



October 27, 2026

Re: Inquiry into the nature and drivers of radicalisation in Australia

Executive Summary

The Computer and Communications Industry Association (CCIA) is pleased to provide evidence in response to the Parliamentary Joint Committee on Intelligence and Security (PJCIS)'s age assurance guidance (Guidance).¹ CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.² Many of CCIA's members operate innovative, global digital services where consumers have high expectations for privacy and security. Proposed encryption legislation can therefore significantly impact CCIA's members and users.

CCIA believes that, rather than furthering radicalism, encryption plays a key role in combating it. Encryption safeguards citizens' communications against attacks by malicious actors, limiting radicalised groups' ability to harm civilians. These threats can arise from foreign governments as well as civilian groups. Furthermore, encryption is critical for compliance with the CLOUD Act³ and similar agreements, which enable Australian law enforcement to obtain expedited access to data stored abroad. Such access is crucial to combating the influence of radicalism in Australia.

1. Encryption safeguards Australians' communications against radicalised actors

Weakening encryption inevitably creates opportunities for threat actors and radicalised groups to exploit. As CCIA has noted previously, "There is no such thing as an encryption backdoor that can only be used for good actors."⁴ Creating such vulnerabilities "will give bad actors and meddlesome regimes an opening to infiltrate private communications, business data and consumer information."⁵ Moreover, these weaknesses leave citizens more vulnerable to spyware and surveillance tools, which both extremist foreign regimes and radicalised civilian groups may deploy.⁶

¹ *Inquiry into the nature and drivers of radicalisation in Australia*, Parliament of Australia (2026), https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Radicalisation.

² For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than \$100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at <https://www.ccianet.org/members>.

³ *Cloud Act Agreement Between the Governments of the U.S. and Australia*, U.S. Dep't of Justice (last updated Aug. 11, 2023) (hereinafter *Cloud Act Agreement*), <https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-and-australia>.

⁴ CCIA et al., *Threats to Global Encryption in the UK 2* (Mar. 12, 2025), <https://ccianet.org/wp-content/uploads/2025/03/Industry-Coalition-Letter-on-UK-Encryption.pdf>.

⁵ *Id.*

⁶ *Id.*

For these reasons, there is broad consensus among security professionals that the risks to cybersecurity, national security, economic security, public safety, and fundamental rights that arise from undermining encryption outweigh the benefits of granting law enforcement easier access to information.⁷ Undermining encryption compromises potentially sensitive data and creates additional complexity in network security system infrastructure, making data security less feasible. In 2013, former United States National Security Agency director of research Fred Chang testified that “[w]hen it comes to security, complexity is not your friend.... as software systems grow more complex, they will contain more flaws and these flaws will be exploited by cyber adversaries.”⁸ More recently, following the Salt Typhoon attack in 2024, FBI and Cybersecurity and Infrastructure Security Agency (CISA) officials cautioned Americans against sending text messages through unencrypted apps, noting the potential exposure to hackers.⁹ As Australian Security Intelligence Organisation director general Mike Burgess noted, these hacking efforts have already threatened critical infrastructure in Australia.¹⁰

When governments mandate encryption backdoors, many businesses may find that their only option, from a cybersecurity standpoint, is to stop offering the encrypted service altogether. Thus, these mandates deprive law-abiding citizens of the most secure methods of communication, making it easier for radicalised groups to execute cyberattacks.

Developments in AI and quantum computing have only accentuated the dangers of compromising encryption. Hackers have more powerful tools at their disposal than in the past, and can find security vulnerabilities much faster than was previously possible. In this environment, commensurate strengthening of encryption (such as adopting post-quantum encryption) is increasingly necessary to protect Australians against malicious attacks.¹¹ Weakening encryption moves Australia away from what is needed to protect its citizens.

2. Authoritarian regimes can exploit encryption vulnerabilities in other nations

Authoritarian regimes often used encryption backdoors to undermine democracy and civil liberties.¹² International law professor Antonio Ali notes that “[j]ournalists, activists and other vulnerable groups depend on these systems to operate securely, often in contexts where their own safety is at risk. For them, weakening encryption could mean the difference between

⁷ See, e.g., Jesse Lieberfeld, *Why Encryption Matters*, Disruptive Competition Project (Feb. 20, 2025), <https://project-disco.org/privacy/why-encryption-matters/>.

⁸ *Is Your Data on the Healthcare.gov Website Secure?* Hearing before the H. Comm. on Science, Space and Technology, 113th Cong. 2-3 (2013) (statement of Fred Chang, Chair in Cybersecurity, SMU).

⁹ See, e.g., *Mobile Communications Best Practice Guidance*, CISA (Dec. 18, 2024), <https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf>.

¹⁰ Kirsty Needham, *Australian spy chief says Chinese hackers probing telecoms, key facilities*, Reuters (Nov. 12, 2025), <https://www.reuters.com/world/china/australia-spy-chief-says-chinese-hackers-probing-telecommunications-critical-2025-11-12/>.

¹¹ See, e.g., Melissa Chambers, *Why post-quantum encryption should be treated as critical infrastructure*, World Econ. Forum (June 11, 2026), <https://www.weforum.org/stories/cybersecurity/cybersecurity-post-quantum-encryption>.

¹² See Lieberfeld, *supra* note 7.

being able to do their work safely and being exposed to real and tangible dangers.”¹³ As the UN Special Rapporteur on Freedom of Expression and Belief notes, encryption weaknesses “invariably undermine the security of all users online, since a backdoor, even if intended solely for government access, can be accessed by unauthorized entities, including other States or non-State actors.”¹⁴

Consequently, undermining encryption has a chilling effect on speech: In 2016, after Russia instituted mandatory encryption backdoors, a Brookings Institute report found that “Civil society groups and independent media have been the primary targets of legalized surveillance, repression, and censorship” as a result.¹⁵

Crucially, authoritarian regimes’ use of such backdoors need not be restricted to their own subjects. As the Australian Strategic Policy Institute has recognized, encryption vulnerabilities can allow such regimes to access foreigners’ communications as well— between 2011 and 2023, at least 44 authoritarian regimes contracted with spyware companies to exploit these vulnerabilities.¹⁶ Weakened encryption will thus allow authoritarian regimes to more easily radicalise groups within Australia.

3. Encryption is critical for maintaining Australia’s data sharing agreements

Many radicalised groups operate internationally, and combating threats from such groups often requires close coordination between Australia and other countries. To expedite cross-border data requests and data productions from U.S.-based service providers, Australia entered into a CLOUD Act executive agreement with the United States in 2021. This agreement allows Australia to bypass the MLAT process and make direct requests for data from U.S. providers, expediting the process by which Australian authorities may access data when investigating serious crimes.¹⁷ Additionally, the CLOUD Act requires that such executive agreements “not create any obligation that providers be capable of decrypting data.”¹⁸

¹³ Antonio Ali, *Human Rights Implications of Encryption Backdoors* 61 (2025), <https://iris.unitn.it/retrieve/c1c3440c-f0de-4fcc-bfa7-7ebf6422df5f/Koine3-DeCifrisEruditorum%20copia.pdf>.

¹⁴ David Kaye, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, United Nations Human Rights Council 15 (May 22, 2015), <https://docs.un.org/en/A/HRC/29/32>. See also *Unofficial Companion to Report of the Special Rapporteur (A/HRC/29/32) on Encryption, Anonymity and the Freedom of Expression*, U. of Calif. Irvine L. Int’l Justice Clinic (June 2015), https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/States/Selected_References_SR_Report.pdf; *Encryption and Anonymity follow-up report*, United Nations Human Rights Council (July 13, 2018), available at <https://digitallibrary.un.org/record/1638475?ln=en&v=pdf>.

¹⁵ Alina Polyakova & Chris Meserole, *Exporting digital authoritarianism: The Russian and Chinese models*, Brookings Inst. (Aug. 27, 2019), https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

¹⁶ Angela Suriyasene, *Spyware is spreading far beyond its national-security role*, Austl. Strategic Pol’y Inst. (Feb. 7, 2025), <https://www.aspistrategist.org.au/spyware-is-spreading-far-beyond-its-national-security-role/>.

¹⁷ *Cloud Act Agreement*, *supra* note 3, art. 3, § 4.c.

¹⁸ 18 U.S.C. § 2523(b)(3) (2018), <https://www.law.cornell.edu/uscode/text/18/2523>.



Requiring providers to weaken encryption is therefore directly at odds with Australia's CLOUD Act obligations.

Compromising encryption has already caused great concern among US officials regarding the viability of CLOUD Act executive agreements. Following the United Kingdom's use of a technical capability notice to demand access to encrypted data, United States lawmakers from across the political spectrum expressed concern that the action jeopardised US security policy.¹⁹ Lawmakers have expressed similar concerns that Canada's C-22 bill could create encryption vulnerabilities that might impede a CLOUD Act agreement between the US and Canada.²⁰ Exercising existing authorities or establishing new laws that can undermine encryption would compromise Australia's ability to provide the data security necessary for CLOUD Act compliance.

The CLOUD Act illustrates an important cybersecurity principle: Protecting civilians' data is a transnational endeavor. Security vulnerabilities in one country can also jeopardise data in countries with which it has cross-border data sharing agreements. Combating radicalised groups often requires international collaboration, and encryption is vital to ensure that radicalised actors cannot avail themselves of security vulnerabilities in any of the countries where they operate.

Conclusion

CCIA believes in empowering law enforcement to avail itself of every practical and ethical tool at its disposal when pursuing malicious actors. However, undermining encryption will lead to grave consequences for cybersecurity and privacy, creating more vulnerabilities for radicalised actors to exploit, both within Australia and abroad. Australia's ability to protect its citizens from attacks by radicalised actors and maintain its CLOUD Act obligations depends on preserving encryption.

Sincerely,

Jesse Lieberfeld

Policy Counsel

Computer & Communications Industry Association

¹⁹ See, e.g., Letter from Senator Ron Wyden (D-OR) and Representative Andy Biggs (R-AZ) to Tulsi Gabbard, Director of National Intelligence (Feb. 13, 2025), <https://www.wyden.senate.gov/imo/media/doc/wyden-biggs-letter-to-dni-re-uk-backdoors.pdf>; Letter from Sen. Alex Padilla (D-CA) and Rep. Zoe Lofgren (D-CA) to Pam Bondi, Attorney General (Feb. 26, 2025), <https://www.padilla.senate.gov/wp-content/uploads/Padilla-Lofgren-DOJ-Letter-2.26.25.pdf>.

²⁰ See, e.g., Letter from Representative Jim Jordan (R-OH) et al. to Gary Anandasangaree, Minister of Public Safety (May 7, 2026), <https://justthenews.com/sites/default/files/2026-05/Jordan%20letter.pdf>.