



Trusted Future Comments to the Inquiry into the Nature and Drivers of Radicalisation in Australia

Submitted by:
Trusted Future
1100 G Street, Suite 750
Washington, DC 20005
United States of America
Contact: James Lamond, james@trustedfuture.org

Introduction

On behalf of [Trusted Future](https://www.trustedfuture.org/), a non-profit organization dedicated to the belief that we need smart well-informed policies to drive trust throughout today's digital ecosystem, we welcome this opportunity to provide input to the inquiry into the nature and drivers of radicalisation in Australia, following the referral from the Minister for Home Affairs.

At the outset, we wish to express our deepest sympathies to all those who have been impacted by violent extremism and radicalisation within Australia's borders. The tragic events of last year—most notably the devastating and senseless attacks that took place on Bondi Beach last December that killed 15 people and wounded another 40 -- serve as a sobering reminder of the very real, human cost of extremist ideologies. These events have deeply shaken communities, left lasting trauma and understandably prompted urgent calls to ensure that Australians are kept safe from those who seek to cause harm. We unequivocally share the government's commitment to addressing the root causes of radicalisation and preventing future tragedies.

Tackling the complex drivers of radicalisation requires robust, fact-based, and strategic solutions. It takes targeted, collaborative approaches that empower law enforcement and intelligence professionals, bolster community-led intervention programs, and utilize focused intelligence gathering to identify, deter, and disrupt bad actors before they can strike. Protecting the public is paramount, and there is a critical need for policies that directly address the spread of extremist content and the radicalisation pathways that lead to physical violence.

Understanding the Threat Landscape and the Complex Challenge

As the Committee looks at the pathways that lead to radicalisation, we'd like to first highlight some of the important research that allows us to better understand the complex challenge of online radicalisation. Experts have come to understand that tackling online radicalisation requires a multi-layered approach combining digital literacy, platform accountability, and real-world community support.

One of the most comprehensive studies was performed by the U.S. National Institute of Justice's (NIJ) Domestic Radicalisation to Terrorism program research on the [Role of the Internet and Social Media on Radicalisation](#). This report looked at a broad range of research and found that radicalisation often takes different pathways, is complex, and there is still much we still don't know.

The study recommends policymakers:

- **Consider the Role of the Internet and Social Media in Relation to Other Factors and Activities.** Online behaviors, activities, and engagement do not occur in a vacuum. They suggest, "[r]ather than consider the role of the internet in isolation, policymakers and practitioners should consider the interplay between online and offline communications and engagement in developing efforts to address the influence of both on radicalisation processes."
- **Consider Specific Interventions Tailored to Different Types of Online Engagement.** Interventions and activities designed to address the impact of the internet and social media on radicalisation processes should be appropriately tailored based on the type of online engagement and the online spaces in which they are carried out. According to their research, "attention to how offline dynamics may impact online engagement, and the development of proactive messaging efforts to address these circumstances, may be prudent in mitigating their impacts."
- **Understand When Efforts To Address Violent Extremism Online May Overlap With Broader Social Goals and Violence Reduction Efforts.** Their research found, "simply engaging with or viewing hateful or violent extremist content online does not, in itself, imply a greater propensity to radicalize to violence." They specifically cite the University of Massachusetts-Lowell's [Center for Terrorism and Security Studies \(CTSS\)](#) considerations and guidelines for ethical engagement in preventing and countering violent extremism as useful in thinking through the ethics of this type of engagement.

Strengthen, Don't Weaken, Encryption Safeguards

A common suggestion that emerges in these debates involves weakening encryption and enabling "back door" access to encrypted communication for law enforcement and intelligence agencies. In times of crisis, there is rapid interest in seeking broad access to private communications – often proposed in ways that require weakening end-to-end encryption. Law enforcement has an understandable interest in wanting the unrestricted



ability to surveil those suspected of politically motivated violence, terrorism, and violent extremism. Yet, weakening end-to-end encryption would be a profound misstep. Undermining the strength of encryption is a step backward, not forward, in efforts to tackle radicalisation and advance a more trustworthy digital ecosystem.

Law enforcement and intelligence agencies absolutely need the ability to identify possible avenues for radicalisation, and the ability to identify and prosecute crimes within the law. But too often there are well-intentioned proposals dealing with encryption that rely on solutions that we have long known are unworkable. These proposals are effectively aimed at removing the "lock" from the encryption "lock box" or providing law enforcement with a digital master key.

Proponents of these encryption backdoor solutions make three primary arguments:

1. The first argument is that access to encrypted communication is necessary because it can enable law enforcement to obtain convictions they otherwise can't. However, sophisticated criminals and terrorist networks can simply download one of many open-source encryption tools to doubly encrypt their data. In this easily accomplished scenario, even if the primary encryption is unencrypted, the communication content remains encrypted, beyond law enforcement's reach, and the data would still look like gibberish. Nothing is gained.
2. The second argument is that officials can be trusted to keep a master key safe and the backdoors secure. But cryptographic researchers have demonstrated that it's [impossible to create](#) a backdoor for the "good guys" that doesn't eventually get exploited by the "bad guys." And terrorists, adversaries, and those seeking to radicalise would love access to a backdoor for encrypted data because it enables them to do vastly more harm.
3. The third argument is that there is a way to create a secure backdoor for one-person, without harming the integrity of encryption for everyone else – that the technical community can find a way to invent such a technology, they just need to "nerd-harder." But there is no way to overcome one of the inherent mathematical features of encryption – a feature which ensures that only the sender and intended recipient have the mathematical keys necessary to read it. The provider doesn't have a key and has no way to access it regardless of its engineering prowess. No technology can change the fundamental laws of math.

As the Committee considers the tools necessary to combat these threats, it's important to avoid solutions, while well intended, that create a new set of harms that could impact every consumer, business, and law enforcement entity. More specifically, we strongly caution against pursuing steps that would undermine the vital role of digital encryption in protecting Australian consumers, business data, and national security operations.



Encryption is Vital for the Safety, Security, and Prosperity of Australians Now and Into the Future

End-to-End Encryption is one of the most powerful tools available to protect Australia's digital world. As new technologies emerge from AI to quantum computing, this importance only grows. *Encryption is the Foundational Bedrock of Modern Digital Security.*

Encryption protects the personal privacy of everyday Australians, secures our financial systems, shields vulnerable communities, and defends our national infrastructure against cybercriminals and hostile state actors.

In today's modern economy, encryption has become ubiquitous in nearly every part of the technology stack, and essential for almost everything we do. We rely on the strong encryption built into our web browsers to protect our login credentials every time we log in to our bank, our work, or a health provider's website. We rely on strong encryption to protect our credit card numbers every time we purchase something online, to protect the data on our phones in case they are lost or stolen, to protect data in the cloud, and increasingly, to protect the content of messages — so that only the sender and intended recipient can read it.

Salt Typhon was a wakeup call and inflection point. It was a moment when China's Ministry of State Security managed to gain access deep inside major networks including burrowing into [Australia's critical infrastructure](#) networks and collecting the content of communications. It led the US, Australia, the UK, Canada, Germany, New Zealand and others to jointly [recommend internet traffic](#) be "end-to-end encrypted to the maximum extent possible," and led leaders to [state the obvious: encryption is our friend](#).

Encryption has become so important and such a powerful protector of our data because it has inherent super-powers. No third party has access to the data. Only the sender and intended recipient can access it. For anyone else who intercepts it – the data just looks like gibberish – so it can keep our data safe, even if it is lost or stolen.

Strong encryption is the invisible backbone of Australia's digital economy.

Encryption ensures that everyday financial transactions, corporate operations, and personal communications remain private and secure from cybercriminals.

- **Protecting Customer Data:** Under Australia's Privacy Act of 1988 and the Notifiable Data Breaches (NDB) scheme, businesses face significant fines for leaking customer data. Companies use encryption at rest (storing data) and in transit (moving data) to safeguard customer files and use encryption as a primary method to protect data both in transit and at rest, helping organisations meet their obligations under the Act.

- **Securing Remote Work:** With hybrid work standard across corporate Australia, employees access internal networks via encrypted Virtual Private Networks (VPNs). This keeps corporate networks secure even when staff work from a local café or home Wi-Fi.
- **Safeguarding Intellectual Property:** Australia's booming tech, defense, mining, and agricultural sectors rely on encryption to protect proprietary algorithms, mining survey data, and trade secrets from industrial espionage.
- **Supply Chain and B2B Invoicing:** Australian businesses use encrypted Electronic Data Interchange (EDI) channels to automatically order stock and process multi-million dollar invoices safely, preventing invoice redirection scams.

AI has the potential to hack into systems and put sensitive Australian data at risk.

As AI cyber-risks advance, use of strong encryption is becoming even more important to Australia's future. Australia's leaders were rightfully outraged when a rogue [OpenAI agent infiltrated an Australian government website](#). This new kind of AI threat was so unexpected, unfathomable, and so critical, [Prime Minister Albanese](#) quickly raised the alarm on the threats posed by new AI hacking models to world leaders at the UN. Fortunately, in this instance, the AI agent did not obtain any personally identifiable health data. But if it did, the government health data would look like gibberish and be useless to the AI agent, or anyone else, because the data is encrypted. Australia's government health data—such as records in the national My Health Record system and related databases—is protected by encryption. Government health platforms and associated clinical databases employ [standard encryption measures to protect health data both in transit and at rest](#) (such as AES-256 or equivalent government-approved frameworks.) As new AI superhacking models make data breaches more likely they put personal and corporate data at greater risk, making strong encryption even more vital for protecting it.

With growing AI threats and risks, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) joined with the US Cybersecurity Infrastructure & Security Agency (CISA), the Federal Bureau of Investigation (FBI), New Zealand's Government Communications Security Bureau's National Cyber Security Centre (NCSC-NZ), and the United Kingdom's National Cyber Security Centre (NCSC-UK) to publish [AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems](#). In this new AI world, it highlights the importance of continuous encryption (encryption of data in transit, at rest, and in use) at every stage of the technology and AI lifecycle. Steps we should not undermine.

AI superhacking models aren't the only threat to Australia's personal data.

Experts now warn that advances in quantum computing mean we need to strengthen our encryption policies even further. Major companies and the government are now dramatically shortening their readiness deadlines for the [arrival of Q Day](#), the point at which existing

quantum computers can break public-key cryptography algorithms that secure decades' worth of secrets belonging to militaries, banks, governments, and nearly every individual on earth. Earlier this year, both Google and Cloudflare [bumped up](#) their internal deadline for PQC (post-quantum cryptography) readiness to 2029. The [Australian Signals Directorate](#) (ASD) is moving fast too, requiring organisations to have a refined post-quantum cryptography (PQC) transition plan by the end of 2026, to commence migration for critical systems by the end of 2028, and complete the full transition away from traditional asymmetric cryptography (such as RSA and elliptic curve cryptography) by the end of 2030.

Weakening Encryption Will Not Stop Terrorism or Violent Extremism

Given the importance of encryption across society and the tradeoffs for weakening it, by building in a back door, it is important to also understand how such efforts would or would not prevent terrorism and violent extremism.

The reality is that encrypted communications are not what is causing radicalisation or even necessarily the coordination tool for terrorism and violent extremism. The [Australian Federal Police \(AFP\)](#) confirmed that the father-and-son perpetrators of the Bondi Beach attack, Sajid and Naveed Akram, were inspired by Islamic State ideology but acted entirely as lone actors. They did not receive direct operational instructions or tactical training from an overseas terror cell via encrypted networks. The reality is that modern terrorism is frequently not hierarchical. It instead often relies on diffuse ideological influence prompting individuals to plan and execute complex attacks autonomously. This dates back further, but has been a [mainstay of terrorist strategy](#) since 2010 when al Qaeda launched its "*Inspire*" strategy marking a pivot away from relying on heavily coordinated, central command attacks, instead seeking to incite "lone-wolf" actors or small cells in target countries with "do it yourself" instructions.

Rather than fundamentally undermining encryption and compromising the digital security of everyone in an attempt to monitor a dangerous few, there are smarter, more effective approaches. By focusing on metadata analysis, improving law-enforcement technical training, utilizing authorized intelligence activities, and investing in open-source intelligence and community-based preventative measures, leaders can equip Australia's security agencies with the tools they need.

A Pragmatic Action Plan for Addressing Radicalisation

Foster Digital Literacy and Critical Thinking.

Digital literacy and parental engagement can help teach young people and internet users how algorithms, memes, and gaming spaces can be used to normalize extreme views. Critical thinking skills are also important to encourage both open-curiosity, fact checking to question emotionally charged content, and the skills to recognize extremist propaganda without violating free speech rights. For example, the [US Department of Homeland Security](#)



highlights ways schools and educators are building resilience against the consumption and spread of false narratives through digital literacy and critical thinking. Likewise, organizations like [Stanford Social Media Lab](#) promote media literacy in schools and communities to "inoculate" young people against extremist rhetoric and hateful online content.

Platform content moderation.

Major social media and internet platforms use a combination of automated technology, industry collaboration, and policy guidelines to detect, restrict, and remove extremist content aimed at radicalisation. Accurate [content moderation on gaming platforms](#) can save lives in a number of ways, including by acting as a warning system about the risks of extremist violence and [removing the fuel that incites extremist violence](#).

Strengthen user reporting.

Developing stronger user reporting mechanisms to identify and address online harms can help without impacting encryption. When a participant in an encrypted conversation reports it, the plaintext they already hold can be shared with the platform. This keeps the encryption model intact because a party to the chat discloses it voluntarily. Investments and requirements here could include better reporting interfaces, trusted-flagger channels for NGOs and researchers, and quick escalation to law enforcement when there is an imminent threat.

Promote researcher access to data.

Governments should develop legal frameworks for platforms to allow researchers, journalists, think tanks, and academics to access data for research and reporting purposes. This could specifically include viral content that passes an established threshold, allowing them to analyze and better understand the dissemination of content and contribute to better metadata analysis.

Enhance efforts to disrupt illicit financial flow.

Law enforcement and intelligence agencies can disrupt crowdfunding and crypto flows that support extremist movements. The Financial Action Task Force (FATF), which Australia is a member of, [has found](#) that challenges in this space "include the complexity of crowdfunding operations, the use of anonymising techniques, and lack of training and terrorist financing expertise within the crowdfunding industry to detect suspicious activity." Investing in these capabilities and requirements of safeguards for the crowding funding industry would help detect coordinated plans without undermining encryption tools.

Combine technical solutions and human intelligence to disrupt and deter.

Investing more resources with organizations like the Australian Security Intelligence Organisation (ASIO) to apply authorized exquisite technological solutions to monitor and



surveil communications outside of end-to-end encryption combined with greater human intelligence analysis and on-the-ground intelligence will be able to provide a fuller intelligence picture without breaking encryption.

Conclusion

We believe that addressing the threats of online radicalisation is of immense importance to the safety and security not only of Australia but to countries around the world. We need to be able to trust that our digital ecosystem is safe and secure. Trust in technology platforms and infrastructure is a vital prerequisite for countering violent extremism, as effective security measures depend heavily on user participation, early intervention, and system integrity. When trust breaks down, the tools and avenues used to detect, disrupt, and prevent radicalisation become significantly less effective. This is why we argue for a comprehensive and multi-level approach that does not undermine encryption – the very tool that keeps people safe and secure online.

We need to continuously do more to make sure the law-enforcement and intelligence communities have the resources, training and tools it needs to effectively perform their jobs in the most effective ways – and in the process to better protect the public. We should ensure that companies are held accountable for moderating content on their platforms, that citizens are empowered and able to act, and that we continue to increase our understanding of this dangerous threat. But as the [research group](#) on encrypted messaging and extreme speech at the Center for Advanced Studies, LMU Munich found “indiscriminately targeting encryption... can undermine safety and security of encryption for ordinary users.” Put simply, you cannot protect people by making them less safe.

We urge the Committee to recognize that Australia does not have to choose between public safety and digital security; through strategic, targeted approaches, we can effectively combat radicalisation while preserving the secure technologies that keep all Australians safe.