unlikely that Australian legislature will wait for other jurisdictions to take similar action.