Dr Isaac Kfir

18 September 2019

Submission to the Independent National Security Legislation Monitor on the Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA Act)

Dr Isaac Kfir

This submission does not reflect the Australian Strategic Policy Institute (ASPI) perspective. It is the opinion of the author Dr. Isaac Kfir, Deputy Director Defense, Strategy and National Security Program, Head of the Counterterrorism Policy Centre, at ASPI.

1. On 15 August 2019, the Independent National Security Legislation Monitor (INSLM), Dr. James Renwick CSC, SC, begun a public consultation phase regarding the *Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018*. The review comes at the behest of the Parliamentary Joint Committee on Intelligence and Security (PJCIS).
2. The PJCIS has requested that the INSLM consider whether the Act achieves a balance between the need to secure the public from nefarious elements, whilst ensuring that the law does not undermine public trust nor is needlessly intrusive. Moreover, the INSLM was also requested to consider whether there are appropriate safeguards for protecting the rights of individuals and that the measures are proportionate and necessary.
3. This submission is restricted to how the *Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018* impacts counterterrorism, and whether the Act aids Australia's counterterrorism regime. I argue the following
    a. Theoretically, there is a need for the government to have the right to access, upon meeting specific requirements, encrypted communication however the measures don't appear to be proportionate or even necessary when considering the nature of the current threat from violent extremists.[1]

[1] This current review could and should serve as an indication that parliamentarians are concerned that the legislation is disproportionate and may have a negative impact on social cohesion.

1. In terms of the threat it seems that al-Qaeda and ISIL are less focused on targeting western targets as they are transitioning into the disseminators of ideology – al-Qaedaism.[2]
2. There is a proliferation in lone actor activities with violent extremists opting to not reach out to known terrorist entities or communicate with such entities via extremely secure communication such as Telegram, Signal and the Dark web.[3]
3. The new generation of violent extremists seem to adapt quickly to counterterrorism measures which makes the legislation redundant in countering terrorists as they are using tools and equipment not covered by the legislation.

b. There is no evidence to suggest that when the act was considered an attempt was made to win support from minority communities. These communities often feel that counterterrorism legislation is directed at them and that little is done to address for example hate crimes, Islamophobia, racial attacks, etc.

c. Practically, there is no publicly available evidence that access to encrypted communication has helped forestall terrorist attacks. It is for the government to find a way to show that such measures as necessary, without simply stating that to do so would undermine operational capabilities.

1. It is important to note that encryption is a 'double-edged sword' as that many law-abiding citizens use encryption because so much of their lives is 'online' from banking to photos to conversion with loved ones, etc. and they want that data secured, especially in lieu of the growth of cybercrime.
2. Law abiding citizens are using encryption because they are worried about government overreach, which is why people are 'going dark'.[4]

4. One of the key shortcomings of the Act is that it fails to recognise the typology of encryption, treating it as a singular concept. Encryption appears in many forms:[5]

a. End-to-End encryption

Under this type of encryption, it is only the people (sender and recipient) that are in the communication loop who can read the message as they share

---

[2] Isaac Kfir, 'A primer on the ideological and theological drivers of AQ and Daesh: al-Qaedaism', *ASPI Special Report*, Canberra, June 2018, online; Isaac Kfir, 'The post-caliphate Salafi-jihadi environment', *ASPI Strategic Insight*, Canberra, July 2019, online.

[3] Peter Nesser, 'Military Interventions, Jihadi Networks, and Terrorist Entrepreneurs: How the Islamic State Terror Wave Rose So High in Europe', *CTC Sentinel*, 12(3), 2019, online; Joshua D. Freilich, et al. 'Patterns of Fatal Extreme-Right Crime in the United States', *Perspective on Terrorism*, 12(6), 2018, online.

[4] Valerie Caproni, General Counsel Federal Bureau of Investigation, 'Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security', Washington, D.C. 17 February 2011, online.

[5] Robert Graham, 'How terrorists use encryption', *CTC Sentinel*, 9(6) 2016, online.

a cryptographic key and even the company that created the software/platform does not have the 'key' serving only as an illiterate messenger. The system relies on two 'keys': a public key, which encrypts the message, and a private key composed mainly of extremely large prime numbers, which the software than multiplies to create the public key, which decrypt the message.[6]

The end-to-end encryption process is constantly evolving as seen for example with such applications as Signal, which are designed not to keep records of users' contacts, conversation lists, location, avatars, profile names, group memberships, group titles or private keys,[7] making it harder for security agencies to keep up with what is developed.

b. Full device (disk) encryption

Personal devices such as iPhones and Android phones are 'full device encryption' which means that everything on the device is encrypted.

Full device encryption can be achieved through software and hardware.

The challenge with full device encryption was brought to light with the iPhone of Syed Rizwan Farook, one of the individuals responsible for the 2 December 2015 San Bernardino terrorist attack in which 14 people were shot and killed. The FBI demanded that Apple assist it in cracking the PIN code. The matter ended up in court, which ruled in favour of the government, but ultimately, the FBI paid a third-party to get it to access to the iPhone.[8] It remains unknown whether gaining access to the iPhone has helped the FBI with its investigation, although what is known is that the FBI was able to acquire a technique to gain access to other iPhone 5C models running iOS 9.[9]

Notably, full disk encryption is also available on personal computers as seen with Microsoft Windows (BitLocker), Macintosh (FileVault) and Linux (LUKS). Additionally, many people also use a Trusted Platform Module, making access to hardware more challenging.

c. Anonymization

There is increasing evidence that individuals look for a way to engage online whilst ensuring that they leave no digital footprint. Through such browsers as **T**he **O**nion **R**outer (TOR), which could be used on Windows,

---

[6] Andy Greenberg, 'Hacker lexicon: What is end-to-end encryption?', *Wired*, 25 November 2014, online.

[7] LiamTung, 'Signal: we can't comply with Aussie encryption law even if we wanted to', *CSO*, 18 December 2018, online.

[8] Transcript of Argument Before the Honorable James Orenstein U.S. Magistrate Judge at 55–56, *In re: Order Requiring Apple, Inc. Assist in Execution of Search Warrant*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) (No. 1:15-mc-01902); Anusha Asif, *Apple vs. FBI: Encryption case timeline*', *Tech News Today.Com*, 19 February 2016, online; Alina Selyukh, 'The FBI has successfully unlocked the iPhone without Apple's help,' *NPR*, 28 March 2016, online.

[9] Mark Hosenball, 'FBI paid under $1 million to unlock San Bernardino iPhone: sources', *Reuters*, 29 April 2016, online.

Macintosh, and Linux computers, information is passed through many proxy servers, managed by different organisations.[10]

d. General Operations security (procedural security)

Many people are adopting general operation security (OpSec) methods to avoid detection. In engaging in OpSec an individual view their actions from the perspective of an adversary.

The first stage in any successful OpSec calls on one to identify one's sensitive data, which can range from the browser history, financial records, etc. all of which could be encrypted. Secondly, one must identify the threat that one faces which would determine the level of security that one should apply. Thirdly, OpSec calls on the individual to rank their vulnerabilities. A key assumption to any OpSec is the recognise that no system is 100% secure. A further component in OpSec is to implement countermeasures.

When looking at terrorist usage of OpSec, there is evidence that they use burner phones[11] and a host of messaging platforms such as Telegram, Wickr, Signal, et. al. that limit their digital footprint.[12]

e. User-Controlled Encryption

Law enforcement agencies around the world are recognising the growth in user-controlled encryption which refers to the system where the customer or the end-user has control over encrypt and decrypt information, thus facilitating the 'going dark' phenomenon. The growth in user-control encryption stems from the decline in the cost of computational encryption/decryption which used to be prohibitive.[13]

5. Notably, the idea that one can have off-the-shelf encryption technology available only to government and institutions of the state and consumers is a fallacy.[14] Individuals will pay to get the best form of security

The Disaggregate threat: violent extremists as an adaptable network

6. Terrorists and would-be terrorists have been using encryption to communicate and to survive.[15] From the early-to-mid 2000s, al-Qaeda has shown a commitment to invest in technology, creating a jihadi cloud to ensure that its

---

[10] Lee Mathews, 'What Tor is, and why you should use it to protect your privacy', *Forbes*, 27 January 2017, online.

[11] Rukmini Callimachi, Alissa J. Rubin, Laure Fourquet, 'A View of ISIS's evolution in new details of Paris attacks', *The New York Times*, 19 March 2016, online.

[12] Abu Sa'ad al-Sudani, known as Abu Isa al-Amriki was an ISIL virtual recruiter would instruct interested parties to connect with him via Telegram. One potential recruit was a young engineer named Mohammed Ibrahim Yazdani who was seeking to carry ISIL's first attack on Indian soil. Rukmini Callimachi, 'Not 'Lone Wolves' after all: How ISIS guides World's terror plots from afar', *The New York Times*, 4 February 2017, online.

[13] 'Likely future adoption of user-controlled encryption' *Encryption Working Group*, Carnegie Endowment for International Peace, April 2019, online; Jim Baker, Susan Landau, 'New perspectives on the future of encryption', *Lawfare*, 28 May 2019, online.

[14] See for example William Barr's speech to the International Conference on Cybersecurity in which he sought to distinguish between military-grade encryption and consumer encryption. Zack Whittaker, 'US attorney general William Barr says Americans should accept security risks of encryption backdoors', *TechCrunch*, 23 July 2019, online.

[15] For example, Khalid Masood who carried out the 22 March 2017 terrorist attack along Westminster Bridge and Parliament had used WhatsApp.

ideas will remain and spread. ISIL has also invested in technology and cyber using the *munasirun* (volunteer media operatives), which serve as amplifiers of official content, which is distribute through mainstream and boutique platforms.

7. Governments around the world have demanded that corporations that provide encryption install either 'backdoors'[16] or aid governments to gain access to an encrypted message(s). There is clearly a learning competition and an adaptability competition between terrorist groups and between terrorists and governments to see who can address changes faster. It is worth recalling that one of the key ideologues of the Salafi-jihadi movement and an associate of Ayman Al-Zawahiri, Sayyed Imam Al-Sharif (best known as Dr Fadl) pointed out in *The Obligation Of Holding Steadfast To The Book And The Sunnah* of the importance of learning from one's mistake so as to improve.[17]

8. It is also important to understand the nature of the threat which in the post-2018 period has become disaggregated as many of those seeking to employ or engage in violent extremism are no longer operating as part of coherent, organised, top-down unit, but rather as a network of individuals using the Swarmcast model (content is distributed mainly by a network as opposed to the original producer of the content[18]), multiplatform communication paradigm (MCP) and shortlinks.[19]

9. By adopting the Swarmcast/MCP/shortlinks methodology, violent extremists are able to avoid or make detection harder as they move away from operating in hubs and nods as savvy operators such as Samata Ullah, a British man who supported ISIL, Ullah who in 2017 was jailed for eight years, created a 'one-stop-shop' for would be terrorists from his bedroom in Cardiff. Ullah advised his followers not to store incriminating information on computers but use USB sticks. He created instructional videos on how to secure sensitive data, use TOR, etc. Ullah had taught himself. Cdr Dean Haydon, head of the Metropolitan police's SO15 counter-terrorism command had said in respect to Ullah,

> 'It is the first time we have seen anything on this scale. He had set up a self-help library for terrorists around the world and they were

[16] See, for example, Matthew Deluca, 'Draft encryption bill would mandate companies assist investigators', *NBC News*, 13 April 2016.

[17] 'Abdul-Qādir Ibn 'Abdil-'Azīz. *The Obligation of Holding Steadfast to the Book and The Sunnah* (The Manhaj Of Ahl As-Sunnah Wal-Jama'ah). Translated edition, al-Tibyan Publications, online; Ali Fisher, 'Netwar in Cyberia: Decoding the Media Mujahidin', *USC Center on Public Diplomacy*, Paper 5, 2018, online.

[18] Ronfeldt and Arquilla define swarming as 'is seemingly amorphous, but it is a deliberately structured, coordinated, strategic way to strike from all directions, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off positions. It will work best—perhaps it will only work—if it is designed mainly around the deployment of myriad, small, dispersed, networked maneuver units (what we call "pods" organized in "clusters").' John Arquilla, David Ronfeldt, *Swarming and the Future of Conflict*, Santa Monica, CA: RAND Corporation, 2000, p. vii.

[19] Ali Fisher, 'How Jihadist networks maintain a persistent online presence', *Perspectives on Terrorism*, 2015, 9(3): 4; Mustapha Ajbaili, 'How ISIS Conquered Social Media', *Al Arabiya*, 24 June 2014, online; Scott Shane, Ben Hubbard, 'ISIS displaying a deft command of varied media', *The New York Times*, 30 August 2014, online; Ali Fisher, Nico Prucha and Emily Winterbotham, 'Mapping the Jihadist information ecosystem towards the next generation of disruption capability', *RUSI*, Global Research Network on Terrorism and Technology: Paper No. 6, July 2019, online.

> using his library … He has accessed it online himself and compiled a lot of material and put it into his own library.'.[20]

10. It seems that the British police were able to arrest him due to a tip that they received from the FBI, who had received information from Kenyan authorities who had arrested a man communicating with Ullah.[21]

11. Entities such as ISIL have shown remarkable resilience and adaptability to effective counterterrorism measures. The horrific killing of Muath Safi Yousef al-Kasasbeh on 3 January 2015 led to a massive campaign by states and tech companies to limit ISIL's ability to use social media to proselytise and promote its brand. Within several months ISIL's presence on Twitter declined substantially (between June and October 2015, tweets per day per ISIL stood at around 14.5 per day, but by October 2015, it was down to 5.5).[22] Although ISIL doesn't have the same capacity nor volume of tweets, it continues to operate in the space by simply changing its method or simply creating new accounts.[23]

People use encryption because they want security and privacy

12. There evidence that distrust of government, big business, institutions, etc. is on the rise.[24] Many have pointed to the 2013 Edward Snowden revelation as serving to encourage the public to be wearier of the government surveillance.[25]

13. It is such concern, whether warranted or not, that is driving the encryption debate. People turn to encryption because they want to secure their private information and because they want greater privacy (or at least the ability to determine what is private or not to them).[26]

---

[20] Press Association, 'Cardiff terrorist who hid extremist data on Bond-style cufflink is jailed', *the Guardian*, 2 May 2017, online.

[21] ''Cufflink terrorist' Samata Ullah jailed for eight years', *BBC*, 2 May 2017, online.

[22] J.D Maddox, 'Lessons from the information war: applying effective technological solutions to the problems of online disinformation and propaganda', *GW Program on Extremism*, September 2019, online.

[23] Ben Makuch, 'Banning Islamic State Jihadists from Twitter is like playing whack-a-mole', *Vice*, 22 August 2014, online.

[24] Any Cheema, 'We don't trust the internet. And it's putting our digital future at risk', *World Economic Forum*, 13 April 2017, online; '2019 CIGI-Ipsos Global Survey on Internet Security and Trust', *Centre for International Governance Innovation*, 2019, online.

[25] Snowden was a former the defence contractor with Booz Allen Hamilton who working at the National Security Agency leaked to the media, details of mass Internet and phone surveillance by the U.S. National Security Agency (NSA). Snowden revealed that the US run a program, code named PRISM that involved support from several technology companies such as Yahoo!, Google, and Microsoft, that enabled the US government to collect information such as search history, the content of emails, file transfers and live chats. Glen Greenwald, 'Edward Snowden: the whistleblower behind the NSA surveillance revelations', *The Guardian*, 11 June 2013, online; Glen Greenwald, Ewen MacKaskill, 'NSA Prism program taps in to user data of Apple, Google and others', *The Guardian*, 7 June 2013, online.

[26] Article 12 of the Universal Declaration of Human Rights states 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.' UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), online.

a. It is worth noting that countries, institutions, people struggle with how to balance an individual's right to privacy and the security of the public.[27]

14. One of the major issues with the act was the speed in which it was introduced (the government introduced the bill 10 days after closing a public consultation), raising questions as to whether there was sufficient consultation and debate.[28] Moreover, it doesn't seem that the government reached out to minority communities to get their view on what the measure would entail or how such measures are perceived by these communities who already feel marginalised.[29]

Lack of public evidence that access to encrypted communication prevents terrorism

15. It is for the government to show that access to encrypted communication prevents terrorism. There is a body of academic literature suggesting that making social media platform hostile spaces for violent extremist is counterproductive. The argument appears in two forms

a. De-platforming

The increasing use by extremists to use social media and technology to promote their ideas, visions, messages has led to them being 'deplatformed' only for them to find or develop their own messaging platforms as seen with developers at Gab, an alt-right movement, which forked Mastodon, a free and open-source self-hosted social networking service. What the developers at Gab did is take the open-source code used by Mastodon to revamp Gab, making it into decentalised platform.[30]

b. Counterterrorism

There is some evidence to suggest that violent extremists that use the mainstream platforms and tools are more likely to come to the attention of the security services. In one study by START, US extremists that were active on mainstream social media were less likely to carry out successful attacks.[31] Paul Gill and Emily Corner looking at

---

[27] The case of Andreas Lubitz underlines how difficult is to balance the two in that Lubitz was a pilot with Germanwings. On 24 March 2015, Lubitz intentionally flew his plane into the French Alpes killing 150 passengers. Lubitz suffered from severe depression and he had seen 41 doctors in the previous five years. Privacy protections meant that he could hid his condition from his employers. 'Germanwings co-pilot Andreas Lubitz saw 41 doctors in five years; crash inquiry to consider possible manslaughter charges, prosecutor say', *ABC*, 12 June 2014, online; 'Germanwings crash: Who was co-pilot Andreas Lubitz?', *BBC*, 23 March 2017, online.

[28] Rohan Pearce, 'Alarm over government's encryption bill rush', *ComputerWorld*, 20 September 2019, online; Cynthia Wong, 'Turning our technology against us', *The Strategist*, 21 September 2018, online.

[29] Usha M. Rodrigues, 'New research shows how Australia's newsrooms are failing minority communities', *The Conversion*, 11 October 2018, online.

[30] Loránd Bodó, 'Decentralised terrorism: The next big step for the So-Called Islamic State (Is)?', *Vox*, 12 December 2018, online; 'Analysis: The use of open-source software by terrorists and violent extremists', *Tech against Terrorism*, 2 September 2019, online.

[31] 'The Use of Social Media by United States Extremists', *National Consortium for the Study of Terrorism and Responses to Terrorism*, July 2018, online.

extremists in the UK found that extremists that use the internet to plan their attacks were less likely to kill or injure.[32]

The Israelis have been especially apt as using predictive analytics to gather information from open sources in their assessment of potential terrorist attacks.[33]

16. The *Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2019* was billed as an integral component of Australia's counterterrorism regime. However, one wonders whether enough thought was placed on what to do with the collection of encrypted and decrypted messaging. Salafi-jihadi often market their messages in a careful, nuanced way requiring a deep understanding of Sunni extremist theology. For example, Ali Fisher looking at ISIL's Salil al-Sawarim (Clashing of Swords). The title draws influence from a book by Ibn Taymiyya, *al-Sarim al-maslul 'ala shatim al-rasul*, (The Sharp Sword on whoever Insults the Prophet). Fisher adds that this is why a sword being drawn from its scabbard appears in many of ISIL's videos.[34] Thus, collecting encrypted information but without analysing it through cultural, religious, political, regional lenses is counterproductive.[35]

    a. Its noteworthy that the Salafi-jihadi milieu is very diverse, composed of individuals from so many different backgrounds, which therefore mean that often messages will be sent in different languages. For example, in its heyday, ISIL would distribute its messages in more than 40 different languages.

17. In sum, it seems that the *Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018* came about because there was a recognition that the government and the agencies no longer had a technological edge over the private sector when it came to encryption.[36] However, what the measure doesn't take into consideration are the following

    a. The Salafi-jihadi milieu has drastically changed as is the threat perception;

---

[32] Paul Gill, Emily Corner 'Lone actor terrorist use of the Internet and behavioural correlates', Lee Jarvis, Stuart MacDonald, Thomas M. Chen (ed.) *Terrorism Online: Politics, Law and Technology*, Routledge, 2015, 47-65.

[33] Shoshanna Solomon, 'Israel cyber spying helped foil terror attacks in 'dozens' of countries, PM says', *The Times of Israel*, 26 June 2019, online; Isaac Kfir, 'Israel's approach to counterterrorism', *The Strategist*, 27 September 2018, online; Isaac Kfir, 'Learning from Israel's cyber playbook How the country became a force to be reckoned with in cyberspace', *Asia & The Pacific Policy Forum*, 5 November 2018, online.

[34] Ali Fisher, 'Netwar in Cyberia: Decoding the Media Mujahidin', *USC Center on Public Diplomacy*, Paper 5, 2018, online.

[35] For example, for al-Awlaki victory against the infidels will only take place when Muslims are able to practice their religion freely and properly. Anwar al-Awlaki, *44 Ways to Support Jihad*, Victorious

Media, undated, online.

[36] John Coyne, 'Encryption: the perils of 'going dark'', *The Strategist*, 22 August 2017, online; Andrew Davis, 'Going dark—strong encryption and security (part 1)', *The Strategist*, 19 June 2017, online; Andrew Davis, 'Not dark yet—strong encryption and security (part 2)', *The Strategist*, 27 June 2017, online.

b. Collecting data and not analysing it through appropriate cultural, religious, social, political and economic lens is redundant, wasteful and counterproductive;

c. Ordinary people increasingly use encryption to secure their information;

d. The cost of encryption has declined substantially which is why it is easy to acquire and use (encryption doesn't require or call on the user to have any technical skills) and it also why people would continue to use it.

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