Australian Government
Department of Home Affairs

Home Affairs Portfolio submission to the review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

Parliamentary Joint Committee on Intelligence and Security

12 February 2021

Table of Contents

Introduction 4

Background 5

The threat environment 5

What is the dark web? 5

Overview – Australia's current electronic surveillance and investigatory powers framework 6

The *Surveillance Devices Act 2004* 6

The *Crimes Act 1914* 7

The need for reform 8

New powers for the AFP and the ACIC to combat cyber-enabled crime 8

Disruption to frustrate criminal offending 9

Criminal intelligence collection via computer access 9

Account takeovers for evidentiary purposes 10

Comprehensive Review of the Legal Framework of the National Intelligence Community Legislation (Richardson Review) 11

Overview of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 12

Summary 12

Data disruption warrants – Schedule 1 12

Purpose and overview 12

Network activity warrants – Schedule 2 14

Purpose and overview 14

Account takeover warrants – Schedule 3 16

Purpose and overview 16

Amendments to the controlled operation framework – Schedule 4 17

Use of powers to deliver enhanced law enforcement outcomes 17

Key elements of the Bill 18

Strict thresholds for application 18

Independent scrutiny and issuing criteria 20

Authorisations for emergency situations 22

Extraterritorial application of the new powers 22

Ability to seek assistance from persons with knowledge 23

Safeguards and limitations 23

Judicial review is available 23

Revocation and discontinuance requirements apply 24

Limits on interception and surveillance 24

Limits on interference and causing loss or damage 24

Restoration of access to online account 25

Information security 25

Use and disclosure 25

Record-keeping and destruction requirements 26

Protection of sensitive capability and methodology 26

Accountability and transparency 26
Reporting 26
Oversight 26
Impact on industry 27
Industry assistance 27
Conclusion 28

Introduction

1. The Home Affairs Portfolio welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security's (the Committee) review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (the Bill). This submission is made on behalf of the Department of Home Affairs, the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC). This submission provides an outline of the Bill and the policy challenges underpinning this legislative reform. This submission has been made at the request of the Committee. In addition to this submission, the AFP is separately preparing a submission providing additional operational context for the Committee's consideration. It is recommended that these submissions be read in conjunction with one another.

2. The Bill modernises Australia's law enforcement and intelligence legal framework to better equip the AFP and the ACIC to deal with serious cyber-enabled crime in the digital era. A particular focus of the Bill is addressing the challenges posed by the increasing criminal use of the dark web and anonymising technologies. The measures in the Bill are based on the following key principles:

    a. Law enforcement agencies should be provided with the ability to protect Australians online, just as they do in the physical world.

    b. Laws must keep pace with advances in technology if our agencies are to remain effective in combatting cyber-enabled crime.

    c. Investigations into online criminality must adapt if our agencies are to be depended upon to keep Australians safe now and into the future.

3. Criminals are using the dark web to commit serious crimes, including buying and selling stolen identities, trading in illicit commodities and producing and disseminating child abuse material. The encryption underpinning the dark web, and the increased use of anonymising technologies allow criminals, including terrorists and other malicious actors to hide from law enforcement. This has made committing serious crimes at volume and across borders easier than ever before.

4. Current electronic surveillance powers, while essential for investigating many aspects of online criminality, are not suitably adapted to identifying and disrupting serious crime where anonymising technologies are being used – including at scale – to conceal the identities and illegal activities of offenders. The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (**Assistance and Access Act**) was enacted as one legislative response to address challenges that technologies like encryption pose to law enforcement. While the powers introduced by that Act have significantly assisted Australia's law enforcement, security and intelligence agencies to tackle online criminal threats, more must be done to provide the AFP and the ACIC with effective powers of response in the fight against cyber-enabled crime.

5. This Bill addresses gaps in the current suite of electronic surveillance powers to enable the AFP and the ACIC to discover, target, investigate and disrupt the most serious of crimes, including child abuse, terrorism, and drug and firearms trafficking. The Bill is one part of the Australian Government's response to counter online criminality, including on the dark web, as highlighted in Australia's Cyber Security Strategy 2020 (the Strategy).[1] The Bill supports the objectives of the Strategy by establishing a robust and durable framework for law enforcement to respond to the challenges posed by anonymising technologies and cyber-enabled crime. This supports the Australian Government's vision of a more secure online world for Australians, their businesses and the essential services upon which we all depend.

6. Throughout the development of the Bill, the Department of Home Affairs worked closely with the AFP and the ACIC to ensure that the measures are responsive to these agencies' needs in the rapidly evolving modern communications environment. Noting the important roles of the Commonwealth Ombudsman (Ombudsman) and the Inspector-General of Intelligence and Security (IGIS), the Department consulted these entities to ensure that the new measures are supported by strong

[1] The Australian Government (2020), *Australia's Cyber Security Strategy 2020*, Commonwealth of Australia, p. 40

safeguards and oversight mechanisms. Engagement with the Department of Infrastructure, Transport, Regional Development and Communications and the Attorney-General's Department was valuable in ensuring that the Bill strikes an appropriate balance between the impact on Australians' privacy and civil liberties and the operational requirements of our agencies.

Background

The threat environment

7. Increasingly, criminal activity is assisted by advances in technology and a greater community reliance on digital platforms. The evolving online environment provides criminals with new avenues to commit serious crimes, including terrorism, firearms and drug trafficking, human trafficking and child sexual abuse. Australia continues to be an attractive and vulnerable target for both organised crime and individuals committing serious crimes online, due to our nation's relative wealth and high uptake of new and emerging technology.

8. The significant and ongoing challenges facing Australian agencies due to criminal activity 'going dark' was identified by Dennis Richardson AC in the Comprehensive review of the legal framework of the National Intelligence Community (Richardson review). In particular, the review noted:

> Over the past two decades there has been a rapid uptake of internet-based communications platforms, including social media, messaging and voice over internet protocol services. Internet-based communications pose considerable challenges to intelligence and law enforcement agencies, including by:
>
> - providing users with more anonymity, and
> - enabling users to communicate using platforms based outside of Australia's jurisdiction – that is, offshore.[2]

9. New and emerging technology continues to change the landscape in which criminals operate by providing new opportunities for countering law enforcement efforts, in particular by disguising activity and hiding identities. Technology that enables people to be anonymous online, whilst having legitimate uses, is increasingly used by criminals so that they can remain invisible to law enforcement. Often these technologies are cheap, commercially available and require little technical expertise, allowing the scale and sophistication of cyber-enabled crime to grow. The use of the dark web and anonymising technologies (such as bespoke encrypted devices) has made it easier than ever before for criminals to commit serious crimes at volume and across multiple jurisdictions. This has significantly degraded law enforcement agencies' ability to access communications, gather evidence, prevent crimes and conduct investigations.

10. This threat has only increased during the COVID-19 pandemic. In the past 12 months, we have seen opportunistic cyber criminals quickly adapting their methods to take advantage of more Australians working, studying and communicating online. These criminals are also hiding on the dark web to traffic drugs and other illicit goods, share abhorrent images of child abuse and undertake other insidious activities. The Australian Centre to Counter Child Exploitation (ACCCE) identified a 163 per cent increase in child abuse activity on the dark web between April and June 2020 compared with the same period in 2019. However, the true picture is difficult to estimate.

11. The problem is not just on the dark web. Although the dark web creates particular challenges for law enforcement officers, the surface web also enables the threat, not least because of the sheer number of Australians who use the internet. Criminals can exploit commonly used communication methods, such as social media platforms, for their own use.

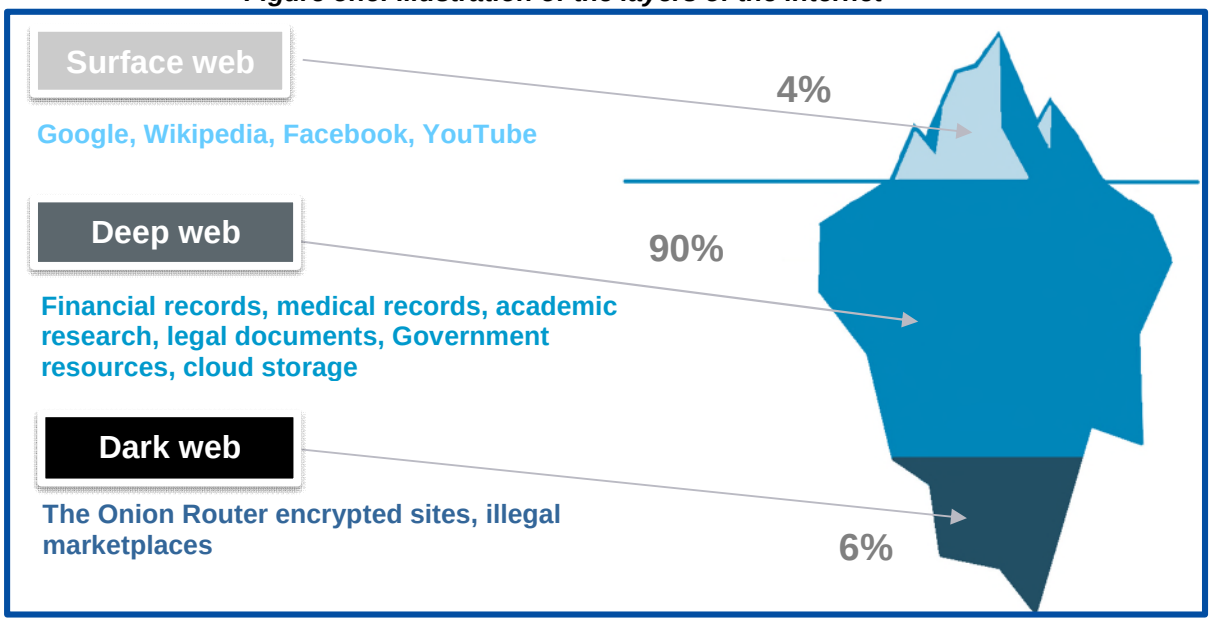
What is the dark web?

12. The dark web is a hidden part of the internet that is only accessible by specialised software or authorisation. The dark web forms part of the much larger deep web, which is the part of the internet not indexed by web search engines. The deep web has many legitimate uses such as web mail, online banking, private social media pages and closed web forums. Separate to the deep web is the surface

[2] Mr Dennis Richardson AC (2020), *Comprehensive review of the legal framework governing the National Intelligence Community*, volume 1, p. 204, para 9.25

web or 'clear net' which hosts content accessible to all users of the internet (such as Google, Wikipedia, Facebook and YouTube).

Figure one: Illustration of the layers of the internet[3]



13. On the dark web, users can communicate and conduct business anonymously without revealing information about their identity or location. The dark nets which constitute the dark web include both small peer-to-peer networks as well as large networks operated by individuals or public organisations, such as 'The Onion Router' (Tor). Dark net markets are able to circumvent law enforcement capabilities and intervention with layers of encryption and digital subterfuge, posing a resilient threat to safety and security all over the world.

14. As discussed above, while criminals are notorious for operating on the dark web, serious criminal activity occurs on the surface web and the deep web as well, including at scale and using technology that obfuscates the identity of offenders. The Bill is technology-neutral in this regard. Agencies will be able to target serious criminal activity wherever it is occurring online and access the necessary information, where technically possible within their capabilities, on platforms on the surface web, the deep web or the dark web. This approach reflects the technical reality of law enforcement's tools, and the reality of where serious criminal activity is occurring.

Overview – Australia's current electronic surveillance and investigatory powers framework

The *Surveillance Devices Act 2004*

15. The *Surveillance Devices Act 2004* (**SD Act**) governs the use of surveillance devices by agencies, including state and territory law enforcement agencies when using surveillance devices under Commonwealth law, or when investigating State offences that have a federal aspect. There are 17 agencies that have powers under the SD Act, including the AFP, the ACIC, the Australian Commission for Law Enforcement Integrity (ACLEI), the police forces of the States and Territories, and the integrity bodies of the States and Territories. The Australian Security Intelligence Organisation's (ASIO) use of surveillance devices is governed by the *Australian Security Intelligence Organisation Act 1979* (**ASIO Act**).

[3] Mr Soumick Chatterjee and Mr Asoke Nath (2017), 'Auto-Explore the Web – Web Crawler' in *International Journal of Innovative Research in Computer and Communication Engineering* Vol: 5, p. 6614

16. The SD Act allows agencies to access content directly from a device, rather than from a telecommunications service. Unlike the *Telecommunications (Interception and Access) Act 1979* (**TIA Act**), the SD framework is not predicated on assistance from the telecommunications industry. As criminals increasingly avail themselves to technologies which hide their activities, the device-based warrant powers in the SD Act are critical for enabling agencies to uncover serious criminality.

17. The SD Act provides for multiple forms of surveillance, all of which are currently available to the 17 agencies under the Act. Data surveillance devices monitor the inputs and outputs of computers. Listening devices are used to listen to and record conversations. Optical surveillance devices record and observe activities. Tracking devices are used to locate or track a person or object. Most recently, the Assistance and Access Act inserted computer access warrants into the SD Act, which allow agencies to remotely and covertly search devices, going beyond what is allowed under a data surveillance device warrant, that is, the monitoring of inputs and outputs. The SD Act also allows agencies to obtain warrants to retrieve devices covertly, and provides for circumstances in which surveillance and access to computers needs to be conducted in emergency situations.

18. Introducing computer access warrants into the SD Act was a crucial step in ensuring that agencies can meet the challenges posed by encryption. The Assistance and Access package as a whole was aimed at modernising the electronic surveillance framework underpinned by the TIA Act, the SD Act and the *Crimes Act 1914* (**Crimes Act**), in particular, to provide agencies with tools to overcome technological obstacles to investigations into serious crimes. The application of computer access warrants (available to ASIO since 1999 under section 25A of the ASIO Act) to law enforcement agencies now allows access to data held on a device, directly from that device.

19. The powers available to law enforcement in the SD Act enable the gathering of evidence to support investigations into serious crimes. To apply for an SD Act warrant in an offence investigation, there must be reasonable grounds to suspect that an offence (generally attracting a penalty of three years' imprisonment or more) has been, or will be, committed and investigated and the surveillance activity is necessary in the course of that investigation for enabling evidence to be obtained. There are strict protections on the use and disclosure of information collected under SD Act powers. It is an offence to use information except in limited circumstances such as for the purposes of an investigation of a relevant offence or making a decision about whether or not to bring a prosecution. Information collected under an SD Act power may be used in evidence in a relevant proceeding. The SD Act also imposes requirements for the secure storage and destruction of records, the making of reports, and inspections by the Commonwealth Ombudsman.

The *Crimes Act 1914*

20. The Crimes Act is a key piece of Commonwealth legislation dealing with federal crimes in Australia. The search warrant framework in the Crimes Act allows law enforcement to conduct searches of premises or persons and to seize property. These are overt evidence-gathering powers, and include the ability to search devices remotely and seize devices in order to collect evidence about serious crimes. Law enforcement also have the ability to compel persons with relevant knowledge to assist in accessing electronic evidence under a search warrant (for example, by providing a password to assist in accessing a computer). There are strict penalties for non-compliance with such an order. Information compelled under an assistance order can only be used in conjunction with a search warrant, including to enable access to data held on a seized device, and cannot be used for broader investigatory purposes, such as using a password to take control of a person's online account without the person's consent.

21. The Crimes Act also provides the ability for the AFP, the ACIC and the ACLEI to investigate serious crime covertly through an undercover operation. The controlled operations framework permits law enforcement agencies to undertake covert activity which would, apart from legislation, constitute an offence. The framework allows law enforcement to use covert activity to uncover, interdict and dismantle criminal activity occurring both online and in the physical world. However, controlled operations must be conducted in a way that ensures that, to the maximum extent possible, any illicit goods (including illegal content such as child exploitation material) will be under the control of law enforcement at the end of the operation. This does not acknowledge how easy electronic data is to copy and disseminate, and that there may be a limited guarantee that all illicit electronic goods will be under law enforcement's control at the end of a controlled operation conducted online.

The need for reform

22. Existing law enforcement powers in the electronic surveillance framework are designed to assist in gathering evidence of the commission of criminal offences, to lead to the prosecution of offenders. This is in line with policing agencies' longstanding roles and responsibilities. However, those roles and responsibilities must evolve as agencies respond to how criminals operate in the modern environment. This is especially pronounced where offenders are actively seeking to obfuscate their identities and activities through the use of the dark web or anonymising technologies. To keep pace with changes in technology, agencies tools and capabilities must be complemented by legislation if they are to remain effective in the fight against cybercrime.

23. As noted in the Richardson review:

> Cybercrime is the fastest-growing class of criminal activity, as sophisticated criminal organisations take advantage of the borderless and anonymous nature of the internet. There is obviously a need for an agency to have the skills and capability to tackle cybercrime, especially when it goes 'dark'.[4]

24. Just as law enforcement agencies use their full suite of methodologies to investigate, disrupt and protect against crime occurring in the physical world, our agencies also need these options online. Otherwise, law enforcement will be left behind in the fight against serious cyber-enabled crime. Law enforcement agencies have strong tools and capabilities at their disposal, as well as cooperative networks across the Commonwealth. They must be provided with a broader legislative and operational remit to use those tools and adequately and proactively respond to the challenges posed by anonymising technologies and cybercrime.

New powers for the AFP and the ACIC to combat cyber-enabled crime

25. The Bill responds directly to these challenges by strengthening the capacity of Australia's leading federal law enforcement and criminal intelligence agencies — the AFP and the ACIC — to discover, target, investigate and disrupt the most serious cyber-enabled crime.

26. A central role of the AFP is to enforce Commonwealth criminal law, contribute to combatting complex, transnational, serious and organised crime impacting Australia's national security, and protect Commonwealth interests from criminal activity in Australia and overseas. This includes the prevention of crime and the protection of persons from injury or death, and property from damage. The AFP has an existing intelligence function which supports operations through the production and provision of criminal intelligence for use in support of operations and investigations. The AFP's criminal intelligence functions are underpinned by the Australian Criminal Intelligence Management Strategy.

27. One of the ACIC's central roles is to protect Australia from criminal threats through collecting, assessing and disseminating criminal intelligence and policing information. The ACIC's coercive powers, and other special collection strategies, allow the agency to inform and contribute to national strategies to combat serious and organised crime, cybercrime and national security threats.

28. To fulfil these functions, the powers and capabilities of the AFP and the ACIC must keep pace with technological trends to ensure that these agencies maintain an edge in tackling serious cyber-enabled crime. The operational expertise of the AFP and the ACIC, and the existing technical and analytical tools at their disposal, mean that these agencies are well-placed to ensure strong law enforcement outcomes to protect Australians online against criminals and nefarious actors, as they do in the physical world. Enhancing the ability of the AFP and the ACIC to collect intelligence, investigate and disrupt criminal activity is a priority in ensuring that these agencies can effectively respond to the challenges posed by anonymising technologies and cyber-enabled crime.

29. The central purpose of the Bill is to provide the AFP and the ACIC with the powers they need to continue enforcing the criminal law and protecting the Australian community. The Bill's disruption, intelligence collection and account takeover powers will complement the AFP and the ACIC's existing powers by

[4] Mr Dennis Richardson AC (2020), *Comprehensive review of the legal framework governing the National Intelligence Community*, volume 1, p. 204, para 3.81

providing new avenues to gather information and respond to serious online crime. The measures in the Bill are grounded in the principle that the powers granted by Parliament to the agencies charged with enforcing the criminal law should not be nullified by advances in technology. The Bill is designed to provide the AFP and the ACIC with the enhanced ability to protect the Australian community from harms online, as these agencies protect the community in the physical world.

Disruption to frustrate criminal offending

30. Investigations into cyber-enabled crime are often lengthy and complex due to the internet's ability to anonymise users and remove the geographical barriers to communication. Criminals operating online, particularly those on the dark web or using anonymising technologies, are often unknown or inaccessible. There may also be too many suspected (but not immediately identifiable) offenders for law enforcement to feasibly pursue through ongoing investigation or prosecution. Targets may also be located offshore or their jurisdiction may be unknown, further complicating law enforcement's response.

31. As described above, traditional law enforcement powers have been framed by reference to action that is primarily focused on the gathering of evidence for use in a criminal prosecution. The availability of these existing powers presupposes a particular outcome of law enforcement work rather than being focused on whether the activity is within the functions of law enforcement agencies.

32. The AFP and the ACIC already undertake disruption activity in the physical world in the course of investigating criminal offences, including to prevent criminal activity by disrupting it. These agencies have powers at their disposal to target persons suspected of engaging in criminal activity, including the controlled operations framework. The controlled operations framework enables the collection of evidence that may lead to the prosecution of a person for a serious offence, and allows for the authorisation of conduct which would otherwise be unlawful, under specific constraints. However, these powers are increasingly less effective against campaigns of cyber-enabled crime, including campaigns at large scale or obfuscated through the use of the dark web and anonymising technologies. To remain competitive, and lessen the volume and wide impact of cyber-enabled crime, the AFP and the ACIC must be provided with a new power to disrupt serious cyber-enabled crime.

33. The ability to carry out disruption (by adding, copying, deleting or altering data) would provide a practicable and effective option for preventing the continuation of serious criminal activity and minimising harms.

34. The AFP, the ACIC and some other designated agencies are able to add, copy, delete or alter data under a computer access warrant in the SD Act, but only for the purpose of obtaining access to the relevant data that is held in the targeted computer. Computer access warrants enable access to data held in computers to obtain evidence of the commission of offences, or the identities and locations of offenders. This is very different to disrupting data for the purpose of frustrating the commission of criminal offences. However, being able to add, copy, alter or delete data for the purposes of frustrating the commission of serious offences will provide agencies with more scope to respond to, and protect Australians from, high-risk, complex and time critical criminality online. This may present new information or evidence that would allow for the application of separate warrants or authorisations, as a means to identify, arrest and prosecute offenders. The ability to carry out disruption activity would also provide agencies with more options to minimise harms to victims.

Criminal intelligence collection via computer access

35. While computer access warrants have been, and will continue to be, critical for understanding more about known targets, they do have limitations. One of these limitations is when law enforcement is seeking to map out the criminal landscape before targeting their evidence-gathering inquiries. In the discovery phase of an investigation, law enforcement agencies will frequently have only small fragments of information or early leads. In these circumstances, the lack of sufficient information about a target's identity or location, or particular communications devices means that law enforcement agencies may not be able to use targeted investigatory powers, such as computer access warrants. Without the support of powers to enable the identification of potential offenders and understand the scope of their offending, these investigations into serious crime will fall at the first hurdle. Law enforcement agencies

need a new, complementary information-gathering power that will provide comparable pieces of the intelligence jigsaw.

36. The ability to collect criminal intelligence via computer access techniques would assist the AFP and the ACIC to, with an appropriate warrant, more effectively identify criminal activity where perpetrators are hiding behind anonymising technologies. Intelligence collected through computer access techniques would be used to inform decisions on how best to prioritise and direct resources to maximise law enforcement's impact on serious criminality. The utility of an intelligence collection power would be further enhanced if the AFP and the ACIC were permitted to target networks of criminality using computer access powers rather than specific individuals or particular devices. Collecting intelligence on criminal networks through computer access powers would assist law enforcement agencies' understanding of how serious, global criminal networks communicate and operate. This would allow agencies to follow up with crucial action against criminals using other investigatory powers.

37. Consistent with recommendation 162 of the Richardson review, these powers would enable the AFP and the ACIC to leverage existing Commonwealth capabilities to produce better results in combatting cybercrime. The Bill does not amend the existing powers and functions of the ASD, but instead provides three new powers to more effectively fight online criminality to the AFP and the ACIC, who will be able to utilise assistance from ASD in line with that agencies's existing functions, which include the provision of advice and expertise to assist Australian Government agencies.

38. This power will also facilitate joint operations with members of the National Intelligence Community, who currently conduct complex and interrelated intelligence operations. For example, information collected under a network activity warrant by the AFP about a terrorist organisation may be shared with ASIO if it is related to ASIO's functions.

Account takeovers for evidentiary purposes

39. Currently, there is no express power allowing law enforcement to take control of a person's online account without first having obtained the person's consent. This constrains law enforcement's ability to further their investigations, and gather valuable evidence, where the account holder does not consent. Providing the AFP and the ACIC with a clear authority to conduct account takeovers in these circumstances will provide new investigative powers to takeover a person's account without consent, either covertly (without the account holder's knowledge), or by compulsion where an assistance order requires the person to provide their account details.

40. Law enforcement's ability to identify and penetrate criminal networks is becoming increasingly hampered by offenders who are constantly adapting their technical tools and methodologies to remain one step ahead. For example, to deter law enforcement infiltration, child exploitation networks operating on the dark web often require new users to produce and upload new material in order to gain access to restricted areas. Providing the AFP and the ACIC with the ability to take control of a person's online account (where the person does not know, and does not consent) would allow them to gather evidence about that person's online criminality and the activity of their associates. Account takeovers would supplement existing investigatory powers, to target people who are already known within illegal online communities and uncover the identities of other offenders. This would allow the AFP and the ACIC to use the trusted relationships and networks which have been built between criminal associates against those same criminals.

41. In the same way that occurs when law enforcement agencies take over a person's account with their consent, the AFP and the ACIC would use the new account takeover power to support the exercise of existing investigatory powers, including search warrants, computer access warrants and controlled operations being conducted online. For example, an account takeover power could be used in conjunction with a controlled operation which would authorise the AFP or the ACIC to assume the account holder's identity, engage in ongoing interactions with associates to elicit information and assist in the identification of offenders and collection of evidence of the offending. Enabling the AFP and the ACIC to take control of an online account in these circumstances is an extremely valuable tool and would facilitate better evidence-gathering against criminals, mapping of their criminal networks and potential identification of victims.

Comprehensive Review of the Legal Framework of the National Intelligence Community Legislation (Richardson Review)

42. On 4 December 2020, the Government released the report of the Richardson review, along with the Government's response to this report. The review, undertaken by Mr Dennis Richardson AC, is the most substantial review into the legislation governing Australia's intelligence community since the Hope Royal Commissions in the 1970s and 1980s. The central recommendation for reform made by the review is the creation of a modernised legislative framework to govern electronic surveillance activities. This new framework will replace parts of a number of existing acts that govern electronic surveillance powers, including the TIA Act, SD Act and ASIO Act.

43. While the Government has agreed to take forward the Richardson review's central recommendation for broader electronic surveillance reform, this Bill is intended to address specific and time critical gaps in the existing legal framework preventing law enforcement agencies from identifying and disrupting serious crime online, particularly that perpetrated on the dark web. These gaps stem from advances in technology, and new powers are needed to ensure that our agencies can remain effective in combatting cyber-enabled crime.

44. Consistent with recommendation 161 of the Richardson review, this Bill does not extend the ASD's cybercrime function to apply onshore. Any technical assistance provided by the ASD in support of the new powers proposed in this Bill would be provided consistent with the ASD's existing statutory powers to assist Commonwealth agencies.

45. This Bill is consistent with recommendation 162 of the Richardson review, to the extent that the review recommended the AFP should be responsible for fighting cybercrime and undertaking disruption activities onshore. However, as set out in the Government's response to the Richardson review:

    a. The ACIC, drawing on its specialist criminal intelligence capabilities, also plays a vital role in discovering serious and organised crime activity that is perpetrated online, including by identifying priority cybercrime and cybercrime targets. The ACIC's intelligence functions directly enable investigative and disruption activity undertaken by law enforcement and intelligence partners, both within Australia and offshore.

    b. The Government disagrees with the Richardson review's position that the AFP does not need new powers to disrupt online offending. As recommended by the Richardson review, the AFP and the ACIC should fully utilise existing powers to combat cybercrime. However — as outlined above — those agencies' current powers are increasingly ineffective against mass campaigns of cybercrime, including those that use the cover of the dark web and anonymising technologies on the surface web. The increasingly large-scale use of the dark web, and other technologies that allow users to remain anonymous, to enable serious crime and terrorism is inhibiting agencies' ability to protect the community, including protecting children from sexual abuse. New powers should enable agencies to identify and collect intelligence on dark web targets, and to take action against those targets, whether that be through traditional investigation and prosecution, or through further disruption of criminal activities.

    c. Legislative reform is necessary to enhance the ability of the AFP and the ACIC to discover and disrupt serious criminality online. This Bill is designed to achieve that legislative reform. The powers proposed in this Bill are targeted at activities that have a direct and real impact on Australia's most vulnerable and are usually orchestrated by the most sophisticated of criminal networks. The proposed new powers are proportionate to the identified risk, and subject to robust safeguards and oversight. Oversight arrangements are appropriately apportioned between the IGIS and Ombudsman.[5]

[5] Government response to the Comprehensive Review of the Legal Framework of the National Intelligence Community, Recommendation 162, page 42, paragraphs 1-3.

46. The Richardson review noted concerns regarding new disruption powers for the AFP. In particular, the report notes that:

> At one end of the spectrum, the AFP could engage in reasonably uncontroversial 'disruption' activities, such as interfering with communications to a particular child abuse website. However, at the other end of the spectrum are 'disruption' activities that result in the destruction of property, such as a computer or server.[6]

47. It is important to note that the data disruption power proposed by this Bill does not provide the AFP or the ACIC with the ability to 'zap'[7] — that is destroy or damage — a computer. Rather, any damage incurred as a result of disruption must be in relation to data and not physical property, such as a computer or server. The data disruption power is available only upon application to an eligible judge or nominated Administrative Appeals Tribunal (AAT) member, and is supported by strong safeguards that expressly prohibit causing loss or damage to data that is not justified and proportionate or causing any permanent loss of money, digital currency or property other than data. Any activity resulting in the seizure of money or property by law enforcement remains governed by existing legislation, such as the *Proceeds of Crimes Act 2002*. Key elements of the disruption power are discussed in more detail below.

Overview of the Surveillance Legislation Amendment (Identify and Disrupt) Bill

Summary

48. The Bill introduces three new powers to enhance the ability of the AFP and the ACIC to respond to serious cyber-enabled crime:

    a. a **data disruption warrant** to enable the AFP and the ACIC to access computers and disrupt data by adding, copying, deleting or altering data in order to frustrate the commission of serious offences online

    b. a **network activity warrant** to allow the AFP and the ACIC to access computers for the purpose of collecting intelligence on a network of individuals suspected of engaging in or facilitating criminal activity, and

    c. an **account takeover warrant** to authorise the AFP and the ACIC to take control of a person's online account for the purposes of gathering evidence to further a criminal investigation.

49. The Bill also makes minor amendments to the controlled operations framework in the Crimes Act to improve the capacity for agencies to conduct controlled operations online. In particular, the Bill amends the requirement for illicit goods, including content such as child abuse material, to be under the control of law enforcement at the conclusion of an online controlled operation. To be clear, the category of illicit goods this amendment is targeted at is illegal, online content. This amendment is not intended to change the framework in place for other (non-content) illicit goods.

Data disruption warrants – Schedule 1

Purpose and overview

50. Schedule 1 of the Bill establishes a new framework in the SD Act for the AFP and the ACIC to obtain warrants to disrupt data held in a computer. Unlike traditional law enforcement powers sought for investigatory purposes, data disruption warrants will be sought for the **frustration of criminal activity**. Frustrating the commission of an offence could involve taking action to prevent an offence from ever occurring, making an offence more difficult to carry out, or stopping the continuation of an offence that is already occurring.

---

[6] Mr Dennis Richardson AC (2020), *Comprehensive review of the legal framework governing the National Intelligence Community*, volume 3, p. 220, para 38.66

[7] Mr Dennis Richardson AC (2020), *Comprehensive review of the legal framework governing the National Intelligence Community*, volume 3, p. 220, para 38.72

51. The new disruption power will provide the AFP and the ACIC with more options for responding to serious crime online. Under a data disruption warrant, the AFP and the ACIC will be permitted to covertly access computers to disrupt data (by adding, copying, deleting or altering that data) in order to frustrate the commission of relevant offences of a particular kind. This will be a covert power also permitting the concealment of data disruption activities. While the activities that may be authorised under a data disruption warrant are similar to those under a computer access warrant, the purposes for which these things may be done under each warrant are distinct. Computer access warrants may authorise access to data held in computers to gather evidence about relevant offences, whereas data disruption warrants authorise access to, and disruption of, data held in computers for the purposes of frustrating the commission of relevant offences.

52. Although evidence may be gathered incidentally under a data disruption warrant, the framework is intended to provide for data disruption activity and does not replace the computer access warrants as an evidence gathering regime. Noting the data disruption warrant authorises data modification and deletion, the AFP and the ACIC are experienced in deploying their tradecraft and capabilities to ensure any evidence obtained is preserved in its original form. This will help preserve the integrity of evidence obtained through a data disruption warrant, whilst also giving agencies confidence to perform disruption activities.

53. The power to disrupt data under a data disruption warrant will allow the AFP and the ACIC to prevent the continuation of serious criminal activity and minimise harm to victims. These warrants could be used to disrupt or deny access to a computer that is being used for illegal purposes, or to illegal content. For example, removing content or altering access to content (such as child abuse material) could prevent the continuation of serious criminal activity, minimise harm to potential victims and be the safest and quickest option where offenders are in unknown locations or obfuscating their identity.

54. Data disruption warrants will assist when the use of anonymising technologies or the dark web has constrained the ability of the AFP or the ACIC to respond to the criminal activity. For example, where the use of anonymising technologies has meant that offenders are too numerous, well-hidden or inaccessible for law enforcement to successfully use existing powers. The purpose of this warrant is to offer an alternative pathway for law enforcement to respond to serious crime online and minimise harm to victims, particularly where it is not feasible to pursue the traditional methods of investigation and prosecution.

Hypothetical example: ***Disrupting service to prevent continued access and offending – Organised crime***

Through human source intelligence, the ACIC identifies an encrypted communications platform being used by a known criminal syndicate to facilitate organised crime, including the importation of commercial quantities of drugs and laundering proceeds of crime. Access to the platform occurs through a customised handset designed and distributed by the criminal syndicate. Due to the use of anonymising technologies, the ACIC is unable to identify and locate users to effectively undertake traditional investigative action.

With the suspicion that organised crime is occurring, the ACIC apply for and obtain a data disruption warrant. Once the warrant is issued, the ACIC are able to remotely access the platform and perform disruption activities by disrupting communications to and from the platform, making it difficult for offenders to continue using the encrypted handsets and the platform. This may include, for example, changing passwords to prevent users' access to the platform, introducing malware onto the devices connecting to the platform and denial of service attacks to prevent the server hosting the platform from operating. The ACIC may also carry out disruption by removing details of where to deposit money for those seeking to buy the drugs or re-directing the funds transfer into a different financial account without causing a person to suffer a permanent loss of money.

The disruption activities authorised by the data disruption warrant allow the ACIC to frustrate the organised criminal activity, while also enabling evidence to be obtained on the service and its users. Information gathered by virtue of disruption may be used in prosecution of offenders or to support the furthering of the investigation under a subsequent evidence gathering power.

While this example focuses on organised crime, the principle could be applied to many other crime types – for example, if the AFP was investigating terrorist groups.

Network activity warrants – Schedule 2

Purpose and overview

55. Schedule 2 of the Bill introduces an intelligence collection power for the AFP and the ACIC in the SD Act to enable them to target groups of individuals suspected of being a criminal network – for example where individuals are exchanging child abuse material over a common platform, or they are an organised syndicate engaged in a variety of criminal offences. A network activity warrant will authorise access to data held in computers used by the individuals in the criminal network, even if agencies have not yet ascertained the precise identities or locations of individuals or their particular computers. The AFP and the ACIC will also be authorised to add, copy, delete or alter data but only if necessary to access the relevant data (e.g. to overcome security features like encryption). For clarity, this does not enable the AFP or the ACIC to modify data for the purposes of frustrating offences, which instead (or in addition) requires a data disruption warrant.

56. Network activity warrants will enable the AFP and the ACIC to target criminal networks about which very little is known, other than that there is a group of persons using a particular online service to carry out criminal activity. A criminal networks of individuals is a group of individuals who are linked electronically, and one or more of whom are engaging in, or facilitating, conduct constituting a relevant offence. To be linked electronically means to either be using the same electronic service or communicating electronically. A criminal network may be an organised criminal group, or may be individuals who are not coordinated in any way, and may not even have knowledge of each other's existences, but are still electronically linked. For example, persons accessing the same dark web marketplace to buy and sell illicit drugs. The criminal network of individuals being targeted must be specified in the warrant meaning that the issuing authority will have to consider whether accessing the devices used by those individuals is reasonable and proportionate in all of the circumstances. This ensures that the concept of a 'criminal network of individuals' cannot be construed so broadly as to capture all users of Facebook, for example.

57. The number and identities of the individuals making up the criminal network do not have to be known, nor do the details of the relevant offences, in order to apply for a network activity warrant. The composition of the criminal network may also change over time as individuals enter and exit the group. This ensures data that is unknown or unknowable at the time the warrant is issued can be discovered, including on devices that have disconnected from the network once the criminal activity has been carried out (for example, a person who disconnected from a website after downloading child exploitation material). This reflects the purpose of the network activity warrant in enabling intelligence to be collected about offences and offenders, before there is enough specific information to obtain an evidence-gathering warrant, such as a computer access warrant. The purpose of the warrant is to allow for the collection of intelligence about the commission of offences at the discovery phase of an investigation rather than to gather evidence to prove the exact nature of the offending.

58. Under a network activity warrant, the AFP and the ACIC will be able to collect intelligence to support their existing law enforcement and criminal intelligence functions. Intelligence collected under a network activity warrant must be relevant to the prevention, detection or frustration of one or more kinds of relevant offences, it cannot be for any purposes that would constitute a 'fishing expedition', or for broader intelligence purposes which will remain within the remit of ASIO and intelligence agencies empowered under the *Intelligence Services Act 2001*. A nexus to agencies' law enforcement functions ensures that this power can be used to support further investigatory powers, which will allow agencies to target their resources towards the highest levels of criminality.

59. Intelligence collection targeting criminal networks will allow law enforcement agencies to discover the scope of criminal offending and the identities of the people involved. This power will be particularly useful where the use of anonymising technologies or the dark web has rendered potential offenders unidentifiable, limiting law enforcement's ability to target criminality using existing investigative powers. The ability to target criminal networks through a network activity warrant will allow the AFP and the ACIC to respond to large-scale criminal offending in the same way they would in the physical world, for example by observing how criminal groups operate through surveillance This will assist the AFP and

the ACIC in developing a clear intelligence picture of serious criminal activity online enabling more targeted investigatory powers (such as computer access warrants) to be deployed.

Hypothetical example: *Targeting a criminal network suspected of money laundering offences*

While monitoring a suspected organised crime group, the AFP becomes aware of an encrypted messaging platform being used by a member of the group to communicate with a number of unknown individuals. The AFP cannot yet ascertain the precise identities of group members, and the offender's conduct has not met the threshold for arrest.

Even though the computers being used by the group members to communicate on the encrypted messaging platform cannot be specifically identified, and their true internet addresses are masked by anonymising technology, the AFP could now seek a **network activity warrant** authorising access to data held in computers that are using the encrypted messaging platform to communicate. The warrant does not need to individually identify those computers, but may specify the particular encrypted messaging platform being targeted and the potential money laundering offences targeted by the warrant.

Importantly, the network activity warrant enables the AFP to target any computers used by members of the criminal network to access the platform over the life of the warrant, even if members change computers regularly. This ensures that the AFP can access as much relevant information about the criminal network as possible, and allows the AFP to gather intelligence about the group, its participants (including the identities of ring leaders) and the scope of planned offending. It is revealed that the encrypted messaging platform is being used by a large number of people who are laundering money through Australia.

The AFP may then use the information obtained under the network activity warrant in an application for a subsequent investigatory power, such as computer access warrant, which will enable the gathering of evidence about the flow of finances, and to find out who is the leader in charge of the international organise crime operation. The AFP may also share the information obtained under the network activity warrant on a police-to-police basis with foreign law enforcement partners, to target further offenders overseas.

Hypothetical example: *Using the industry assistance framework to support a network activity warrant*

In the course of an investigation into the trafficking of illicit drugs, the ACIC identifies a type of encrypted handset being sold specifically to transnational, serious and organised crime entities to facilitate drug importations. The only known use of this handset is to communicate with other members of drug smuggling syndicates. The device does not contain any regular consumer features, only a specialised communications platform, advertised as being particularly robust against law enforcement intervention. The technology in use poses challenges to law enforcement as all communications are encrypted and the users are anonymised.

By issuing a technical assistance request under Part 15 of the *Telecommunications Act 1997* (**Telecommunications Act**) to a relevant internet service provider to obtain network information associated with the encrypted handset, the ACIC is able to confirm the unique signature used by these devices on the telecommunications network. This allows for identification of other handsets around the country, as well as where and when they are being used.

In order to further understand the use of these devices by serious and organised crime networks, the ACIC applies for a network activity warrant to collect intelligence on the criminal network planning the drug importation and the wider group of users of the particular specialised handset.

During the course of the warrant, the ACIC collects intelligence to inform a number of things, including the group's members, their identities, location and associated offending. The ACIC copies data for the purposes of analysing it to determine its relevance and intelligence value. The ACIC finds detailed

plans outlining modifications made to various ships to include concealed compartments which are to be used to transport illicit drugs. This information is copied in order to analyse and determine which vessels are relevant, what vulnerabilities exist in the networks' planning and criminal intent. The intelligence gained under this warrant then assists the ACIC to inform future prevention and disruption strategies and is used to make out the grounds for an application for another warrant.

Account takeover warrants – Schedule 3

Purpose and overview

60. Schedule 3 adds to the investigatory powers of law enforcement agencies by introducing a new warrant in the Crimes Act allowing the AFP and the ACIC to take control of a person's online account for the purposes of gathering evidence about serious offences. An online account may include, for example, an account on a dark web forum or marketplace, an email service, social media account, subscription to a news service or a user profile of a messaging platform. An account takeover warrant will facilitate covert and compelled (without consent of the account holder) account takeovers. This power is designed to support the exercise of other evidence-gathering powers, such as search warrants, computer access warrants and controlled operations being conducted online.

61. To take control of an online account involves law enforcement taking steps that result in them having exclusive access to the account. Having exclusive access to the account will mean that the law enforcement officer can operate the account fully, without interaction or interference from the account holder or users of the account. In most cases, taking control of an online account will involve depriving the account holder or a user of their access to the account.

62. Under an account takeover warrant, law enforcement will be able to use account credentials to change passwords, or other log-in details, associated with an account to lock out the account holder or user to gain exclusive access to the account. Any other activities, such as accessing data or performing undercover activities while in control of the account such as assuming a false identity, must be performed under a separate warrant or authorisation. At the conclusion of the warrant, the officer must take reasonable steps to restore access to the account to the account holder, if it is lawful for the account holder to operate the account.

63. Account takeover warrants may authorise the taking control of multiple online accounts (for example, a social media account and the email service associated with that account). Depending on the nature of the investigation (particularly where the target is unaware), it may be necessary to take control of multiple online accounts to maintain the covert nature of the investigation, or to ensure the successful execution of the warrant. In order to take control of multiple accounts it must be necessary to do so in the course of the same investigation, and each of these accounts must also be specified in the warrant.

64. The new framework ensures that information compelled from a person under a section 3LA assistance order to support a search warrant (such as account credentials or passwords) can be used in the execution of an account takeover warrant. This information could then be used to take control of an online account under an account takeover warrant but only where the matter relates to the same investigation. Account takeover warrants are designed to be used in conjunction with other investigatory powers, including search warrants. To further support the interoperability of the frameworks, the Bill also allows information compelled from a person under an assistance order to support an account takeover warrant to be used for the purposes of a search warrant.

65. Account takeover warrants will allow law enforcement to use the trusted relationships and networks that have been built between criminal associates against those same criminals. In many cases, taking control of an online account will, when used in conjunction with other investigatory powers, be an efficient method for law enforcement to penetrate online networks, uncover the identities of criminal actors, and gather evidence of the commission of serious offences online, including on the dark web and where using anonymising technologies.

Hypothetical example: *Account takeovers warrants used with search warrants and controlled operations*

An AFP officer executes a search warrant under section 3E of the Crimes Act on the premises of a person suspected of using a dark web forum to distribute child abuse material. During the course of executing the warrant, the AFP officer recovers a laptop and other devices used by the person that is the subject of the warrant. The person complies with an assistance order under section 3LA of the Crimes Act, and provides the AFP officer with the password to their forum account, but does not consent to the AFP officer taking control of their account.

The AFP officer now applies for an account takeover warrant, which permits the officer to take control of the person's account. This enables the AFP officer to use the password obtained using the section 3LA assistance order to take control of the person's account which prevents the person's continued access to the forum and the continuation of their alleged offending.

The AFP officer could then use the account, as part of a controlled operation under Part IAB, to covertly engage with other members of the dark web forum. This may require engaging in certain controlled conduct (authorised by the controlled operation) to convincingly interact with offenders. Used in this way, the account takeover may help identify other offenders, map the forum hierarchy and potentially identify victims.

If the original account holder was sufficiently senior (for example, an administrator or moderator) in the forum hierarchy, the AFP could work towards an outcome similar to the FBI's 'Playpen' investigation, which identified a number of users and resulted in the takedown of the service. The AFP could use the powers proposed in the Bill, including **account takeover warrants** and **data disruption warrants**, in combination with existing powers such as computer access warrants and controlled operations, to identify and disrupt criminal forum activity.

Amendments to the controlled operation framework – Schedule 4

66. Schedule 4 amends the controlled operations framework in the Crimes Act to enhance the AFP and the ACIC's ability to conduct controlled operations online. In particular, the Bill amends the requirement for illicit goods (including content such as child abuse material) to be under the control of law enforcement at the conclusion of a controlled operation conducted online. To be clear, the category of illicit goods that this amendment is targeted at is illegal, online content. This amendment is not intended to change the framework in place for other (physical) illicit goods.

67. While law enforcement will always ensure that illicit content is controlled, to the best of their ability, this amendment addresses how easy data is to copy and disseminate, and the limited guarantee that all illegal content will be able to be under control of the AFP and the ACIC at the conclusion of a controlled operation conducted online.

Use of powers to deliver enhanced law enforcement outcomes

68. The powers in the Bill will improve the AFP and the ACIC's overall capacity to respond to serious crime online. When used in conjunction, the powers will enhance the AFP and the ACIC's ability to identify and disrupt threats to the safety of Australians.

69. For example, the combination of new powers proposed in this Bill could enable Australian agencies to identify users and disrupt access to dark web services hosting illicit material, similar to the outcome achieved by the United States Federal Bureau of Investigations (FBI) in Operation Pacifier. This operation led to the arrest of over 900 users of the dark web child exploitation site 'Playpen'.

70. In 2014, the FBI received a tip from a foreign law enforcement agency that The Onion Router 'Tor' hidden service site 'Playpen' was hosting child exploitation material and appeared to be located within the United States. After additional investigation, the FBI obtained a search warrant and seized the server hosting the site. The FBI continued to observe users visiting the 'Playpen' for almost two weeks, before shutting the site down. During this time, the FBI obtained a second warrant authorising them to use technical capabilities which exploited a system vulnerability, thereby revealing users' identities. The

operation led to the arrest of over 900 website users. The 'Playpen' investigation was ultimately successful because of the way the FBI was able to take advantage of a technological error made by the website creator.

Hypothetical example: *Use of the powers to target the distribution of child abuse material*

The AFP receives a tip from a foreign law enforcement agency that a dark web service is being used to distribute child abuse material among hundreds of users. The AFP obtains a **network activity warrant** to enable access to computers used by individuals accessing the dark web service. The intelligence collected allows the AFP to determine the scope of offending, and identify one of the users as an Australian. The AFP can now apply for evidence-gathering warrants, such as interception, computer access or search warrants, to investigate this person's activity further.

Ultimately, the AFP (working through the Joint Anti-Child Exploitation Teams) executes a search warrant under section 3E of the Crimes Act on the premises of the Australian suspect, and locates a laptop which has been used to access the child abuse forum (via an anonymising browser). The person is arrested and charged, but does not consent to the AFP taking control of their account. Analysis of information retrieved from the laptop and other devices indicates the person is a site administrator.

In order to progress the investigation into the broader network, an AFP officer obtains an **account takeover warrant**, and accompanying order under section 3ZZZU of the Crimes Act, requiring the person to provide relevant account credentials and passwords. The person complies and the AFP takes exclusive control of the person's account on the dark web forum.

Once the AFP has control of the account, and the account holder's relevant access rights on the forum, the AFP officers could then attempt to identify other users on the dark web service. This could be facilitated by using the account holder's forum access, or conducting a covert operation to engage with other users, in an attempt to de-anonymise and collect evidence of their criminal activities.

However, it may be that the sheer scale of membership of this group means arrest and prosecution is not the most effective way of addressing the offending. The AFP could then apply for a **data disruption warrant**, enabling the AFP to remove material from the dark web service and disrupt users' continued access and distribution of child abuse material.

Key elements of the Bill

Strict thresholds for application

71. The warrants in the Bill are subject to strict thresholds which ensure that they may only be sought where reasonable, proportionate and necessary. Each power has been designed to align with the framework in which it sits, and, as much as possible, to align with other powers that agencies are likely to use in conjunction with these new warrants. This is to reflect the fact that agencies require and use a suite of powers in order to tackle online crimes that are complex, evolving, and often occur on multiple devices and across multiple jurisdictions.

72. Each of the powers must be sought in respect of *relevant offences*, that is, generally offences punishable by a maximum term of imprisonment of three years or more. This threshold limits the availability of data disruption warrants, network activity warrants and account takeover warrants to serious crimes, such as terrorism, child exploitation and drugs and firearms trafficking.

73. Commentary about the Bill since its introduction has pointed to the lower offence threshold for the application of these warrants than some other offence thresholds in the electronic surveillance framework. It is important to note that the offence threshold is just one element that has to be met and that there are strict requirements for the application and issuing of these warrants. Under the TIA Act, to approve an application for a telecommunications service warrant or a named person warrant, the issuing authority must be satisfied that there are reasonable grounds to suspect that the information sought is likely to assist with an investigation into a *serious offence*. If an offence is punishable by life or

a maximum term of imprisonment of at least seven years it is a serious offence under the TIA Act. Whilst this is a higher threshold than those provided in the Bill, it is important to note that there are a range of other offences which constitute serious offences under section 5D of the TIA Act, not all of which carry a seven year penalty. For example, the computer offences in Part 10.7 of the *Criminal Code Act 1995* (the **Criminal Code**) carry a penalty of five years' imprisonment.

74. The offence thresholds in the Bill have been designed to match the offence thresholds in the SD Act and the Crimes Act. Surveillance device warrants and computer access warrants can be issued in respect of *relevant offences*. Relevant offences are offences listed in section 6 of the SD Act and are generally offences against the law of the Commonwealth that are punishable by a maximum term of imprisonment of three years or more or life. Examples of Commonwealth offences that are punishable by a maximum term of imprisonment of three years include threatening to commit offences, interfering with political rights and duties, associating with terrorist organisations, and conduct by Commonwealth officers causing harm to Australia's interests. It is important that data disruption warrants and network activity warrants carry this same threshold, as these warrants will often be used as part of the same investigation or related investigations. As outlined above, it is also important that serious crimes that carry penalties of less than seven years can be captured by these warrants.

75. There are some exceptions to the three year penalty threshold. The existing definition of 'relevant offences' in the SD Act also includes some offences with a lower penalty. For example there are several important offences in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, including failure to report the importing of more than $10,000 in physical currency, which carry a maximum term of imprisonment of 2 years.

76. To apply for a **data disruption warrant** there must be a reasonable suspicion that disrupting the data held in the computer is likely to substantially assist in frustrating the commission of an offence. Similarly, to apply for a **network activity warrant**, there must be a reasonable suspicion that accessing data will substantially assist in collecting intelligence about a criminal network. This threshold is borrowed from section 25 of the ASIO Act under which search warrants can only be issued if there are reasonable grounds for believing that access to things on premises will substantially assist in the collection of intelligence in respect of a matter that is important in relation to security. It is not enough that there is a suspicion that the information is simply relevant to the investigation, or will simply *assist* in the collection of intelligence or the disruption of data; the word 'substantially' has been deliberately chosen to ensure a higher threshold that is proportionate to the activities being undertaken under the power of these warrants.

77. These thresholds were set as it will not always be possible for an agency executing a data disruption warrant or a network activity warrant to know the full extent of the criminal activity that is the subject of the warrant before the warrant is carried out. For example, in removing child abuse material from an online platform under a data disruption warrant, it will not always be known that a specific crime (such as possession of child abuse material) will be frustrated, as, for example, account holders may have decided not to access the platform due to other reasons. In other words, it is difficult for agencies to quantify offending which does not occur. For this reason, the warrant requires satisfying the issuing authority that disrupting data held in a computer is likely to substantially assist in frustrating offences, as opposed to the other formulation of thresholds in the SD Act, which is generally that the use of the warrant is necessary in the course of an investigation.

78. Similarly, the requirement that there be a reasonable suspicion that access to a computer will substantially assist the collection of intelligence under a network activity warrant (rather than a higher threshold as in the rest of the SD Act) reflects the fact that an agency will not know the extent of intelligence to be collected prior executing the warrant. Like ASIO warrants for intelligence purposes, this threshold is appropriate for network activity warrants, which are also for criminal intelligence and not evidentiary purposes.

79. Account takeover powers have been dealt with differently. An **account takeover warrant** may be sought if an officer of the AFP or the ACIC suspects on reasonable grounds that taking control of one or more online accounts is **necessary** in the course of that investigation for the purposes of enabling evidence to be obtained. The definition of an 'online account' is deliberately broad in order to capture the types of accounts that the AFP or the ACIC may need to take control of during the course of a criminal

investigation. Accounts include social media accounts, bank accounts, email accounts, and web forum accounts.

80. For example, the AFP or the ACIC may be authorised to take control of a person's online banking account, but only where doing so does not result in the permanent loss of money, digital currency or property that is not data (discussed in more detail below). The ability to take control of online banking accounts is important as online criminality will often be identified through a pattern of unusual financial transactions linking individuals to the money trails that follow criminal activity.

81. The broad definition of 'online account' is balanced against the high threshold to which applications for account takeover warrant are subject. In applying for an account takeover warrant, the applicant will be required to demonstrate to the issuing authority that taking control of the account is **necessary** in the course of a criminal investigation, rather than likely to assist in that investigation. Account takeover powers are intended to be used when the agency has deemed it necessary to further an investigation; that is, when there is a clearer picture of the particular offending than that seen in the intelligence collection phase.

Independent scrutiny and issuing criteria

82. All of the warrants in the Bill must be sought by the AFP and the ACIC by way of application to a judicial officer or AAT member, who may grant the warrant sought if they are satisfied that there are reasonable grounds for the suspicion founding the application for each warrant. Oversight of decisions to apply for warrants by judicial officers and AAT members provides for independent scrutiny of the warrant application and satisfaction of reasonableness and proportionality.

83. Consistent with other powers in the SD Act, **data disruption warrants** and **network activity warrants** can only be issued by an eligible Judge or nominated AAT member, whereas, consistent with other powers in the Crimes Act, **account takeover warrants** can only be issued by a magistrate.

84. AAT members, eligible judges and magistrates (issuing authorities) all play critical roles — nominated or appointed in their personal capacity — as independent decision-makers in authorising investigatory powers in the current regimes in the SD Act (judges and AAT members) and in the Crimes Act (magistrates). In accordance with this existing framework, the Bill recognises that the complex decision-making involved in authorising the new powers in the Bill requires the independence offered by the judges, AAT members and magistrates who already issue other warrants under those Acts and have the skills and experience to do so.

85. The power to authorise warrants under various pieces of legislation is conferred on AAT members, judges and magistrates in their personal capacity (*persona designata*) as a means of ensuring accountability in the course of a sensitive investigation or law enforcement procedure. *Persona designata* functions for warrant applications are not an exercise of the formal judicial or administrative powers of the court or tribunal. Rather, an AAT member, judge or magistrate when exercising *persona designata* functions is acting as an independent decision-maker.

86. While an AAT member is not independent of government in the same way as a judge (although some members of the AAT are also judges), the AAT and its members are similarly seen to require a high degree of independence from government, by virtue of their role to undertake independent merits review of administrative decisions made under Commonwealth laws. AAT members exercising *persona designata* functions are also afforded the same protection and immunity as a Justice of the High Court of Australia. An AAT member's appointment can only be terminated by the Governor-General following prayer for the termination by both Houses of Parliament on specific grounds. The independence of AAT members exercising *persona designata* functions is strongly safeguarded.

87. Further, AAT members provide written consent prior to being authorised to perform *persona designata* functions, and will do so for functions under the Bill. Consent also serves to protect an AAT members' independence and autonomy to decide whether or not to exercise *persona designata* powers.

88. Whilst there has been some commentary about whether AAT members are appropriate to issue these new warrants, it is important to note that the ability for nominated AAT members to authorise the use of investigatory powers is not new. Nominated AAT members issue surveillance device warrants and

computer access warrants under the SD Act, and have played a key role in issuing interception and stored communications warrants under the TIA Act since 1998.

89. The skills and experience of AAT members make them suitable to assess applications for data disruption warrants and network activity warrants in accordance with the legal requirements under the Bill. To be appointed as a member of the AAT, a person must have been enrolled as a legal practitioner for at least five years or, in the opinion of the Governor-General, have special knowledge or skills relevant to the duties of an AAT member, being to undertake independent merits review of administrative decisions. AAT members are similarly well-placed to conduct dispassionate assessments of evidence, reasonableness and proportionality of warrant applications in their *persona designata* functions.

90. Providing a wide, but always suitably qualified, range of independent decision-makers ensures that there is a sufficient number of available decision-makers in order to consider applications made by the AFP and the ACIC.

91. Having a magistrate issue account takeover warrants ensures consistency with other law enforcement powers in the Crimes Act.

92. Alignment of the issuing authorities ensures that the warrants in the Bill can be sought in conjunction with existing investigatory powers. For data disruption warrants and network activity warrants, this will often be computer access warrants in the SD Act. For account takeover warrants, this will often be controlled operations and search warrants in the Crimes Act.

93. In deciding to issue each of the warrants in the Bill, there are certain matters to which the issuing authority must have regard. A key requirement in each of the warrant frameworks is consideration of proportionality:

    a. For **data disruption warrants**, the Judge or AAT member must be satisfied that the activities authorised by the warrant is justified and proportionate with regard to the offences targeted.

    b. For **network activity warrants**, the Judge or AAT member must consider whether the activities authorised by the warrant are proportionate to the likely value of intelligence to be collected, as well as the extent to which the warrant is likely to result in access to data of persons lawfully using a computer.

    c. For **account takeover warrants**, the magistrate must consider the extent to which the privacy of any person is likely to be affected.

94. The issuing of a data disruption warrant or network activity warrant must meet a test of proportionality. This is to ensure that the use of these warrants is proportionate to the alleged or suspected offending in all circumstances.

95. When considering whether the actions are justified and proportionate in respect of data disruption warrants and network activity warrants, the issuing authority will take into account, for example, the scope of the warrant in terms of how many people are affected, the exact nature of the potential intrusion on people's private information, and whether that intrusion is justified by the serious nature of the criminality being targeted. Each of these warrants can only be applied for on the basis of a link to serious offending. These warrants target activity of the most serious nature, including terrorism, child exploitation, drug trafficking and firearms trafficking.

96. An explicit privacy consideration is appropriate for the issue of account takeover warrants as a targeted evidence gathering power.

97. Central amongst other considerations that issuing authorities must take into account is consideration of the existence of any alternative means of achieving the objective of the warrant.

    a. For **data disruption warrants**, the Judge or AAT member must consider alternative means of frustrating the criminal activity.

    b. For **network activity warrants** and **account takeover warrants**, the issuing authority must consider alternative (or less intrusive) means of obtaining the information sought to be obtained.

98. These safeguards are particularly important for ensuring that avenues of investigation, information collection or disruption that are less intrusive on privacy are considered. This ensures that, where there

are narrower activities that involve a more targeted approach, this will be taken into account by the issuing authority.

Authorisations for emergency situations

99. The activities permitted by the **data disruption warrant** and **account takeover warrant** may also be internally authorised where there is an imminent risk of serious violence to a person or substantial damage to property. In order to do so, the circumstances must be so serious, and the matter of such urgency, that the data disruption or an account takeover activity is immediately necessary for dealing with that risk.

100. The ability to disrupt data in emergency situations is important for ensuring that the AFP and the ACIC will be able to respond to rapidly evolving and serious threats in a timely and effective manner. Approval for the giving of an emergency authorisation must then be sought by application to a Judge or AAT member (for data disruption) or a magistrate (for account takeovers). This provides independent scrutiny of decisions to authorise data disruption in emergency situations.

101. It is important to note that the emergency authorisation provisions do not amount to warrants being able to be internally issued. All of these warrants are independently authorised by judges, AAT members or magistrates. Emergency authorisation provisions are crucial tools for law enforcement in the most extreme circumstances. Emergency authorisations are only to be used when there is an imminent risk of serious violence to a person or substantial damage to property and it is not possible to seek out a usual issuing authority from whom to apply for the warrant in the limited timeframe available before that imminent risk becomes a reality. Emergency authorisations must stand up to independent scrutiny after the fact, at which time the eligible Judge, nominated AAT or magistrate (in respect of account takeover warrants) must take into account strict issuing criteria, such as the nature and risk of serious violence to the person and the existence of alternative methods that could have helped to avoid the risk. If the issuing authority approves the emergency authorisation, the issuing authority may issue a warrant for continued action under the data disruption warrant or account takeover warrant, or alternatively order that the activity cease. This would be in cases where access is no longer required. If the issuing authority does not approve the giving of the emergency authorisation, he or she may order that activity immediately cease, and he or she can make orders about how the information collected under the warrant should be dealt with.

102. Officers must make records of emergency authorisations as soon as practicable. The information gathered under emergency authorisations is protected information, in the same way as that collected under a warrant. The Ombudsman will have oversight of emergency authorisations associated with both data disruption warrants and account takeover warrants, and has the same inspection powers for emergency authorisations as for warrants.

103. Emergency authorisations are not available for the activities permitted by the **network activity warrant** noting the purpose of this warrant in assisting target discovery, rather than responding to time-critical situations.

Extraterritorial application of the new powers

104. If there is a need to access and disrupt data in a computer in a foreign country under a **data disruption warrant** or **network activity warrant**, consent must be sought from an appropriate foreign official. The ability to apply these warrants extraterritorially ensures that the AFP and the ACIC will be able to address criminal activity threatening Australians where the data is located overseas or offenders are not in law enforcement's jurisdictional reach. Consent from a foreign official is not required if the persons executing the warrant are physically located in Australia, and the location of where the data is held is unknown or cannot reasonably be determined.

105. **Account takeover warrants** may be used to take control of an online account regardless of where the account data is located. However, this power is only available in circumstances where the AFP or the ACIC is investigating a relevant offence as described above, and where taking control of the account is likely to substantially assist in the course of that investigation for the purpose of enabling evidence to be obtained. Consistent with other powers in the Crimes Act, these warrants can only be exercised by the AFP or the ACIC where the particular offence is one that is within AFP or ACIC's functions to investigate.

106. Account takeover warrants only permit officers to take control of an online account to gain exclusive access to that account. Further activities are only permitted if the AFP or the ACIC were to obtain and use another warrant or authorisation in conjunction with an account takeover warrant. Those other warrants or authorisations have, where appropriate, their own frameworks regarding extra-territoriality, for example, the provisions in the SD Act regarding obtaining the consent of an appropriate foreign official. This means that if the AFP or the ACIC need to conduct covert activities after gaining control of a person's account, such as modifying or accessing other data on a person's account or targeted device, to enable access to data accessible under the warrant, and they know that the data is held in a foreign jurisdiction, they will need to seek the consent of an appropriate foreign official.

Ability to seek assistance from persons with knowledge

107. The AFP and the ACIC can apply to a judicial officer for an order to compel a person to provide information or assistance that is reasonable and necessary to carry out the warrant. Only a specified person can be required to give this assistance. Specified persons include the owner or lessee of the particular computer that the officer needs to access, the employee of the owner of the computer, a person who uses the computer, or a person who is a system administrator for the system that includes the particular computer. It will be an offence for a person who has been issued an order, and is capable of complying with the order to contravene the order.

108. Orders requiring assistance already exist in relation to computer access warrants. This mechanism is not intended to allow law enforcement to compel assistance from the technology industry, but rather from a person with relevant knowledge of a particular computer or computer system, or online account in the case of account takeover warrants, to the investigation or operation (such as a person who uses a computer or online account).

Safeguards and limitations

109. The Bill is supported by strong safeguards and limitations to ensure that the activities authorised by the warrants are justified and proportionate for the purposes of the warrant, and are only exercised where necessary.

Judicial review is available

110. Decisions made in regard to data disruption warrants, network activity warrants and account takeover warrants can be challenged through judicial review. As these are covert powers, in practice the challenge to these decisions will likely only be after the particular investigation has become overt. To make information available in order to bring about such a challenge, the Bill ensures that protected network activity warrant information (which are not for evidence collection and therefore have strict prohibitions on adducing information in evidence) may be admitted into evidence in proceedings that are not criminal proceedings. This is an important exception to the general secrecy provisions that apply to covert intelligence gathering activities. The Bill also applies the same exception to information gathered under an account takeover warrant.

111. Decisions made under the SD Act and the Crimes Act are not exempt from judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (**ADJR Act**). The Bill does not seek to depart from this precedent. There is an error in the human rights compatibility statement in the explanatory memorandum supporting the Bill, which states that the Bill excludes judicial review under the ADJR Act. This is incorrect, and the human rights compatibility statement will be amended accordingly.

112. While judicial review is available, agency decisions to exercise a power and issuing authority decisions to issue warrants are not subject to merits review. This is consistent with longstanding principles and practice relating to national security legislation and powers.[8] However, a defendant may seek to challenge evidence obtained under a warrant, should this evidence be used in the course of an eventual prosecution. The use of powers in the Bill will be independently overseen by the Commonwealth

[8] Decisions of a law enforcement and national security nature were identified by the Administrative Review Council in its publication What decisions should be subject to merits review as being unsuitable for merits review.
https://www.arc.ag.gov.au/Publications/Reports/Pages/Downloads/Whatdecisionsshouldbesubjecttomeritreview 1999.aspx

Ombudsman (for data disruption warrants and account takeover warrants) and the Inspector-General of Intelligence and Security (for network activity warrants). While this is not a merits review process, these oversight bodies play an important role in auditing and inspecting the records of agencies which increases transparency and accountability, and monitors and encourages compliance with the legislative requirements in the Bill.

Revocation and discontinuance requirements apply

113. There are strict revocation and discontinuance requirements that ensure that each of the warrants can only be used for the purpose for which they were originally sought, and if these circumstances cease to exist, the warrant must be revoked and execution of the warrant must be discontinued. The chief officer of the AFP or the ACIC has an obligation to revoke each of the warrants after having become satisfied that the warrant is no longer required for the purpose in which it was sought. The chief officer also has an obligation to ensure that the execution of the warrant is discontinued if the warrant is no longer necessary.

Limits on interception and surveillance

114. As with existing computer access warrants, **data disruption warrants** and **network activity warrants** also permit the interception of a communication passing over a telecommunications system but only if doing so is for the purposes of executing the warrant. Often it will be necessary for law enforcement agencies to intercept communications to make access to and disruption of data practicable or technically possible. Data disruption warrants and network activity warrants cannot authorise the collection of evidence or intelligence by interception. If the AFP or the ACIC require interception to do anything more than facilitate execution of a data disruption or network activity warrant — for example, if the AFP or the ACIC want to gather evidence by interception — those agencies must seek a separate interception warrant from an eligible issuing authority under the TIA Act.

115. Similarly, **network activity warrants** also permit the use of surveillance devices but only for the purposes of facilitating the execution of a network activity warrant. It will often be necessary for law enforcement to use a surveillance device while executing a network activity warrant to make the things authorised by the warrant possible or to maintain the covert nature of the warrant. For example, it may be necessary to surveil a computer to determine whether it is being used, or whether it can be accessed covertly. The use of surveillance devices under a network activity warrant is permitted to facilitate the execution of that warrant, as it may not always be feasible for law enforcement to obtain a separate surveillance device warrant for this purpose. This is because the threshold tests for application for a network activity warrant and a surveillance device warrant are not aligned. These threshold tests are not aligned because these warrants are for different purposes. In particular:

    a. A network activity warrant is directed at the collection of intelligence relevant to the prevention, detection or frustration of criminal activity. As discussed above, a key threshold in this respect — based on equivalent ASIO Act thresholds for intelligence collection — is that the AFP or the ACIC must have a reasonable suspicion that accessing data will substantially assist in collecting intelligence about a criminal network. As discussed below, this intelligence cannot be used in evidence in criminal proceedings (other than for a contravention of the secrecy provisions that apply to this intelligence).

    b. A surveillance device warrant is focused on evidence-gathering in the course of criminal investigations. A key threshold in this respect is that a law enforcement officer must suspect on reasonable grounds that the use of a surveillance device is necessary in the course of an investigation for the purpose of enabling evidence to be obtained of the commission of a relevant offence, or to find the identify or location of offenders.

116. Similar to permissible interception, a network activity warrant cannot authorise the collection of evidence or intelligence by using a surveillance device.

Limits on interference and causing loss or damage

117. There are certain actions that are specifically prohibited on the face of the legislation for each of the three warrants. Specifically, the warrants do not authorise the doing of any thing that is likely to materially

interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer, unless doing those things is necessary for carrying out the purpose of the warrant. Data disruption warrants cannot authorise causing material loss or damage to other persons lawfully using a computer, unless the loss or damage is justified and proportionate to the offences covered by the warrant. This is because there may be circumstances in which it is necessary to interact with data on a third party's computer, for example, a person hosting a website that, without that person's knowledge, is being used for illicit purposes. Network activity warrants and account takeover warrants, however, cannot authorise causing any material loss or damage to persons lawfully using a computer under any circumstances.

118. There are also statutory conditions providing that neither a **data disruption warrant** nor an **account takeover warrant** can result in loss or damage to data unless justified and proportionate.

119. Under a **data disruption warrant**, the AFP and the ACIC may be authorised to access and modify data associated with a person's financial accounts (such as bank account credentials) where doing so will not cause a permanent loss of money. The ability to interact with financial data will be critical for determining the scope of the offending, and for linking individuals to the money trails that follow criminal activity. The Bill expressly prohibits disruption activity from causing a person to suffer a permanent loss of money, digital currency or property (other than data). Any activity resulting in the seizure of money or property by law enforcement remains governed by existing legislation, such as the *Proceeds of Crimes Act 2002*.

Restoration of access to online account

120. There are additional protections in place to minimise the impact of **account takeover warrants** on persons who are using an online account lawfully. Where an account takeover warrant ceases to be in force (either by expiry or revocation), and it is lawful for the account holder to operate the account, law enforcement must take all reasonable steps to ensure that the account holder is able to operate the account. For example, restoration of an account may be effected by changing the account credentials back to what they originally were before the account was taken over.

Information security

121. Each of the three warrant frameworks in the Bill contain measures governing security requirements and record-keeping obligations for information gathered. An overview of these measures is provided below.

Use and disclosure

122. Information collected under these warrants will be subject to strict protections. It will be an offence to disclose this protected information except in limited circumstances. The maximum penalty for the offence is two years imprisonment or 10 years if the disclosure endangers the health or safety of any person or prejudices an investigation into an offence.

123. There are similar purposes for which information obtained under a **data disruption warrant** and information obtained under an **account takeover warrant** may be used, including the investigation of a relevant offence or the making of a decision about whether or not to bring a prosecution for a relevant offence.

124. The Bill has a different approach to information collected under a **network activity warrant**. That information is for intelligence purposes, and will not be permitted to be used in evidence in criminal proceedings, other than for a contravention of the secrecy provisions that apply to this intelligence. However, this information may be the subject of derivative use, allowing it to be cited in an affidavit on application for another investigatory power (which will themselves contain protections on information gathered). This will assist agencies in deploying more sensitive capabilities with confidence that they would not be admissible in court. This information may also be shared where relevant to the AFP and the ACIC's functions. The AFP's functions include providing police services to assist or cooperate with foreign law enforcement or intelligence agencies, allowing network activity warrant information to be used or disclosed for this purpose.

125. Information collected under each of these powers may also be shared to an intelligence agency if the information relates to a matter that is relevant to the agency's official functions. Information may also be shared with the Ombudsman and the IGIS, and between those agencies to allow them to fulfil their oversight responsibilities in relation to the powers in the Bill.

Record-keeping and destruction requirements

126. The chief officer of the AFP or the ACIC must ensure that information obtained under each of these powers is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report. Records must be destroyed as soon as practicable if the material is no longer required, and at most within five years of the material no longer being required. This is consistent with existing record-keeping and destruction obligations in the SD Act. Requiring the security and destruction of records ensures that the private data of individuals subject to a warrant is only handled by those with a legitimate need for access, and is not kept in perpetuity where there is not a legitimate reason for doing so. These are the same obligations that apply in relation to existing powers in the SD Act.

Protection of sensitive capability and methodology

127. A court is empowered to make orders preventing the release of sensitive technologies and methods relating to each of these powers into the public domain. This recognises that the disclosure of such sensitive information would be inherently harmful to future capabilities and investigations. Law enforcement capabilities are fundamental to ongoing investigations and their ability to protect essential public interests, including national security and public safety. Before making such an order, the public interest in protecting sensitive operational and capability information may be weighed against the defendant's right to a fair trial and other public interests.

Accountability and transparency

Reporting

128. The Bill includes robust reporting requirements to provide assurance to Parliament and the Australian community that the powers are being used only as required. Agencies will be required to provide a report to the Minister for Home Affairs on the high-level details and outcome of each **data disruption warrant** and **network activity warrant** as soon as practicable after it ceases to be in force. Agencies will also be required to make six-monthly reports to the Commonwealth Ombudsman and the Minister for Home Affairs on the use of **account takeover warrants** during that period. Statistics on the use of each of these warrants will be published in annual reports to the Minister for Home Affairs to be tabled in Parliament.

Oversight

129. Agencies must also keep records about each of these warrants, including in relation to decisions to grant, refuse, or revoke warrants and how the information in the warrant has been communicated. This information will also allow the Commonwealth Ombudsman to review the performance of **data disruption warrants** and **account takeover warrants** through an inspection and determine compliance with law. The Ombudsman will report the results of their inspections to the Minister for Home Affairs bi-annually. The Minister must table the Ombudsman reports in Parliament.

130. The IGIS will have oversight responsibility for **network activity warrants** given their nature as an intelligence collection tool. In recognition of the network activity warrant's departure from traditional evidence gathering powers, the IGIS will be responsible for overseeing network activity warrants. Given the IGIS' role in reviewing the activities of the Australian Intelligence Community, whose powers and functions relate to intelligence collection, the IGIS is appropriately placed to oversight the use of network activity warrants which are directed at the collection of criminal intelligence by the AFP and the ACIC. This is consistent with (but separate to) the Richardson review's finding that it is not necessary for the IGIS to oversee the AFP's existing powers.

131. The IGIS' oversight of network activity warrants will include conducting inspections, inquiries and investigations into complaints. The IGIS will review the activities of the AFP and the ACIC in relation to

network activity warrants for legality, propriety and consistency with human rights. The IGIS' annual report must include the Inspector-General's comments on any inspection conducted.

Impact on industry

132. The Bill is focused on enhancing the ability of the AFP and the ACIC to use their capabilities as opposed to imposing any new obligations on the technology industry. The powers are targeted at devices, that is, they are not powers enabling the collection of information over Australia's telecommunications networks. The Bill empowers law enforcement officers to employ techniques on devices. These techniques can involve the AFP or the ACIC using a telecommunications facility operated or provided by a carrier in the course of target devices, but this will not necessarily involve any action by a carrier. The Bill contains a number of protections that seek to minimise any negative impact that the exercise of the new powers may have on members of the technology industry and the legitimate users of devices, including limitations on interference and causing damage (as discussed above).

133. In addition to these safeguards, the powers in the Bill are supported by compensation arrangements that provide that the Commonwealth is liable to compensate a person who has suffered loss of or serious damage to property or personal injury as a result of the execution of the warrant. This does not apply where a person has suffered the loss, damage or injury as a result of engaging in criminal activity. Compensation may be agreed to between the Commonwealth and the person, or in default of agreement, as determined by action against the Commonwealth in a court of appropriate jurisdiction.

Industry assistance

134. Should the AFP or the ACIC wish to seek assistance from industry to support the new powers in the Bill, they must do so through existing mechanisms.

135. For example, agencies can seek assistance from carriers and carriage service providers where reasonably necessary under section 313 of the Telecommunications Act.

136. In addition, the industry assistance framework in Part 15 of the Telecommunications Act (introduced by the Assistance and Access Act) is another mechanism through which agencies can see assistance. The framework allows Australia's law enforcement, security and intelligence agencies to request or compel assistance from communications providers where there is a technological obstacle to investigations and operations. Industry assistance can be sought by the AFP or the ACIC for the relevant objective of enforcing the criminal law, so far as it relates to *serious offences*, that is, offences punishable by a maximum term of imprisonment of three years or more. This provides a structure through which industry can assist agencies in carrying out their lawful functions and protecting the community.

137. The industry assistance framework may, in appropriate circumstances, be used to support the powers in the Bill, just as it can be used to support other law enforcement powers, such as those in the TIA Act. For example, the AFP or the ACIC may request a communications provider to delete an activity log in customers' devices relating to the execution of a network activity warrant to conceal access under the warrant.

138. Use of the industry assistance framework will not replace the need to meet the thresholds established by the Bill for the exercise of the powers. Instead, the framework can be used, in appropriate circumstances, to seek technical assistance to facilitate agencies' exercise of the new powers. The industry assistance framework is supported by strong safeguards and limitations to protect the commercial interests of providers, and the privacy of individuals. These protections will also continue to apply if the industry assistance framework is used to support the powers in the Bill. Importantly, the industry assistance framework expressly prohibits any request that would, at a systemic level, undermine cyber security or make data less secure. This would rule out, for example, requesting a provider to give assistance in support of a data disruption warrant that would involve implementing systemic weaknesses into electronic services to frustrate criminal offending.

Conclusion

139. The Home Affairs Portfolio recognises the importance of the Committee's review of the Bill, and hopes that this submission assists the Committee in understanding the purpose and intent of the proposed measures in the Bill. The Bill will substantially boost the powers of the AFP and the ACIC to combat cyber enabled crime.

140. Cyber-enabled crime, often enabled by the dark web and anonymising technologies, presents a direct challenge to community safety and the rule of law. On the dark web, criminals are able to carry out the most serious of crimes, including exchanging child abuse material, planning terrorist attacks and buying and selling illegal drugs and weapons, with a significantly lower risk of identification and apprehension. The growing use of such technologies is increasingly inhibiting agencies' ability to investigate and prosecute serious crime, and protect our community.

141. The Bill responds directly to these challenges by introducing three key measures to enhance the AFP and the ACIC's ability to identify and disrupt serious criminal activity online. Specifically the Bill enhances our agencies ability to:

- identify targets amidst the mass of information online by introducing a new network activity warrant to collect intelligence on criminal networks operating online
- disrupt criminal activity by introducing a data disruption warrant enabling the modification and deletion of data to protect victims and prevent future crimes, and
- gather evidence on criminals and their associates by introducing an account takeover warrant to allow for the control of a person's online account.

142. The Bill also makes minor amendments to the controlled operations framework in the Crimes Act to improve the capacity for agencies to conduct controlled operations online. In particular, the Bill amends the requirement for illicit goods, including content such as child abuse material, to be under the control of law enforcement at the conclusion of an online controlled operation.

143. The Bill contains the necessary safeguards, including oversight mechanisms and controls on the use of information to ensure that the AFP and the ACIC use the powers in a targeted and proportionate manner to minimise the potential impact on legitimate users of online platforms.

144. Australians do not accept serious crime in our communities, and neither can we continue to accept it online. Our laws must keep pace with technology if our agencies are to continue to do the job we expect of them — to keep Australians safe. The Bill supports this goal by providing the AFP and the ACIC with the powers they need to identify and disrupt threats to the safety of Australians, particularly the most vulnerable members of our community.