Isaac Kfir

9 July 2019

Submission to the Joint Parliamentary Committee on Intelligence and Security in respect to a review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Isaac Kfir

This submission does not reflect the Australian Strategic Policy Institute perspective. It is the opinion of the author Dr Isaac Kfir deputy director of director defence, strategy and national security, head of the counterterrorism policy centre, ASPI.

1. The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 is a reaction to several terrorist attacks, attempts at attacks, and pressure from the security agencies (ASIS, ASIO, ASD) and local and federal police, the Australian government introduced the. The legislation amended several other Acts: the 1997 Telecommunications Act, the 1979 Australian Security Intelligence Organisation Act, and the 2004 Surveillance Devices Act.
2. The measure has attracted enormous interest and controversy.[1]
3. Australia is at the forefront internationally in promoting access for intelligence and law enforcement agencies to data held by telecommunications and technology companies and in legislating on the duty to remove online violent extremist materials through such measures as the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019).[2] A further indication of

[1] See for example the report issued by the Parliamentary Joint Committee on Intelligence and Security in April 2019 referencing the written submission from a host of entities and individuals. Parliamentary Joint Committee on Intelligence and Security, 'Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018', Parliament of the Commonwealth of Australia, Canberra, April 2019, online. Jennifer Wilson, 'When an opposition votes for bad laws, democracy is broken', *Independent Australia*, 12 June 2019, online; Paul Karp, 'Home Affairs plays down encryption law fears and promises to help industry cover costs', *The Guardian*, 20 January 2019, online; Ariel Bogle, 'Police use new phone-cracking powers as Government works out the fine print', *ABC News*, 7 February 2019, online.

[2] Paul Karp, 'Coalition's surveillance laws give police power to access electronic devices', *The Guardian*, 14 August 2018, online; Paul Karp, 'Tech companies not 'comfortable' storing data in Australia, Microsoft warns ', *The Guardian*, 27 March 2019, online; Paul Karp, 'Australia passes social media law penalising platforms for violent content,' *The Guardian*, 4 April 2019, online; Josh Taylor, 'Terrorism crackdown laws could give greater power to block Australians from websites', *The Guardian*, 1 July 2019, online.

Australia being a leader in this field was that at the G20 Summit in Osaka, Prime Minister Scott Morrison got the other world leaders to support his 'Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism (VECT).[3]

4. However, these initiatives are not addressing the root problems of violent extremism,[4] nor as will be argued below are they appropriate to the current threat environment.

5. Empirical evidence indicates an increase in lone actor activities often with the individual not reaching out to others. Concomitantly, there is evidence that violent extremists who have a social media presence are more likely to come to the attention of the security services.[5]

6. The explanatory materials issued with the legislation states that over 90 percent of the lawfully intercepted telecommunication information is encrypted. The implication is that by not having access to decryption, Australia, Australians and Australian interests are put in danger.[6]

7. The legislation, which focuses on encrypted information gathered from terrorists, sex offenders and criminal organisations were meant to:

    a. empower law enforcement and national security agencies to request, or compel, assistance from telecommunications providers;

    b. established powers that permit law enforcement and intelligence agencies to obtain warrants to access data and devices;

    c. amended the search warrant framework under the Crimes Act and the Customs Act;

    d. expand the ability of criminal law enforcement agencies to collect evidence from electronic devices;

8. Several arguments have been provided to defend the measure, and the two key ones have been:

    a. the pervasive use of encryption by criminal organisations and terrorists requires that the security agencies have tools to decrypt messaging so as to protect Australians and Australian interests.[7]

---

[3] G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet For Terrorism and Violent Extremism Conducive to Terrorism (VECT), 29 June 2019, online; Australian Associated Press, 'Scott Morrison wins G20 support to root out terrorist content on the internet', *The Guardian*, 30 June 2019, online.
[4] Isaac Kfir, 'The Christchurch call – so close, yet so far', *APPS Policy Forum*, 27 June 2019, online.
[5] Joe Whittaker, 'How Content Removal Might Help Terrorists', *Lawfare*, 30 June 2019, online.
[6] Telecommunications and other Legislation Amendment (Assistance and Access) Bill 2018, Explanatory Memorandum, The Parliament Of The Commonwealth Of Australia, Canberra, online.
[7] See for example the submission by The Hon Peter Dutton MP to the Joint Parliamentary Committee on Intelligence and Security, 22 November 2018, ref. no. 2018-061418; Submission by the Department of Home Affairs, 'Parliamentary Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, undated.

b. encrypted messaging makes it hard for police and security authorities to track nefarious activities.[8]

9. The submitter understands the reasoning behind the government's purpose in granting the security agencies powers to gain access to lawfully collected encrypted information. However, I argue in this submission, in which I focus on the counterterrorism reasoning behind the legislation, that in respect to dealing with terrorists and violent extremists, the legislation is:

a. disproportionate to any threat of terrorism or threat to national security as the legislation doesn't really address the 'demand side' – the nature of the content – collected by terrorists and would-be terrorists. Moreover, because the information is encrypted, the challenge is to ascertain whether the content is moderate in its hostility towards people or the state, fringe or extreme.[9]

b. doesn't address the reality that those interested in violent extremism and terrorism are technology-affine, which means that they adapt to new media structures and avant-garde ways of communication quickly.

c. violent extremists have moved to smaller, more secure, niche platforms that the legislation doesn't cover nor can cover because of the nature of the platforms and the applications. There is increasing evidence that violent extremists prefer to use such platforms as 8chan, 4chan, Telegram, etc. because they are seen as more secure.

The disproportionate Argument

10. There is evidence that those engaging in online violent extremism have largely left mainstream social media, opting instead to use niche social media platforms and messaging applications such as Telegram, 4chan, 8chan, Viber, Kik, Ask.fm, etc. Moreover, the legislation may not cover other forums used by violent extremist to propagate their ideas. There is for example no reference to gaming platforms.[10]

There is a strong likelihood is that extremists will adapt, as they have done already, their communication strategies in response to legislative changes, creating the risk of 'legislative whack-a-mole which significant unintended consequences.

---

[8] See for example the submission by the Victoria Police to the Joint Parliamentary Committee on Intelligence and Security, 30 November 2018; submission by the Queensland Police to the Joint Parliamentary Committee on Intelligence and Security, undated.

[9] Donald Holbrook, 'The Terrorism Information Environment: Analysing Terrorists' Selection of Ideological and Facilitative Media', *Terrorism and Political Violence*, 2019, doi: 10.1080/09546553.2019.1583216

[10] Steam, a gaming platform, operated by a US-based company Valve, with an annual revenue of more than $US4 billion and 90 million users monthly, was used by David Sonboly, a German-Iranian teenager who shot and killed nine people in and around Munich's Olympia shopping mall in 2016, Sonboly, whom initially the German police concluded was psychological disturbed, had used the platform to rail against 'foreign invaders'. Anya Kamenetz, 'Right-Wing Hate Groups Are Recruiting Video Gamers', *NPR*, 5 November 2018, online; Patrick Begley, 'The hateful fringes of video games giant Steam', *The Sydney Morning Herald*, 21 March 2019, online; Michelle Duff, 'Gaming culture and the alt-right: The weaponisation of hate', *Stuff*, 24 March 2019, online; Der Spiegel Staff. 'The Growing Threat of Online-Bred Right-Wing Extremism', *Spiegel Online*, 28 March 2019, online.

The technological-affine argument

11. I recognise that the legislation was meant to help the security establishment provide protection for Australia, Australians and Australian interests, however it seems to have had the unintended consequence of driving violent extremists away from mainstream social media platforms and to more niche, specialist platforms, where there is no regulatory regime and the encryption methodology is vastly different.

    a. Joshua Geltzer, a former senior director for counterterrorism at the Obama National Security Council, has pointed out that 'In the era of a world wide web, bad actors will always be able to download such platforms somewhere online, even if they're banished from mainstream forums like the App Store.' Geltzer added that by compelling encrypted services to give access to third-party (government) has the potential of encouraging violent extremists or terrorists to simply turn to secure-messaging services like Telegram and Signal who eschew compliance with government.[11]

    b. Alan Z. Rozenshtein, a former attorney advisor with the Office of Law and Policy in the National Security Division of the U.S. Justice Department has argued that because there are few violent extremist, a government can always get around encryption either by paying a third-party to hack a device or simply by using existing software and hardware to gain access. Rozenshtein emphasis that this rational only work in respect to violent extremism or unique crimes and not ordinary criminal enterprises. He also adds that by framing the encryption discussion as a national security one weakens the government as it seems that government use the national security argument too many times.[12]

12. There is evidence that violent extremists use an array of tools beyond sharing violent content to attract supporters and recruits. For example, at one point, ISIL fighters created a Twitter account 'Islamic State of Cats' (@ISILCats). They have also created memes of life from Raqqah, emphasizing how mundane, simple and yet idealistic life under the Caliphate is.[13] Countering this soft power propaganda requires a sophisticated and nuanced approach not currently reflected in the legislation.

Security agencies benefit from having violent extremist on social media

13. Social media is a valuable tool for investigators and law enforcement to identify and track individuals who may be at risk of radicalisation or already participating in extremist activities. By making more demands of the social

---

[11] Joshua Geltzer, 'How to Move the Battle Lines in the Crypto-Wars', *Just Security*, 5 April 2018, online; Alan Z. Rozenshtein, 'The Encryption Debate Isn't About Stopping Terrorists, It's About Solving Crime', *Lawfare*, 9 April 2018, online.

[12] Alan Z. Rozenshtein, 'The Encryption Debate Isn't About Stopping Terrorists, It's About Solving Crime', *Lawfare*, 9 April 2018, online; Alan Z. Rozenshtein, 'Facebook, Encryption and the Dangers of Privacy Laundering', *Lawfare*, 14 March 2019, online.

[13] James Vincent, ''I Can Haz Islamic State Plz': ISIS Propaganda in Twitter turns to Kittens and Lolspeak', *The Independent*, 21 August 2014, online; Rose Powell, 'Cats and Kalashnikovs: Behind the ISIL social media strategy', *The Sydney Morning Herald*, 24 June 2014, online.

media companies to patrol content, and with these companies opting to err on the side of caution, the ability to identify individuals that may be on the way to becoming violent extremists will be curtailed.[14] According to one study, around 90 percent of US-based extremists that used social media were arrested prior to committing an offence.[15] We should think extremely carefully before undermining such a valuable investigative method.

14. I thank the Committee and the Secretary for allowing us to make this submission.

[14] There is evidence that security services already devote an enormous amount of time to troweling cyberspace and social media using predicative analytics and other AI tools to identify individuals that may be on the way to becoming radicalised. Joe Whittaker, 'How Content Removal Might Help Terrorists', *Lawfare*, 30 June 2019, online.

[15] 'The Use of Social Media by United States Extremists', National Consortium for the Study of Terrorism and Responses to Terrorism (START), undated, online; Bennett Clifford, Helen Christy Powell, 'De-Platforming and the Online Extremist's Dilemma', *Lawfare,* 6 June 2019, online.