Penalising digital harms perpetrators rather than platforms may help educate users

Digital harms penalties are under-utilised in Australia

Our research found that current penalty frameworks for digital hostility—such as online abuse, harassment, and threats—are inconsistent, fragmented, and often ineffective in deterring harmful behaviour. Laws vary widely across jurisdictions, with penalties not reflecting the severity or long-term impacts of digital harms. Victims face barriers in reporting and pursuing legal remedies, while offenders often exploit gaps between offline and online legislation. Addressing these shortcomings requires clearer legal definitions, harmonised penalties, and reforms that centre victim wellbeing alongside deterrence and accountability.

What did we do?

- We surveyed 2,500+ everyday Australian users; depending on age group, between 62% and 78% of Australians were in favour of penalising repeat and serious perpetrators of online abuse, harassment and deliberate disinformation.
- We analysed Australian and international legislation, platform terms of service and public inquiries into platform regulation, finding that the current model empowers platforms to do the 'policing' work on behalf of governments, even though they have a conflict of interest. Existing laws that cover abuse and harassment are not referenced in Australia's Online Safety framework.

Why is penalising perpetrators a good idea?

Public education and deterrence of harmful behaviour – Clear and enforceable penalties reduce the likelihood that individuals will engage in online abuse, harassment, or threats; just like penalties for smoking or drink-driving penalties serve as a pedagogical tool.

Accountability for perpetrators – Legal consequences ensure offenders are held responsible for the harm they cause; more importantly they have access to due process which is not currently enjoyed when platforms manage harms themselves.

Support for victim wellbeing – Sanctions validate victims' experiences, provide a sense of justice, and can be paired with protective measures to reduce re-traumatisation.

Strengthening public trust in law and platforms – Effective enforcement signals that authorities and digital platforms take online abuse seriously, encouraging reporting and more ethical civic participation.

Are there challenges in re-incorporating penalties into Online Safety in Australia?

Based on our research, the challenges of enhancing penalties for perpetrators of digital harms include:

- **Interjurisdictional inconsistencies:** Differences in laws across states and countries make it difficult to apply consistent penalties for cross-border online abuse and to charge overseas perpetrators without international agreements in place.
- **Gaps in legal definitions:** Ambiguous or outdated definitions of digital harms hinder the ability to prosecute cases effectively under existing legislation.
- **Evidence and enforcement difficulties:** Collecting admissible digital evidence and identifying perpetrators can be complex, especially when anonymity or encrypted platforms are involved; it may also overwhelm under-resourced Australian courts.

Where can I find out more?

Cover, R., Simcock, R. & Humphries, J. (2025). Digital harms and penalties: Australian regulation, platform moderation and the figure of the perpetrator. *Media International Australia.* **https://doi.org/10.1177/1329878X251350727**

Contact: Professor Rob Cover
Email: rob.cover@rmit.edu.au

This summary brief was supported by the Australian Research Council Discovery Project, "Online Hostility in Australia Digital Cultures" (DP230100870)

The RMIT Digital Ethnography Research Centre (DERC) undertakes comprehensive research on the everyday lived experience of digital cultures, mobile media, platforms, workplaces and settings. Working with a wide array of partners and collaborators in Australia and internationally, we undertake people-centric data collection, design and analysis to help governments, industry and the community make sense of changing factors in our digital lives, including digital harms, AI, disinformation, emergent mobile technologies and online economies.

RMIT UNIVERSITY

Digital Ethnography Research Centre

August 2025