

Consumer Choice Center Comments on the Inquiry into the nature and drivers of radicalisation in Australia

October 29, 2026

**Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600**

The **Consumer Choice Center** is an independent, non-partisan consumer advocacy group championing the benefits of freedom of choice, innovation, and abundance in everyday life. We champion smart policies that promote growth, lifestyle choice, and defend technological innovation.

Herein, we offer our comments on the Inquiry into the nature and drivers of radicalisation in Australia, albeit from a consumer-focused perspective.

General Views on the Consultation

The purpose of the consultation is to examine radicalisation in Australia and its relation to violence, terrorism, and violent extremism. The main focus of this particular inquiry is the role of technology in facilitating this radicalisation.

Ending radicalisation and extremist violence in Australia and around the world is an important political goal. That said, the Consumer Choice Center is concerned that the potential remedies to these problems, especially where they concern consumer technologies, might cause more problems than they are able to solve.

As consumer advocates, we will focus on two main topics that are being explored by this inquiry: encryption, and the obligations of technological providers. We will also use examples from other countries to make the case that consumer privacy must be kept in mind while exploring the topics included in this inquiry.

Our response to the Inquiry's interest in the role of technology and encrypted communications

In response to radicalisation, it is natural to want to be able to dive into encrypted conversations in order to find and correct any radical behaviour. However, this type of action would mean all Australians would no longer have access to truly encrypted platforms online. There is no way to turn off encryption for some without turning it off for all, and any backdoors to encrypted information can easily be abused by bad actors including hackers and hostile foreign governments.

A common misconception is that a government can gain access to encrypted information by approaching tech companies on a case-by-case basis, but that is simply not how encryption technology works. If a service provider opens a backdoor for encryption for one person or one situation, they are essentially breaking down that encryption for all of their customers. Apple, WhatsApp, and Signal have all shown that if encryption is broken for one, it is broken for all. In 2016, Apple's Tim Cook [explained](#) this process in response to a court ruling involving the United States' Federal Bureau of Investigation:

"In today's digital world, the "key" to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge."

The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable."

Indeed, it would be unreasonable for the Australian Government to move in that direction. People's entire lives would be exposed, from political dissidents that fear for their lives to everyday Australians who want their financial

information to remain secure. Apple also sounded the alarm in response to Australia's Bill 2018, [stating](#):

"Some suggest that exceptions can be made, and access to encrypted data could be created just for only those sworn to uphold the public good. That is a false premise. Encryption is simply math. Any process that weakens the mathematical models that protect user data for anyone will by extension weaken the protections for everyone. It would be wrong to weaken security for millions of law-abiding customers in order to investigate the very few who pose a threat."

If the experts who build encrypted systems are sounding the alarm, policymakers should listen. Looking at encryption as playing a role in radicalisation is focusing on the wrong mechanism. Creating a honeypot of information by allowing for a backdoor to encrypted information is essentially handing a gift over to bad actors, from both a safety and privacy perspective.

It may seem that encrypted platforms are shadowy places where bad people meet to talk about doing harmful things, but encrypted information and communication is used for financial information, company intellectual property, family chat groups, private health data, and browsing history, among many other things essential to everyday life in the modern world. In fact, much of the modern Internet relies on encryption to securely and privately transmit data without it falling into the hands of hackers and bad actors like hostile foreign governments.

One group of people that will be particularly harmed by an opening up of encryption technology is Australian political dissidents who have escaped and remain hidden from oppressive regimes. Many political dissidents come to Australia for refuge from oppressive foreign governments, many of which might even fund radicalisation and terrorism. Taking away a tool that would allow political dissidents to organise and communicate in Australia would not only be anti-democratic, it would also put their lives in grave danger.

This is also one of the major problems with [Canada's Bill C-22](#), which would give Canadian law enforcement tools to investigate serious crime by, among

other things, mandating the breaking of encryption by telecom providers. Canada is also home to many political dissidents, and disallowing encrypted communication means that hostile governments can easily access the personal information of dissidents, as well as the personal information of those they are speaking with.

In Canada, there are examples of foreign regimes accessing technological information and harming dissidents as a result. [Omar Abdulaziz](#) left Saudi Arabia in 2009 for Montreal, Quebec, Canada, and became one of the most prominent Saudi opposition voices outside the kingdom, as well as a close confidant of journalist Jamal Khashoggi. In 2018 his phone was infected with Pegasus spyware, which was traced to a Saudi-linked operator and likely played a role in the chain of events that led to Khashoggi's murder. Another example is [Sheng Xue](#), a Chinese dissident who fled to Canada and believes Chinese agents have tracked her movements and threatened her life. Disallowing encryption is handing over the information needed to ruin the lives of dissidents and those they are connected with.

Australia has not been immune to these types of cyberattacks on dissidents. There have been [reports](#) of Chinese hackers targeting around 500 Uyghur activists, some of whom reside in Australia. One Uyghur dissident residing in Australia described a deep fear of being targeted by Chinese hackers and inadvertently exposing the information of other dissidents that she communicates with. This threat was created mostly as a result of malware attacks, but opening a backdoor for these governments to track down and find dissidents in Australia would be like the Australian Government handing over the information and safety of dissidents in its care to the governments that want to see them harmed.

Outside of the harm that could be dealt to political dissidents, any action that would weaken or eliminate encryption technology could be abused against everyday Australians practising free speech or simply using encrypted services to protect their private information. The committee must take into consideration the heavy burden of exposing political dissidents to cross-border intimidation and harm, and of potentially exposing the private

information of all Australians, as it decides how to deal with encryption technology.

Our response to the Inquiry's interest in the obligations of digital platforms, gaming and messaging providers in detecting, reporting and responding to extremist content

As we have shown in the previous section, opening up a backdoor to private information is dangerous and harmful, and should therefore not be required of digital platforms, gaming, and messaging providers.

Companies that develop encrypted technology have sounded the alarm bells many times on why such obligations would take away the privacy of all Australians. In 2025, the head of Signal responded to Australia's push to have a backdoor to encrypted data by saying:

"...our commitment to end-to-end encryption, maintaining robust, technically guaranteed privacy for everyone who uses Signal, never wavers. That's the reason we exist. Our ability to make good on that commitment, for the people of Australia who depend on our services – often for very high-stakes communication where there is real risk involved – does face threats from legislation."

She also said that Signal would leave Australia rather than put millions of Australians' privacy at stake. Signal has made similar threats to leave rather than comply with governmental demands on encryption, including in Sweden, Germany, the wider European Union, the United Kingdom, and Canada.

The head of [WhatsApp](#), Will Cathcart, made a similar pledge of leaving the country rather than complying to the United Kingdom's Online Safety Bill. He told the BBC that this was essentially a threat to western democracy, saying: *"When a liberal democracy says, 'Is it OK to scan everyone's private communication for illegal content?' that emboldens countries around the world that have very different definitions of illegal content to propose the same thing."*

It is telling that corporations would rather exit a market than undermine the security of their users. These companies even feel a responsibility to uphold the democratic values of free speech and anti-authoritarianism. Australia should have a similar goal.

The Consumer Choice Center also urges the Committee to reconsider any steps towards implementing policies that would gather information before users can access online platforms, messaging apps, and gaming sites. Although this may seem like an attractive option to deal with radicalisation, it will only put swathes of personal information of innocent Australians in the hands of corporations that can easily get hacked.

This has already been a problem in Australia: in 2022, [Optus](#) reported a major data breach that affected 9.5 million Australians, more than a third of the population. Customers were informed that their home addresses, ID documents such as driver's licences and passports, phone numbers, medical identification, and customer names had been exposed. The company had retained the sensitive information to [comply](#) with the government's mandate to retain customer information for a number of years.

A similar situation occurred in the same year when [Medibank](#), Australia's largest health insurer, suffered a ransomware attack that affected 9.7 million Australians. User information was exposed, including health data that was posted on the dark web about users' [mental health and alcohol use](#).

The downsides of exposing Australians to the possibility of losing their privacy are too big to ignore. As the Committee struggles with the question of how to quell radicalisation, it cannot hand over the keys to the personal lives of all Australians as a baseline response. Australians would be right to worry about their safety and their personal information under such regulations, and backdoors, once opened, can never truly be closed again.

As with other liberal democratic nations, Australia currently possesses the law enforcement and judicial tools necessary to stem the tide of criminal behaviour and terrorist activity. Decisions about when and whether to use them can be made within the rule of law.

Inventing new powers to break technology that serves the interests of peaceful and innocent Australians would be a costly trade-off, and we advise against it. Protecting secure communications and encryption for Australians is vital, as is ensuring law enforcement can use its existing powers and technology to catch criminals.

Conclusion

Examining the nature and drivers of radicalisation in Australia is an important project that deserves evidence-based solutions. The Consumer Choice Center shares the Committee's concern about radicalisation in Australia and indeed around the world, but we are wary of any solution to this problem that includes taking away the privacy of everyday Australians.

This is a case of using the wrong tools to fix a real problem. The evidence shows that making it harder to use encrypted devices, or mandating a backdoor to encryption, cannot track down radicalisation without exposing millions of Australians to attacks from hackers and hostile foreign governments. Instead of solving one problem, eliminating online privacy will only create another problem for the government to solve in the long run: that of recovering the privacy of its citizenry from bad actors.

Any policy that takes away digital privacy, or hoards personal information in a way that makes hacking easier, is a violation of the principles of security and freedom that the citizens of Australia expect their government to uphold. We therefore urge the Committee to take these grave concerns into account when undertaking this Inquiry.

Yours faithfully,

Sabine Benoit
Canadian Policy Associate

Yaël Ossowski
Deputy Director
Consumer Choice Center