Addressing cybercrime and emerging digital offences in the digital age

Tania Wolff
POLA Summit, Jakarta
8 September 2026

Law Council
OF AUSTRALIA

Law Council
OF AUSTRALIA

Overview

- The scale and evolving nature of cybercrime in Australia
- Australia's legal and regulatory response
- Lessons learned

Law Council
OF AUSTRALIA

Part 1

Scale and evolving nature of cybercrime and digital offences in Australia

Law Council
OF AUSTRALIA

Cybercrime and digital offences in Australia

- **Cyber-dependent offences** – unauthorised access to systems, interference with data.
- **Cyber-enabled offences** – fraud, stalking, harassment, blackmail, image-based abuse; online recruitment to commit offences.
- **What has changed:** scale, speed and reach – across borders, at volume, anonymously.
- **Harm** is economic, psychological, reputational and physical – and enduring.

Law Council
OF AUSTRALIA

Cybercrime and digital offences in Australia

- In the Magistrates Court of Victoria between 2018-23, 70% of sentenced cases involving the use of a carriage service to menace, harass or offend were committed in a family violence context.
- One in 25 Australian teens have been affected by AI-assisted online sexual abuse.
- Australians lost more than AUD 38million in scams in June 2026 alone.

Law Council
OF AUSTRALIA

Part 2

Legal and regulatory responses in Australia

Law Council
OF AUSTRALIA

Legal and regulatory response – **five pillars**

Legislative framework	**Regulatory framework**	**Institutional oversight and support**	**Public education and capacity-building**	**Independent review**

Law Council
OF AUSTRALIA

Criminal offences

- **Commonwealth, State and Territory offences** cover both cyber-dependent and cyber-enabled crime.
- **Technology-neutral drafting** – focus on the perpetrator's conduct, not the platform or service.
- **New offences for new harms** – e.g. doxxing.
- **Expanded investigative powers** – Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Cth).
    - Law Council position: appropriate thresholds, robust safeguards, regular evaluation of necessity and proportionality.
- **The criminal law alone is not enough** – criminal, civil and regulatory responses designed together.

Law Council
OF AUSTRALIA

Strengthening privacy protections

- Misuse or exposure of personal information enables cybercrime – **stronger privacy protection is prevention.**
- **Privacy Act reforms** (first tranche, 2024):
  - stronger obligations on organisations to protect personal information;
  - broader range of penalties – enforcement beyond the most serious breaches;
  - new avenues for redress.
- **New statutory tort for serious invasion of privacy** – in force for just over a year.
- Further reform under way.

Law Council
OF AUSTRALIA

Online Safety Act 2021 (Cth)

- Places obligations on digital service providers – **Online Content Scheme** and **Basic Online Safety Expectations**.
- **eSafety Commissioner:** investigates complaints, directs removal of material, develops and enforces industry codes and standards.
- **In action:**
  - notices to four online gaming services on how they are protecting children;
  - AI ‘nudifying’ service directed to introduce age assurance within 14 days – three such services have since withdrawn from Australia.
- **Next step: proposed Digital Duty of Care** – reasonable steps to prevent foreseeable harm arising from the design and operation of services.

Law Council
OF AUSTRALIA

Scams Prevention Framework

- **Preventative, economy-wide framework** – prevent, detect, disrupt, report and respond to scams.
- **Obligations on banks, telecommunications providers and digital platforms** – from 31 March 2027.
- **ACCC enforcement** and consequences for non-compliance.
- **Private right of action** for victims where a provider fails to meet its obligations.

Law Council
OF AUSTRALIA

Public education

- **Awareness campaigns and practical guidance** – recognise scams, understand the risks, know where to get help.
- **Tailored resources for vulnerable groups** – young people, seniors, First Nations peoples, parents and teachers.
- **Example:** eSafety campaign warning young men about sexual extortion scams and where to find help.
- **Small business** – understanding obligations and putting basic cybersecurity in place.

Law Council
OF AUSTRALIA

Independent review mechanisms

- Technology and harms change fast – **frameworks must be reviewed to remain fit for purpose and proportionate.**
- Especially where laws confer **intrusive or coercive powers**, or impose **significant burdens on business**.
- Reviews should be **independent, consultative and public**.
- **Embedded in legislation** – Independent National Security Legislation Monitor review of SLAID Act powers after three years; statutory review of the Online Safety Act 2021 (Cth).

Law Council
OF AUSTRALIA

Part 3

Lessons learned

Law Council
OF AUSTRALIA

Lessons learned – **five pillars**

Legislative framework	Clear, adaptable and proportionate laws that uphold rule of law principles.
Regulatory framework	Transparent, proportionate and effective regulatory frameworks that contain appropriate safeguards.
Institutional oversight and support	Effective and accountable regulators with appropriate powers and adequate resourcing to fulfil their functions.
Public education and capacity-building	Public awareness and education to prevent and reduce harm, giving particular consideration to vulnerable groups.
Independent review	Regular, independent review of frameworks to ensure they remain fit-for-purpose, effective and accountable.