CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

CSCRC SUBMISSION:
PJCIS Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

cybersecuritycrc.org.au

Dear Sir/Madam,

Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) response to the Parliamentary Joint Committee on Intelligence and Security's *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*. Given the significant and increasing challenges cyber-enabled crime presents to Australian law enforcement and intelligence agencies, review of the Bill is timely and pertinent.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem. The CSCRC has two research programs: Critical Infrastructure Security and Cyber Security as a Service.

The CSCRC is a public company limited by guarantee and will invest $AU50 million of Australian Commonwealth Government funding and additional Participant funding over seven years to 2025 in research outcomes related to our key impact areas. The CSCRC has 25 Participants including seven Research Providers, eight State and Federal Government Agencies/Departments and 10 Industry/SMEs.

We look forward to answering any queries about this submission and welcome the opportunity to participate in future discussions regarding this very important inquiry.

Yours Sincerely,

Rachael Falk
CEO, Cyber Security Cooperative Research Centre
ceo@cybersecuritycrc.org.au

Introduction

The internet and digital communications have changed the way we live, work and do business. Ours is an inter-connected world, with the digital revolution challenging traditional notions of borders and sovereignty and enabling the free flow of information with the click of a button.

While the internet and digital communications have undoubtedly improved many aspects of our lives, they are also used for nefarious purposes. In particular, the advent of the dark web, end-to-end encryption and other anonymising technologies have provided platforms via which paedophiles, terrorists, drug dealers and arms dealers can operate undetected and protected. This is not a problem that can be countered easily – but action must be taken.

If passed, the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (the Bill), will play a key role in countering serious cyber-enabled crime committed domestically and offshore. In particular, the introduction of account takeover warrants will mean authorities will no longer be required to ask serious criminals for permission to access online accounts, as is currently the case.

While the powers authorised under the Bill are undoubtedly extraordinary, the CSCRC submits they proportionate and appropriate in relation to the threat posed. Furthermore, to ensure such extraordinary powers are not misused, exploited or subject to 'legislative creep', the Bill contains a number of key safeguards and protections. It presents a clear opportunity for Australia to ensure domestic laws are properly aligned with digitally perpetrated activities, allowing lawful access to data and devices where it is appropriate to do so.

In this submission, the CSCRC provides an overview of the Bill, its key components, safeguards and oversight measures. In addition, an analysis of the dark web, end-to-end encryption and other anonymising technologies is provided and their utilisation by serious criminals is explored.

To this end, the CSCRC submits:

- The extraordinary powers enacted if the Bill is passed are both proportionate and appropriate to counter cyber-enabled crime;
- The safeguards within the Bill offer appropriate protection against misuse of powers and legislative creep;
- Steps could be taken to define and refine the crimes the warrants would apply to; and
- The Bill should be passed, with consideration of clearly defining what crimes the regime would apply to.

Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

The *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*[1] (the Bill) seeks to amend the *Surveillance Devices Act 2004*[2] (SD Act), the *Crimes Act 1914*[3] (Crimes Act) and other associated legislation to introduce new powers for the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to enhance the investigation and disruption of online crime.

The Bill introduces three new warrants:

- data disruption warrants;
- network activity warrants;
- account takeover warrants.

Data disruption warrants would permit the disruption of data through modification and deletion to frustrate the commission of serious offences.[4]

Network activity warrants would permit the collection of intelligence on serious criminal activity carried out by criminal networks operating online.[5]

Account takeover warrants would allow authorities to take control of a person's online account/s to gather evidence and to further a criminal investigation.[6]

Data disruption warrants

Data disruption warrants would be a covert power allowing the AFP and the ACIC to add, copy, delete or alter data to allow access to and disrupt relevant data in the course of an investigation.[7] Such action would be undertaken to frustrate the commission of an offence and, while not sought to gather evidence, information collected could be used as evidence in a prosecution.[8] As it would be a covert power, concealment of activities would be permitted. As noted in the Explanatory Memoranda (EM): "The purpose of the data disruption warrant is to offer an alternative action to the AFP and the ACIC, where the usual circumstances of investigation leading to prosecution are not necessarily the option guaranteeing the most effective outcome. For example, removing content or altering access to content (such as child exploitation material), could prevent the continuation of criminal

---

1 https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6623
2 https://www.legislation.gov.au/Details/C2016C00433
3 https://www.legislation.gov.au/Details/C2017C00297
4 https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/surveillance-legislation-amendment-identify-and-disrupt-bill-2020
5 Ibid 4
6 Ibid 4
7 https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6623_ems_cdf486bc-4c7c-475f-89cb-78af48798af8/upload_pdf/JC000627.pdf;fileType=application%2Fpdf P3
8 Ibid 7 P3

activity by participants, and be the safest and most expedient option where those participants are in unknown locations or acting under anonymous or false identities".[9]

The warrants would also be able to be used to disrupt data offshore with the consent of an appropriate consenting foreign official if the location of data is known or can be reasonably determined.

The threshold for application of a data disruption warrant stipulates that it must be suspected on reasonable grounds that:

- an offence is being, is about to be, or is likely to be committed;
- the offence involves data held on a computer; and
- disrupting the data is likely to substantially assist in frustrating the commission of an offence.[10]

An applicable offence must carry a minimum term of imprisonment of three years.[11]

Warrants would be issued by an eligible judge or nominated Administrative Appeal Tribunal (AAT) member, who must be satisfied it is justifiable and proportionate. In the event of an emergency, the warrants could also be issued internally and subsequently authorised by a judge or AAT member. Warrants would be valid for a maximum of 90 days, with extensions of up to 90 days available. The regime would be overseen by the Commonwealth Ombudsman, who would be required to report to the Minister for Home Affairs every six months.[12]

In addition, agencies would be required to report to the Minister for Home Affairs after each warrant is executed, with annual reports regarding the use of these warrants tabled in Federal Parliament.[13]

Network activity warrants

Network activity warrants would permit the AFP and the ACIC to collect intelligence on criminal networks operating online by gaining lawful access to the devices and networks used to facilitate criminal activity. Importantly, they would assist the AFP and the ACIC to more easily identify criminals using anonymising technologies, ultimately supporting the deployment of more targeted investigative powers.[14] The warrants would also help target

[9] Ibid 7 P3
[10] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/surveillance-legislation-amendment-identify-and-disrupt-bill-2020/data-disruption-warrants
[11] Ibid 10
[12] Ibid 10
[13] Ibid 10
[14] Ibid 4 P4

criminal networks about which little is known, for example, dark web paedophile rings, helping gauge the scope of activities and the identities of those involved.[15]

The warrants would allow the AFP and the ACIC to access data in computers and digital devices used, or likely to be used, by a criminal network over the life of the warrant. The data does not have to be stored on the devices, but can be temporarily linked, stored or transiting through them (for example, live streams).[16] As a result, data that is unknown or unknowable at the time of a warrant's issue could be discovered, including data on devices disconnected from the network once the criminal activity has occurred.[17] It is important to note information obtained under the warrants would be for intelligence purposes only and not permitted to be used as evidence in a criminal proceeding. Gathered intelligence could, however, be used to support an application for other warrants to collect evidence.[18] The warrants would be able to be used to disrupt data offshore with the consent of an appropriate consenting foreign official if the location of data is known or can be reasonably determined.

The threshold for application of a network activity warrant stipulates that it must be suspected on reasonable grounds that:

- a group of individuals is a criminal network of individuals;
- access to data held in a computer or digital device being used, or likely to be used from time to time by individuals in the group, will substantially assist in the collection of intelligence that relates to the group or its members; and
- the data is relevant to the prevention, detection, or frustration of one or more kinds of relevant offences.[19]

An applicable offence must carry a minimum term of imprisonment of three years.[20]

Warrants would be issued by an eligible judge or nominated AAT member, who must be satisfied there are reasonable grounds for suspicion regarding the likely intelligence value of any information obtained.[21] Warrants would be valid for a maximum of 90 days, with extensions of up to 90 days available. Oversight of the regime would be the responsibility of the Inspector-General of Intelligence and Security (IGIS), with the IGIS annual report to include comments on any inspection conducted. In addition, the IGIS would be permitted to request any relevant information that would assist in determining the legality of the

[15] Ibid 4 P4
[16] Ibid 4 P4
[17] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/surveillance-legislation-amendment-identify-and-disrupt-bill-2020/network-activity-warrants
[18] Ibid 17
[19] Ibid 17
[20] Ibid 17
[21] Ibid 17

warrants.[22] In addition, agencies would be required to report to the Minister for Home Affairs after each warrant is executed, with annual reports regarding the use of these warrants tabled in Federal Parliament.[23]

Account takeover warrants

Account takeover warrants, which would be inserted into the Crimes Act under the Bill, would enable the AFP and the ACIC to take control of a person's online account for the purposes of gathering evidence about serious offences.[24] This would facilitate covert and forced takeovers to add to authorities' investigative powers. As previously noted, take- over of a person's account can only currently occur with the person's consent.[25]

The warrant would enable taking control of a person's account and locking the person out of the account, with separate warrants or authorisations required for other activities like accessing data on the account, gathering evidence or performing undercover activities such as taking on a false identity.[26]

The threshold for application of an account takeover warrant stipulates that it must be suspected on reasonable grounds that:

- an offence has been, is being, is about to be, or is likely to be committed;
- an investigation into those offences is being, will be, or is likely to be, conducted; and
- taking control of one or more online accounts is necessary, in the course of that investigation, for the purpose of enabling evidence to be obtained of the commission of those offences.[27]

An applicable offence must carry a minimum term of imprisonment of three years.[28]

Warrants would be issued by a magistrate and the Commonwealth Ombudsman would have oversight of the regime, responsible for inspecting the records of agencies at least once every six months to determine compliance.[29] The warrants would also be permitted to be issued internally in an emergency situation, and subsequently authorised by a magistrate. Warrants would be valid for a maximum of 90 days, with extensions of up to 90 days available. The Ombudsman would be required to report to the Minister for Home Affairs on inspection results and would be permitted to request any relevant information

[22] Ibid 17
[23] Ibid 17
[24] Ibid 4 P5
[25] Ibid 4 P5
[26] Ibid 4 P6
[27] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/surveillance-legislation-amendment-identify-and-disrupt-bill-2020/account-takeover-warrants
[28] Ibid 27
[29] Ibid 27

from officers to help determine compliance.[30] In addition, agencies would also be required to provide bi-annual reports to the Minister for Home Affairs and the Commonwealth Ombudsman, with annual reports about the use of these warrants tabled in Parliament.[31]

Safeguards and oversight

The CSCRC submits that the safeguards in the Bill in relation to the issuance of warrants and oversight of the various types of warrants are sufficient. Australia is a proud democracy and a nation that strictly observes the rule of law and the principles of natural justice, which is reflected in the safeguards and oversight provisions of the Bill, as outlined above. In particular, the independent oversight of the Commonwealth Ombudsman and the IGIS serve to bolster the integrity of the proposed regime and instil confidence at the proportionate application of the extraordinary powers it entails.

The CSCRC notes the minimum term of imprisonment for which a warrant could be issued under the Bill is three years across all proposed warrants. Such a threshold is sufficiently high and is indicative of serious criminal offending. However, under the Crimes Act such a threshold does cover a wide range of offences, so consideration should be given within the legislation to clearly specify types of crime to which the mechanisms set out in the Bill could apply. For example, the Explanatory Memorandum makes note of "the most serious of crimes, including child abuse and exploitation, terrorism, the sale of illicit drugs, human trafficking, identity theft and fraud, assassinations and the distribution of weapons".[32] The CSCRC submits that if offences that would and would not be captured under the regime were clearly carved out it would serve to allay fears of misuse of the warrants for less serious crimes and perceptions of legislative creep.

Privacy

The CSCRC submits that an absolute right to privacy can never exist and there must always be exceptions, especially when it comes to maintaining the common good. This is a principle recognised in the International Convention of Civil and Political Rights, which makes explicit exceptions where privacy can be overridden, including for the protection of national security, public order, or of public health and morals.[33] There is no doubt that the criminal activities the Bill is designed to capture all fall under such an exception.

The CSCRC contends that while privacy is valuable it must have limitations and these limitations must correlate with the social contract all members of the community enter into, upon which modern democracies like Australia's are built. Social contract theory holds that

[30] Ibid 27
[31] Ibid 27
[32] Ibid 7 P2
[33] https://humanrights.gov.au/our-work/commission-general/international-covenant-civil-and-political-rights-human-rights-your

for society to function properly individuals must give up certain rights. This is a concept that can no longer simply be applied to the physical world – in 2021, it must also incorporate unacceptable behaviour that occurs in the digital domain.

Furthermore, as noted in the Explanatory Memorandum, while the Bill does place limitations on the right to privacy, such limitations are not arbitrary or unlawful. Rather, "they are carefully framed and considered in order to ensure public safety and a balanced approach to the intrusion on private individuals' data with the maximum safeguards".[34]

Criminal network of individuals

The CSCRC notes that the definition of a "criminal network of individuals", as defined in the Bill is fit-for-purpose, especially as it relates to dispersed groups of persons communicating online. It provides that a criminal network of individuals is a group of individuals who are linked electronically and that one or more individuals in the group must have engaged, is engaging, or is likely to engage in conduct that constitutes a relevant offence, or have facilitated, is facilitating, or is likely to facilitate, another person's engagement in conduct that constitutes a relevant offence.[35] As noted in the Explanatory Memorandum, "there is no requirement that every individual who is part of the criminal network is himself or herself committing, or intending to commit, a relevant offence … The word 'facilitating' is used to capture those individuals who are, knowingly or unknowingly, facilitating engagement by another person in conduct constituting a relevant offence."[36]

Importantly, the definition does not require individuals within the group to consider themselves members, or that the group is formalised sufficiently to form a membership base. This is especially relevant in relation to, for example, dark web paedophile groups, which may be dispersed all over the world with members that ensure their identities remain obscured at all times.

The dark web

The dark web is not like the surface web, the external interface of the internet most people are familiar with. And, while it does serve altruistic purposes, such as giving a voice to people living under oppressive regimes, the dark web is overwhelmingly a place of ill intent. It is part of the internet that evades indexing by search engines, instead requiring the use of an anonymising browser (like Tor) that routes traffic through multiple servers, encrypting it along the way. To help ensure anonymity, dark web browsers isolate sites to prevent tracing, automatically clear browsing history, prevent surveillance of connections, clone or dupe users' appearances to avoid fingerprinting and relay and encrypt traffic three times as

[34] Ibid 7 P24
[35] Ibid 1 P40
[36] Ibid 7 P67

it runs across the network. Because access to specific secret sites is required, criminals that use the dark web to plan their activities can hide these activities and work hard to ensure that their groups are not infiltrated by law enforcement. Hence, given the anonymity the dark web affords, it is unsurprising it has been exploited by a wide range of criminal actors.

In this section, the CSCRC provides case studies of dark web crime related to child sexual abuse, drug dealing and terrorism.

Child exploitation material

Over 12 months across 2019-20, the AFP's Australian Centre to Counter Child Exploitation (ACCCE) intercepted more than 250,000 child abuse material files online and 134 children – 67 in Australia – were removed from harm in the 2019-20 financial year.[37]

During the COVID-19 pandemic the ACCCE identified new users of dark web child exploitation sites seeking advice and guidance regarding avoiding detection by law enforcement. Concurrently, the sharing of child exploitation material uploads with the tag 'original content' increased substantially.[38]

In addition, the volume of livestreamed abuse increased, with AUSTRAC reporting a "three-fold" increase of suspicious financial transactions indicating payment for such content in 2019-20.[39]

Case study: Shannon McCoole

In 2015, former Families South Australia carer Shannon Grant McCoole was sentenced to 35 years' jail for his role as leader of a worldwide dark web child pornography ring, which had more than 45,000 members, and for abusing at least seven children in his care.

The website required members to post new child exploitation material every 30 days in order to retain membership, utilising TOR computer software to mask their identity.

Membership came with designated access to different areas of the forum, access to the rules of membership and technical forums directed towards encryption, software and internet safety advice. Members also had access on private areas where there was discussion surrounding the sexual abuse of children and 'rare content'. In addition, members could become special VIPs, honorary members or Private Zone members.

In 2014, authorities became aware the head administrator of the site was an Australian , most likely located in Adelaide. After painstaking police work, McCoole was located after an

[37] https://www.accce.gov.au/news-and-media/releases/2020/operationmolto
[38] Parliamentary Joint Committee on Law Enforcement, *Inquiry into criminal activity and law enforcement during the COVID-19 pandemic*, AFP submission, P4
[39] https://www.austrac.gov.au/sites/default/files/2020-10/AUSTRAC_Annual%20Report%202019_2020.pdf, P178

investigator matched his online vernacular and a freckle on his hand (as seen in dark web CEM content he had posted) to public posts he had made.

McCoole signed over his online identities to police. However, if he had not agreed to this, police would have been unable to lawfully access his accounts. Ultimately, the take-over of McCoole's accounts led to multiple arrests in Australia and overseas and the dismantling of the site. Such a case highlights how network activity warrants and account takeover warrants could be used in a highly targeted way to detect and apprehend such offenders more quickly and efficiently.[40]

Drug dealing

The dark web offers a platform for criminals to buy and sell drugs globally.

One of the most notorious dark web drug sites, The Silk Road (which was moderated by an Australian), was shut down by authorities in 2014 following an undercover operation by the FBI and Europol, whereby officers monitored and engaged with market users. This allowed law enforcement to communicate online and establish trust with the organiser of The Silk Road, who unintentionally gave the officers resources and information that allowed them to target the platforms in The Silk Road that facilitated criminal activity. Undercover agents were able to monitor the market, track user activity and introduce malware which altered the market's operational dynamics. This ultimately allowed law enforcement to seize and shut down The Silk Road.

Since then, a number of other dark web drug bazaars have opened and similarly shut down, including AlphaBay, WallStreet and Valhalla. However, given the clandestine and highly fluid nature of the dark web, as soon as one site is shut down it is quickly replaced with another.

Case study: Cody Ronald Ward

In November 2020, Cody Ronald Ward pleaded guilty to multiple drug offences for his role as the mastermind behind a large-scale dark web drug bazaar, which traded an estimated $17AUD million in drugs. He operated the marketplace for about four years from a small town on the NSW south coast.

In 2019, NSW acting assistant police commissioner Stuart Smith described the operation to unravel Ward's drug marketplace as the "largest penetration of the dark web in Australia".

"He used techniques to prohibit surveillance being conducted on him," Mr Smith said.

"We needed to move up a whole new gear to take this guy on. He learned his skill as a youth and now is a highly capable individual using very complex systems often used by government agencies."

[40] https://www.cdpp.gov.au/news/record-sentence-head-administrator-paedophile-site

Ward will be sentenced in February 2021.[41]

Terrorism

The dark web has been exploited by Salafi-Jihadists and right-wing extremists (RWE) for the dissemination of propaganda, fundraising through cryptocurrencies and the buying and selling of weapons and other illicit goods.[42]

For example, in August 2015, the Islamic State of Iraq and Levant published a 15-page 'how-to guide' in its French online magazine Dar al-Islam, highlighting the importance of secure communications and instructing users how to connect to the Tor network to hide internet addresses and locations, encrypt emails, and perform other obfuscating functions.[43]

The Christchurch terrorist, Brenton Tarrant, told authorities he had accessed the dark web to make purchases and used Virtual Private Networks (VPNs) when travelling and was familiar with Tor browsers.[44]

The dark web and terrorism
• After the 2015 Paris attacks, ISIL announced its Isdarat website, a propaganda archive, would be moved to the dark web due to increasing pressure on surface web sites.
• It is believed the guns used for the 2015 Paris attack were bought on the dark web from a German vendor, DW Guns.
• In June 2017, the UN's disarmament chief warned that terrorists and non-state actors were using the dark web to seek tools to make and deliver weapons of mass destruction.

Source: The Evolution of the Salafi-Jihadist Threat, P 40

Encrypted platforms

Encryption is the conversion of information or data into unintelligible code, which prevents unauthorised access. While it provides a key role in keeping personal and valuable information protected, it is also widely used by criminals to cloak their illicit activities. Encryption makes it difficult for law enforcement to intercept and read messages criminals send each other and to trace cryptocurrency increasingly used to fund criminal enterprise.

[41] https://www.news.com.au/national/nsw-act/courts-law/social-outcast-behind-17-million-dark-web-drug-syndicate/news-story/43c55bb76ac9c52fd46ce421528bbe04
[42] https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181221_EvolvingTerroristThreat.pdf P39
[43] Ibid 42 P58
[44] https://christchurchattack.royalcommission.nz/the-report/download-report/download-the-report/ P193

End-to-end encryption provides a form of communication protection that prevents third parties – including internet service providers, app hosts and law enforcement – from accessing data transferred from one system or device to another. This means data is encrypted on one system or device and only the recipient (who receives the communication) can decrypt it.

Encrypted instant messaging apps use end-to-end encryption to ensure only the person you send messages to is able to read them. Encryption software built into these apps means a third-party intercepting the messages cannot read them, as they will be indecipherable. These services operate 'over the top' of traditional telephony networks, which means it is impossible to know when they are even being used. Examples of well-known encrypted instant messaging apps include Telegram and WhatsApp. Facebook Messenger is not currently encrypted by default, but this feature can be enabled. There is also a high risk that if, as planned, Facebook adopts end-to-end encryption across its services, it will act as a new forum through which extremists can conceal their communications and activities.

Such concerns have been raised by Department of Home Affairs Secretary, Mike Pezzullo, who told a Senate Estimates hearing in 2020 that: "We are particularly concerned about Facebook's plans to go to end-to-end encryption of their entire platform to create, in effect, the world's biggest dark web".[45]

The significant challenge encrypted communications pose to law enforcement and intelligence agencies was made explicitly clear by the Director-General of Security, Mike Burgess, at the PJCIS review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* in August 2020. Mr Burgess told the committee: "It is no exaggeration to say that almost all communications of investigative value would be difficult or impossible to access in an intelligible form without lawful access tools such as those available under the Assistance and Access Act. Encrypted communications damage intelligence coverage in nine out of 10 priority counter terrorism cases".[46]

A high-level (and non-exhaustive) desktop review undertaken by the CSCRC for the purpose of this inquiry indicates that on the Australian Legal Information Institute's database, there were 33 criminal matters since November 2020 to February 2021 involving the key words 'encryption', 'Telegram' and 'WhatsApp'.

45 https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/estimate/e8aaf825-4319-4704-8bb7-b2878b2f3ee7/&sid=0000
46 https://www.asio.gov.au/publications/speeches-and-statements/director-general-opening-statement-pjcis-august-2020.html

Telegram and other encrypted messaging apps

Telegram and WhatsApp remain the "platforms of choice" for many criminals.[47]

In addition to end-to-end encryption, Telegram offers a suite of features that make it attractive to criminals, allowing multiple levels of communications, from private to public, via one platform, and even features a self-destruct timer that allows messages to permanently disappear after a stipulated period.[48] While some of Telegram's policies have changed and its operators have begun to collaborate (to an extent) with law enforcement,[49] it is unlikely criminals will migrate from the platform in the foreseeable future given its features, familiarity and ease of use.

Other encrypted messaging apps used by criminals include Surespot, Signal, Wickr, Kik, ChatSecure, BCM, Gab Chat, Hoop Messenger, Riot.im, Rocket.Chat and TamTam.[50]

Case study: The murder of Curtis Cheng

The terror cell responsible for plotting and carrying out the murder of Sydney accountant Curtis Cheng in October 2015 used WhatsApp to communicate in relation to the crime. The group – known as The Bricks Forum – were all under heavy counter-terrorism surveillance, including phone taps, at the time.[51]

For them, WhatsApp offered a cloak of secrecy, a way to evade authorities. While intelligence operatives could piece together some parts of the puzzle, vital pieces were missing. This was because authorities did not have the powers necessary to access these encrypted communications.

In addition, a member of the forum, Omarjan Azari, used Telegram to communicate with Australian foreign fighter and ISIL recruiter, Ali Baryalei. Azari is currently serving an 18-year sentence for his plan, hatched by Baryalei, to behead up to seven random Australians a month.[52] In planning for the commission of these crimes, Azari often exchanged messages with Baryalei. One such message tendered as evidence at Azari's trial for terror offences read: "Listen, it's gonna be like this. I need you first of all to get a telephone and on that telephone I need you to get Telegram … We're gonna speak, we're gonna speak through Telegram, Allah willing, because Telegram, apparently, praise be to Allah, is very good…"[53]

---

[47] https://gnet-research.org/wp-content/uploads/2020/11/GNET-Report-Migration-Moments-Extremist-Adoption-of-Text%E2%80%91Based-Instant-Messaging-Applications_V2.pdf P1
[48] Ibid 47 P33
[49] Ibid 22 P5
[50] Ibid 22 P1
[51] R v Alou (No. 4) [2018] NSWSC 221 (1 March 2018) (austlii.edu.au)
[52] Omarjan Azari sentenced to 18 years' jail over plan to behead Australians - ABC News
[53] R v Azari (No 12) [2019] NSWSC 314

Case study: CDPP v CCQ (Pseudonym)

In 2019, CCQ, aged 41, had his sentence increased to 16 years' jail on appeal for the transmission and possession of thousands of files containing the most extreme and disturbing level of child exploitation material (CEM).[54] Between 1 January 2016 and 18 November 2017 CCQ used a number of messaging and social media applications including Telegram and Kik to transmit, solicit, access and cause to be transmitted to himself, child abuse material, and in that period he possessed a quantity of child abuse material on electronic devices or online accounts.

The offences were committed for sexual gratification. CCQ's self-professed sexual interest was in the abuse, exploitation and degradation of very young children, particularly babies and toddlers. The material showed very young children, including newborn babies and toddlers, subjected to acts of rape, incest, bestiality and extreme cruelty. The nature of his proclivities was indicated by his responses to various online persons, as being interested in "0 to five" and "I love baby and brutal".

In November 2017 police executed a search warrant at CCQ's home. Initially he told police he had nothing to declare. While providing passwords for his online accounts in compliance with a court order, when questioned by police, he denied ever using the application Kik or having ever exchanged images of children using social media accounts. Even when police found child abuse material on SD cards at his residence, CCQ initially continued to deny any knowledge, telling police "I've told you as much as I know". Ultimately, however, the CCQ made admissions to accessing and possessing CEM.

Between 1 January 2016 and 18 November 2017 CCQ accessed a substantial amount of CEM over the internet, including as many as 5,646 CEM files from Telegram.

Future developments

As law enforcement agencies in Australia and around the world continue to grapple with the challenges posed by the dark web and deep encryption, there is no doubt criminals will continue to seek new ways to avoid detection.

It has been predicted by some that the 'decentralised web' will become a new way for criminals to communicate and evade authorities.[55] This would in effect mean criminals would be able to store data and communicate via their own servers, mitigating the effect(s) of content takedown by creating an independent, decentralised storage network outside the grasp of service providers and law enforcement.[56]

---

[54] Commonwealth Director of Public Prosecutions v CCQ [2021] QCA 4 (22 January 2021) (austlii.edu.au)
[55] Ibid 47 P23
[56] Ibid 47 P23

There is also a likelihood criminal groups could move to encrypted platforms produced outside the West, in less stringently governed states.[57] To this end, it is also likely such groups will move to build their own encrypted platforms or purchase already developed platforms from the dark web.[58]

Case study: Phantom Secure

In 2018 Phantom Secure, a company selling modified BlackBerry mobile phones that operated on a discrete encrypted network, was shut down. The phones were impervious to decryption, wiretapping or legal third-party records requests, and were snapped up by criminal enterprises around the world, including in Australia where Hells Angels bikies used the phones to coordinate several murders.[59]

Phantom Secure's services were located in Panama and Hong Kong, used virtual proxy servers to disguise their physical location, and remotely deleted or 'wiped' devices seized by law enforcement.

By the time the operation was shut down, the FBI estimated there were about 20,000 phones in use globally, with most users "top-level leaders of transnational criminal organisations".[60]

However, the resulting gap in the market has since been filled with a range of other platforms designed to prevent law enforcement surveillance. For example, in June 2020, EncroChat was shut down in the UK. It was a bespoke encrypted communication service providing a secure mobile phone instant messaging service, used exclusively by criminals to coordinate and plan.[61]

[57] Ibid 47 P37
[58] Ibid 47 P37
[59] https://www.unodc.org/unodc/en/untoc20/truecrimestories/phantom-secure.html
[60] https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181221_EvolvingTerroristThreat.pdf, P36
[61] https://www.vice.com/en/article/3aza95/how-police-took-over-encrochat-hacked