Australian Government

Department of Home Affairs

Parliamentary Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Parliamentary Joint Committee on Intelligence and Security

Table of Contents

Introduction

1. The Home Affairs Portfolio welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security's Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill). The submission is made on behalf of the Department of Home Affairs (Home Affairs), the Australian Federal Police (AFP), the Australian Security Intelligence Organisation (ASIO) and the Australian Criminal Intelligence Commission (ACIC).
2. The Bill provides a contemporary framework that will allow law enforcement and national security agencies to work in the increasingly complex digital environment. The Bill's measures operate on three key principles:
    1. Lawful, proportionate access to communications is necessary for authorities to effectively investigate crime and safeguard national security in the modern era.
    2. Communications providers supplying services or products in Australia should have an obligation to give *reasonable, proportionate, practical* and *technically feasible* assistance to Australian authorities.
    3. Encryption and other forms of electronic protection are valuable cyber security tools and Government's should not undermine the security of innocent, third parties.
3. The Australian Government (the Government) supports the use of communication technologies that are critical to securing information and communications. Ubiquitous encryption is one such technology that is increasingly relied upon to protect personal, commercial and government information. Encryption is a vital part of internet, computer and data security, supporting Australian economic growth and national security.
4. However, the evolving digital environment presents an increasing challenge for law enforcement and national security agencies. Secure, encrypted communications are being used by terrorist groups and organised criminals to avoid detection and disruption. Over 90 per cent of telecommunications information being lawfully intercepted by the Australian Federal Police now uses some form of encryption. Malicious actors increasingly communicate through secure messaging applications, social media and Voice over Internet Protocol (VoIP) services.
5. The clear fact is that the powers which Parliament, and by extension the Australian public, have considered appropriate to extend to our agencies no longer achieve investigative outcomes as intended. Consequently, the capacity of Australian agencies to detect and disrupt online crime and threats is being seriously compromised.
6. To deal with the impact of encryption, agencies have traditionally relied upon cooperative relationships with industry and other partners. Domestically, these relationships are underpinned by the *Telecommunications Act 1997* (Telecommunications Act), under which Australian telecommunications carriers and carriage service providers have obligations to provide reasonably necessary assistance to authorities. However, changes in technology have restricted the assistance that these traditional providers can reasonably give and agencies increasingly need to rely on other industry partners to provide similar assistance. The entities who form part of the communications supply chain in Australia have drastically changed since the drafting of the Telecommunications Act.
7. The Bill strengthens cooperative relationships with industry by introducing a new framework for assistance, removing the deficiencies and ambiguities associated with the existing regime, introducing new safeguards for assistance and extending the obligations to secure assistance from key companies in the communications supply chain both within and outside Australia (Schedule 1). These amendments will ensure that agencies can leverage the expertise of industry to effectively discharge their existing powers.

8. Domestic and international legal frameworks must keep pace with rapid changes and technology to enable agencies to adapt to the evolving digital environment. The impact and prevalence of encryption in the digital environment has highlighted the legislative limitations which have affected the ability of agencies to access communications for the collection of evidence and intelligence that may help to protect Australians. The Bill addresses these limitations by modernising and enhancing existing search warrant frameworks and alternative collection capabilities such as computer access (Schedules 2, 3, 4 and 5). The Bill allows domestic law enforcement agencies to engage with international partners to combat the global reach of criminals and terrorists.
9. The Government undertook extensive consultation, including a two stage consultation process on the text of the Bill. This process was productive and led to significant amendments that addressed key concerns, and reinforced the policy intent of the Bill. Importantly, the consultation process also allowed the Government to clarify the strong safeguards and limitations in the Bill that ensure that the privacy of Australians is not compromised, the security of digital systems is maintained and agency powers are utilised appropriately.

Background

What is encryption?[1]

10. Encryption is a technically complex, robust and effective means of concealing the contents of communications. Encryption schemes change otherwise intelligible data and content into ciphertext that reveals minimal information about the original form of the data. Generally, the schemes have three components:
    - a key generation algorithm
    - an encryption algorithm, and
    - a decryption algorithm.
11. Message content and an encryption key are put into an encryption algorithm that scrambles the message and returns unintelligible ciphertext. A decryption algorithm then takes this ciphertext and a decryption key and unscrambles the message to allow it to be read in its original form. Different forms of encryption offer different levels of protection, while this submission does not discuss these types in detail, the diversity of encryption schemes is important to note.

Threat environment

12. Australia's ability to harness the potential of digital technologies is dependent on our trust for communications technologies and the internet. Australians rely upon these technologies for banking, shopping, education, health, communications and other key services. The Australian economy is also highly dependent on digital technologies to improve the nation's productivity, competitiveness, and for access to new markets.
13. Yet the evolving digital environment that spurs prosperity also provides criminals with new avenues to commit a range of serious and complex crimes, including terrorism, firearms and drug trafficking, human trafficking and child sexual abuse. Extremist individuals and terrorist organisations are increasingly using social media and other online tools to facilitate and promote their activities.

[1] See 'What is Encryption' in *Decrypting the Encryption Debate: A Framework for Decision Makers* (2018), National Academies of Sciences, Medicine and Engineering, pp. 15-6.

Similarly, online platforms provide unprecedented connection and storage for the easy sharing, promotion and discussion of child sexual abuse material.

14. The use of technology and digital infrastructure by serious and organised crime is considered a key determinant of significant changes in the criminal landscape. Increasingly, criminal activity is assisted by technology either via the online environment or through advances in technological capabilities, such as secure communications. These include, but are not limited to, communication devices with military grade encryption, remote wipe capabilities, duress passwords, and secure cloud-based services. The commercial availability of secure communication platforms and surveillance equipment, such as tracking devices, provides serious and organised crime groups with the means to conceal their criminal activities from law enforcement.

15. The impact of encryption is clear:

    - Over 90 per cent of data being lawfully intercepted by the AFP now uses some form of encryption.
    - Encryption impacts at least nine out of every ten of ASIO's priority cases.
    - ABF activities to disrupt and deter organised criminal activities, such as the importation of drugs and pre-cursor chemicals, often encounters sophisticated methodologies using Information Communications Technology (ICT).
    - It is estimated that by 2020 all electronic communications of investigative value will be encrypted.

16. These statistics illustrate the effect of encryption on a wide array of investigations. The AFP reports that:

    - In July 2017 plans to blow up an Etihad flight from Sydney to Abu Dhabi remained undetected for over four months due to the use of encrypted messaging application Telegram to plan the attack.
    - Convicted terrorist, Hamdi Alqudsi, used encrypted messaging applications to avoid police monitoring as he facilitated the travel of seven Australian foreign fighters to Syria for the purpose of supporting the Islamic State. Since 2016 the AFP has charged a further 15 persons with terrorist related activity that have been using encrypted applications to frustrate traditional lawful surveillance methods.
    - On average 1400 to 1500 parcel post items are intercepted per week coming into Australia containing illicit drugs that are suspected to have been procured via 'darknet' marketplaces that operate over encrypted networks.
    - The AFP has identified a syndicate of 16 participants who, over a period of two and a half years, had arranged for the import of over 500 kilograms of cocaine via encrypted emails connected to encrypted handsets.
    - Since 2015, the AFP's operation KORE has seized over 500 weapons and disrupted planned mass shootings overseas, all linked to encrypted 'darknet' transactions. This operation has also identified the exchange of fraudulent passports, drivers' licences, hacking and hitman services via these encrypted platforms.

17. The ACIC notes that the majority of serious and organised crime activities are enabled, to a large extent, by the use of technology. Using technology to commit crime is also significantly more efficient and less resource intensive than traditional methods of perpetrating crime. For example, high-end encrypted smartphones continue to be preferred by serious and organised crime groups to reduce visibility of their activities to law enforcement. Multiple outlaw motorcycle gangs and other serious and organised crime groups use encrypted communication devices and software applications as

their primary means of communication, due to the content protection features available on these devices and applications.

18. State and Territory law enforcement have also highlighted the many cases in which encryption and modern communications technologies have defeated or materially frustrated criminal prosecution. A summary of these cases is at **Attachment A.**

19. The market trends that are disrupting lawful collection by Australian agencies are being felt worldwide. A 2017 report by the Center for Strategic and International Studies found that three of the top 12 mobile applications use default end-to-end encryption and that portion of unrecoverable encrypted messages will continue to grow exponentially as the instant and app-based messaging platforms become the dominant providers of global messaging. Instant messaging traffic has been predicted to grow by more than 20 per cent annually through to 2019, doubling to approximately 100 trillion messages per year (that is 274 billion per day).[2]

20. The ready availability of technology to reduce law enforcement visibility of serious and organised crime groups' activities has had an impact on how law enforcement agencies undertake their work. The rapid uptake of new capabilities such as encrypted communication devices and applications will continue to challenge law enforcement in coming years.

21. Law enforcement and national security agencies have the ability to seize devices and access communications such as text messages, provided there is a warrant issued by a judge or similar independent authority. However, lawfully intercepted communications are difficult or impossible to decrypt and used operationally. In most instances encryption is incapable of being overcome, limiting the possible avenues for law enforcement to investigate a criminal operation. In some instances, law enforcement agencies may have to employ expensive and time-consuming techniques to unlock a device or read encrypted communications. Not only does this increase the cost of operations, it delays agencies' operations which could substantially raise the risk of harm or loss of life.

22. The Government understands the importance of encryption and other such technologies for protecting the privacy of information and communications. As a result, the Bill cannot be used to create a 'backdoor' to encryption or impact the security of digital systems.

The status quo

A market for insecurity

23. In the absence of legislative solutions and reliable industry assistance, law enforcement and security agencies are turning to third party vendors to identify means of accessing encrypted information. For example, the FBI reportedly engaged a third party vendor to unlock the target iPhone in the San Bernardino case. Engaging these third party vendors attracts premium costs, particularly as agencies are competing for their services with malicious actors and manufacturers providing rewards.

24. Those intent on using encryption for criminal purposes or to perpetuate national security threats are increasingly conscious of publicity (including that presented through criminal prosecutions) about vulnerabilities in encryption and will actively seek out those platforms and applications where such weaknesses are not reported. In the absence of active cooperation from primary vendors, the services are of 'grey hats' vendors can become the only viable technical solution. This is a less than ideal situation, as it assists in perpetuating a cottage industry that includes vendors willing to provide capabilities to any nation state or other actor regardless of intended use.

[2] See *The Effect of Encryption on Lawful Access to Communications and Data* (February 2017), Center for Independent Studies, p. 6

25. The Bill intends to strengthen cooperative working relationships between agencies and primary manufacturers and industry to reduce the reliance on a grey hat community. This will in turn increase transparency and accountability between industry and government. Schedule 1 is not seeking is not seeking for primary manufacturers and industry to provide the functionality of the grey hat community, but rather that industry proactively identifies opportunities to address current content loss through encryption.

Current industry assistance

26. Currently, carriers, carriage service providers and carriage service intermediaries must, in connection with the operation of telecommunications networks or facilities, give officers and authorities of the Commonwealth and of the States and Territories such help as is 'reasonably necessary for the enforcement of the domestic and foreign criminal law, protection of the public revenue and the safeguarding of national security'.[3]

27. While this obligation has allowed agencies to build productive relationships with domestic industry, it has significant shortcomings. Notably, the scope of providers it captures is an outdated reflection of the telecommunications industry. It fails to acknowledge the increasing importance of over-the-top providers, offshore companies and the multiple contractors and subcontractors that form an integral part of the supply of communications in Australia. Despite the increasing diversity of the communications market, the majority of obligations for assistance sit with a select number of traditional companies. The playing field is not level.

28. Section 313 of the Telecommunications Act is also ambiguous – the scope of what constitutes 'reasonably necessary' help is undefined and the section does not clearly set out what type of assistance may be required. This has led to uncertainty in its application and, in many cases, has meant that law enforcement has not been able to receive the help needed. For example, providers routinely assess reasonableness based on the type of criminality being investigated. As a result, providers have been willing to assist for a terrorism incident but, in some instances, have not afforded the necessary assistance in relation to money laundering or a substantial drug importation.

29. The lack of clearly defined obligations has also meant that critical assistance sought under the authority of section 313 has been neglected in favour of more explicit requirements like the maintenance of traditional interception capabilities.[4] Ambiguity introduces delays into the assistance process as providers (understandably) want to be clear on the legality of the help they provide. Providers have also expressed concern that the lack of definition in current assistance provisions creates uncertainty about what activities are protected by civil immunities.[5]

30. Notably, the existing framework does not list central safeguards, like a prohibition against building systemic weaknesses or vulnerabilities. These protections are instead collapsed into the concept of 'reasonably necessary' assistance. Schedule 1 of the Bill significantly improves the process, certainty and safeguards associated with domestic industry assistance and establishes an expectation that all key persons supplying communications services and devices in Australia, domestic or offshore, have an obligation to help authorities where it is reasonable, proportionate, technically feasible and practical to do so. The Bill also includes provisions to ensure providers are not subject to civil suits for action taken in accordance with a request or notice under Schedule 1.

31. Section 313 will operate concurrently with the proposed powers in Schedule 1 to ensure the smooth delivery of industry assistance from Australian carriers and carriage service providers.

[3] See section 313 of the *Telecommunications Act 1997*
[4] See Part 5-3 of the *Telecommunications (Interception and Access) Act 1979*
[5] Section 314 of the *Telecommunications Act 1979*.

The exceptional access debate

32. Legislative responses to the problems associated with encryption often focus on laws that mandate government access to encrypted information (often referred to as 'exceptional access'). This is notably different from arguments for and against 'access' itself - it is widely recognised that law enforcement should have the capacity to execute lawful surveillance consistent with the rule of law.[6] Instead, debate focuses on whether law enforcement should have the exclusive capacity to view otherwise secure information to aid legitimate evidence and intelligence collection functions.

33. An acceptable policy outcome would be encrypted systems that facilitate lawful access to communications but preserve the security of services and devices, ensuring that malicious actors cannot infiltrate systems. The legislative options that would facilitate exceptional access are varied but largely centre on laws that would require a device vendor or service provider to adopt specific technologies or remedies that provide government with access to unencrypted content.[7] For example, legislation could set out requirements for providers to:

    - Design their systems in a way that creates a unique law enforcement 'key' to selectively access encrypted data ('key escrow').
    - Build devices in a particular way that would store a key on the hardware itself.
    - Retain the capability to unlock devices when requested.
    - Limit the length of their encryption keys, weakening their complexity and increasing the chance that agencies could 'brute force' access by trying all possible key combinations.

34. Critics of the above argue that it is impossible to adopt any of the above measures without introducing weaknesses that malicious actors can exploit. The logic follows that the creation of additional keys and other means of access for law enforcement creates new points in a system's security that may be compromised. Home Affairs received many submissions during public consultation that expressed similar concerns.

35. The Assistance and Access Bill **does not** adopt any of these approaches.

36. Instead, it establishes a technologically neutral framework for industry and government to work together towards access solutions with entrenched security protections. The new arrangements put in place by the Bill will allow, where possible, Australian authorities exceptional access to encrypted communications in circumstances negotiated by industry and Government. Importantly, any arrangement that would introduce weaknesses and make innocent, third-party communications vulnerable would be in contravention of the Bill's legal safeguards.

International context

37. On 26 June 2017, at the Five Country Ministerial Meeting between Australia, Canada, New Zealand, the United Kingdom and the United States ('five country partners') in Ottawa, Ministers and Attorneys-General discussed the shared challenge of encryption and noted that encryption can severely undermine public safety efforts by impeding lawful access to the content of communications during investigations into serious crimes.

38. To address these issues, the five country partners agreed to a Statement of Principles on Access to Evidence and Encryption in August 2018 (**Attachment B**) that sets out a framework for discussion

[6] See 'Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications' (2015), p. 1.
[7] See 'Options for Accessing Plaintext' in *Decryption the Encryption Debate: A Framework for Decision Makers* (2018), National Academies of Sciences, Medicine and Engineering

with industry on resolving the challenges to lawful access posed by encryption, while respecting human rights and fundamental freedoms.

39. The Bill ensures Australia implements the following key principles in the statement:

- Developing a mutual responsibility between Governments and industry to ensure law enforcement agencies have access to lawfully obtained content, and
- Ensuring that assistance requested from providers is underpinned by the rule of law and due process protections.

40. A number of overseas jurisdictions have laws directed at securing industry assistance, most notably:

- **The United Kingdom:** In 2016, the UK Parliament passed the Investigatory Powers Act 2016 (UK IPA). The UK IPA is an extensive rewrite of interception and surveillance powers within the UK. It also enables a Secretary of State's to issue 'technical capability notices' requiring telecommunications operators to maintain the capability to provide data in an intelligible format (i.e. without encryption) where it is proportionate, technically feasible and reasonably practicable to do so. The UK IPA differs from the powers in Schedule 1 of the Bill in several critical ways (including by allowing the construction of decryption capabilities) and is, in many respects, a more expansive regime. A detailed comparison is made between the Schedule 1 of the Bill and the UK IPA below.
- **New Zealand:** New Zealand has imposed a 'duty to assist' with decrypting telecommunications where the person has provided the encryption. The relevant legislation, *The Telecommunications (Interception Capability and Security) Act 2013*, does not appear to discriminate between different forms of encryption, including end-to-end encryption. Home Affairs understands that this duty allows the New Zealand Government to compel assistance from service providers, whether or not that provider is located in New Zealand, in response to a warrant provided by a 'surveillance agency'.
- **France:** French law requires operators to assist agencies investigating a terrorist incident or undertaking criminal investigations. Laws passed in 2016 significantly increased the financial penalties for refusals to provide technical assistance and the French Criminal Code imposes obligations on persons 'having a key to decipher an encrypted message which may have been used to prepare, facilitate or commit a felony or a misdemeanour'.
- **European Union:** Work is being undertaken to update the EU's regulatory framework to account for over-the-top services that send content to end users over public internet. The 'Proposed Directive establishing the European Electronic Communications Code' will bring these providers into the regulatory framework and ensure they are subject to the same obligations as traditional telecommunication operators.
- **United States:** The All Writs Act of 1789 gives United States federal judges the power to issue orders compelling people to do things within the limits of their jurisdiction. The Act operates as a court order and has typically only been used in cases where no other clear law applies, for instance when authorities need access to password-protected devices. The US Department of Justice invoked the Act in 2016 to compel Apple to facilitate access to the iPhone of the person responsible for the San Bernardino shootings. Home Affairs understands that the legal issues associated with the case prompted the F.B.I to seek access solutions elsewhere.

Key elements of the Bill

Summary

41. The Bill addresses the challenges associated with the rapid evolution of communications technology, the increasing use of encryption and strengthens the ability of agencies to access 'content in the clear'. The measures in the Bill represent a holistic answer to the impact of encryption, either by working with industry to overcome failures in traditional forms of surveillance or by strengthening avenues to access data in an unencrypted state. Importantly, no measure in the Bill makes forms of encryption or other methods of electronic protection less secure.

42. The Bill's five schedules facilitate access to content in the clear in three distinct ways:

    1. **Working with industry to access encrypted content without undermining security:** Schedule 1 enhances the existing obligations of domestic communications providers to aid agency investigations and, for the first time, extends assistance obligations to offshore providers. The communications industry designs, builds and operates the services and devices used to perpetrate crime and avoid detection, and persons throughout the communications supply chain are in a unique position to assist agencies with the effective execution of lawful and warranted surveillance activities.
    2. **Warranted computer surveillance:** Schedule 2 establishes a new computer access warrant regime for law enforcement and enhances ASIO's existing computer access powers. These changes modernise the evidence and intelligence collection capabilities of Australia's key agencies and will facilitate the lawful collection of data in a more accessible state.
    3. **Enhancing existing channels of access to data:** Schedules 3, 4 and 5 augment the ability of agencies to access unencrypted data by strengthening search and seizure powers for computers (including mobile devices).

43. These three aspects of the Bill are explained in detail below.

Working with industry to access encrypted content without undermining security - Schedule 1

Purpose

44. The industry assistance arrangements in Schedule 1 of the Bill were built around the key principles discussed above, namely:

    - Lawful, proportionate access to communications is necessary for authorities to effectively investigate crime and safeguard national security in the modern era.
    - Communications providers supplying services or productions in Australia have an obligation to give *reasonable, proportionate, practicable* and *technically feasible* assistance to Australian authorities.
    - Encryption and other forms of electronic protection are valuable cyber security tools and Government's should not undermine the security of innocent, third parties.

45. This Schedule allows agencies to request that providers give bounded support to address operational needs, including the need to collect and scrutinise target communications. The exact technical means of this assistance are not specified (although broader categories of assistance are listed in proposed section 317E for reference and transparency) and any assistance that would

undermine the security of communications is prohibited. This allows industry and Government to partner in determining the most suitable means of accessing encrypted information. This approach was adopted for several reasons:

- The Government, and its agencies, want to work together with industry to address investigative problems - not set a pre-existing solution that may have ramifications for digital security.
- Providers are best placed to understand their services and the technology they work with and are more aware of the technical methods to assist agencies that will not compromise the security of their systems.
- Communications providers operate in a diverse and global industry. The Government does not want to mandate particular methods of encryption that may force industry to adopt different standards in Australia and overseas and acknowledges the practical difficulties of doing so.
- Prescriptive and technologically exact legislation is limiting and not a suitable form of regulation in a rapidly changing industry.
    - Investigations into serious crimes and threats are complex. The nature of industry assistance will turn on the circumstances of each investigation and the assistance provided, subject to global safeguards, must be capable of flexible application.
    - Legislation that imposes requirements on a constantly evolving communications industry must remain technologically neutral if it is to remain effective.

46. Schedule 1 reflects a more nuanced and reasonable approach to the role of industry in aiding law enforcement access to encrypted content that avoids the security risks inherent in mandatory laws for exceptional access.

Overview

47. Schedule 1 establishes three new powers for Australia's key law enforcement, security and intelligence agencies to work with identified entities in the communications supply chain, defined in proposed section 317C as *designated communications providers* (DCP). As noted above, the intent of these powers is to secure critical assistance from DCPs relevant to the Australian market and to establish a legal basis for them to help law enforcement discharge their existing, targeted, surveillance powers. The three specific powers are:
    1. **Technical Assistance Requests (Division 2):** allow agencies to request voluntary assistance from providers.
    2. **Technical Assistance Notices (Division 3):** allow agencies to require a DCP to provide assistance of a kind that they are already capable of providing.
    3. **Technical Capability Notices (Division 4)**: allow Australia's first law-officer, the Attorney-General, to require a DCP to build a new capability to assist agencies.
48. **The types of assistance** that may be requested or required vary between each power but are broadly categorised under the definition of *listed act or thing* in proposed section 317E.
49. **Decision-making** is reserved to the Attorney-General or senior officials of Australia's key law enforcement and security agencies, and requirements set must be reasonable, proportionate, practical and technically feasible. Broader interests, like privacy and cyber security, must also be taken into account.

50. **Compulsory orders are reserved for established agencies:** Only the limited agencies able to apply for interception warrants under the *Telecommunications (Interception and Access) Act 1979* (TIA Act), or the Attorney-General, are able to issue notices for compulsory assistance.

51. **Use and disclosure:** Proposed section 317ZF creates an offence of unauthorised disclosure that protects information about, or received through, the use of these powers. Exceptions to the offence are created for legal proceedings, administration and oversight purposes, among other things.

52. **Systemic weaknesses:** Proposed section 317ZG stipulates that compulsory powers cannot require a DCP to build or implement systemic weaknesses that undermine electronic protections or prevent them from rectifying a weakness. Consistent with the long-standing principle that authorities should be allowed to access targeted communications on a lawful basis, this prohibition does not limit access to a particular device or service where there is lawful authority to do so. A third party expert may be enlisted to scrutinise whether a technical capability notice (TCN) would create a systemic weakness or vulnerability.

53. **No removal or weakening:** Technical capability notices cannot be used to build a capability that removes a form of electronic protection, build a decryption capability or a capability that renders systemic methods of encryption or authentication less effective.

54. **Requirement for warrants and authorisations:** Proposed section 317ZH restricts the ability of the new powers in Schedule 1 to act in replacement of existing warrants or authorisations. This means that, whether a DCP is located within or outside of Australia, agencies cannot use the new regime in lieu of a warrant to collect information of a kind for which a warrant would be required. The access to target communications would still require an underlying judicial authorisation, or equivalent warrant, via statutory authority. The existing territorial limitations of warrants and authorisations still apply.

55. **Costs and immunities**: Companies that assist agencies will have their costs covered, and will receive immunity from civil liability. Industry should not be penalised for aiding legitimate and important investigations.

56. **Enforcement:** In the case of non-compliance, the Commonwealth Communications Access Co-ordinator (CAC) can apply to the Federal Court for several remedies, including injunctions, enforceable undertakings or civil penalties.

Designated Communications Providers

57. The new framework in Schedule 1 compliments and builds upon the obligations on domestic carriers and carriage service providers to provide reasonably necessary assistance under section 313 of the Telecommunications Act. Since the enactment of that obligation the communications industry has become increasingly globalised, and the services and devices which Australians use increasingly operate without direct carrier control through offshore providers. A report from the Center for Strategic and Independent Studies found that foreign mobile messaging applications like WhatsApp, Facebook Messenger, iMessage, Telegram, Skype and Line are quickly becoming the chief mode of communication around the world.[8] Internet and modern communications technologies allow almost anyone to establish and operate messaging services from anywhere in the world with relatively little cost.

58. At present, a wide range of entities who form critical parts of the communications supply chain in Australia have no obligation to assist Australian authorities, even where their services are being used to conduct illegal activity and harm Australians. Over-the-top electronic services, like WhatsApp, are increasingly the default method of communications yet criminals may operate with near impunity through these applications simply because they are located offshore. While many

[8] Center for Independent Studies, *The Effect of Encryption on Lawful Access to Communications and Data* (February 2017), p. 6

offshore providers give valuable assistance to Australian authorities, the existing system largely operates on goodwill.

59. The new definition of designated communications providers (DCP) creates 15 categories of entities that may be asked to assist Australian authorities. This reflects the globalised, multi-layered communications industry and the types of entities that could meaningfully assist law enforcement and national security agencies. It is crafted in technologically neutral language to allow for new types of entities and technologies to fall within its scope as the communications industry evolves.

60. The definition also accounts for the range of providers who form part of the encryption landscape and who are in a position to assist with access to encrypted content without undermining the security of a service or device. If agencies are able to secure assistance from a wider range of providers the burden on any one provider is reduced. In the absence of mandating certain forms of encryption and 'backdoors', collective assistance across the communications supply chain is critical to enabling access to encrypted content. **Attachment C** illustrates the range of entities within the encryption landscape.

61. It is not uncommon for several entities to be involved in providing an electronic service to a customer. For instance, the transmission of a single communication to an end-user may involve:

    - an offshore electronic service provider, like Facebook
    - a Content Delivery Network to facilitate the supply of the communication in the given geographic location
    - the NBN as the dominant fixed line network in Australia
    - an Australian telecommunications carrier like Telstra
    - a contractor of a carrier that maintains a relevant part of the carrier's network
    - a company that develops software that facilitates the transmission of electronic services in the network, or
    - a data centre operator that becomes the physical location of information relevant to the electronic service.

62. Every type of DCP listed in items 1-15 of proposed section 317C may be, and often is, an integral part of the communications supply chain and many may be involved in the transmission of a single electronic service. While an investigation may not require assistance from every single type of DCP, depending on the scenario, one or more may be in a position to play a critical role in facilitating lawful access to a communication. In every instance compulsory assistance from a DCP will be subject to thresholds of reasonableness, proportionality, practicality and technical feasibility.

63. Body corporates, as well as individuals, may be designated communications providers. Restricting the definition of DCP to larger, more established companies ignores the reality of criminal activity. The proposed definition reflects the flexibility and ease of entrance into the communications market and accounts for circumstances where an individual may establish small-scale services that criminals migrate to because of a perceived lack of cooperation. However, individuals within body corporates are not captured and it is not the intent of the Bill to issue requests or notices on individuals within an organisation without that organisation's knowledge. Provisions in proposed sections 317HAA, 317MAA and 317TAA require that authorities support smaller providers who may be subject to a request or notice to ensure that they understand their obligations.

64. Assistance, and immunities connected to assistance, must be related to the *eligible activities* of a provider, ensuring that a DCP cannot be asked to assist with things that are not tied to its

communications functions.[9] For example, a computer parts manufacturer that provides full disk encryption could not be required to provide access to the contents of a device as it not relevant to their communications functions. Importantly, each eligible activity must have a jurisdictional nexus to Australia which grounds the assistance to matters or activities within Australia.

65. **Change from consultations**: In response to industry feedback, comments from the Law Council of Australia and the Australian Human Rights Commission, the issuer of a notice or request must now clearly explain the obligations of the relevant DCP. This will support smaller DCPs subject to a notice by either making explicit that compliance is voluntary or clarifying the nature and extent of a notice's requirements.

Things that may be requested

66. The things that may be listed on a *technical assistance request* (TAR), *technical assistance notice* (TAN) and *technical capability notice* (TCN) must be in reference to the matters specified in proposed section 317E "Listed acts or things".

67. Items 317E(1)(a) – (j) were developed in close consultation with agencies and, to some extent, reflect the nature of assistance received from domestic carriers and carriage service providers under obligations for reasonably necessary assistance in section 313 of the Telecommunications Act.

68. The items are broadly cast in order to be responsive to operational needs and to reflect the rapidly changing capabilities of the communications industry. Regulation in such a dynamic and future-orientated industry quickly becomes overly burdensome, obsolete and ineffective if prescriptive requirements are established in the legislation. Instead, the Bill adopts global safeguards that can be appropriately applied to given circumstances to ensure things required of DCPs are reasonable and proportionate and that the integrity of private information and security of systems is protected.

69. Proposed section 317E operates differently between a TAR, TAN and TCN:

    - Reflecting the voluntary nature of a TAR, the list is non-exhaustive and indicates the kinds of assistance that may be included on a request and the kinds of acts that may attract the immunities under a TAR.
    - Where proposed section 317E relates to compulsory requests for assistance that a DCP is **already capable** of providing, the list is non-exhaustive and is indicative of the kind of assistance that may be listed in a request or notice. Both TANs and TCNs can request assistance that a provider is already capable of providing.
    - Proposed section 317E is exhaustively applied in relation to new capabilities required under a TCN. Further, a TCN cannot require a DCP to do a thing under proposed paragraph 317E(1)(a), which provides for the removal of electronic protection. That is, a TCN is **unable** to require that a DCP build a capability to remove a form of electronic protection, like password rate limits or end-to-end encryption**.**

70. The selective operation of proposed section 317E reflects the relative burden on the DCP subject to the requests.

    - A DCP is under no obligation to action a voluntary request for assistance under a TAR and agencies are already in a position to informally request assistance of this type.
    - Where a TAN or TCN requires a DCP to do a thing it is **already capable of doing**, the DCP is taken to have the functionality to action the notice because of its existing business requirements. For example, if a TAN was issued and, consistent with proposed paragraph

[9] For 'eligible activities' see proposed section 317C.

317E(1)(a), required a DCP to remove a form of electronic protection (like encryption) applied to communications already intercepted under warrant, that DCP must already be able to decrypt the communication in question. There are many reasons a DCP would have this capability. For instance, the ability to analyse and view content transmitted over messaging services might enable the DCP to sell information on consumer preferences to advertising firms who can, in turn, selectively advertise to the user. If the service of the DCP was end-to-end encrypted, and the provider had no existing capability to decrypt the content, then a TAN could not be issued by the agency head.

- New capabilities required by a TCN are ancillary to business requirements and can go beyond the provider's own needs. It is therefore appropriate that the matters for which new capabilities can be built are limited in the legislation and subject to ongoing Parliamentary scrutiny. Proposed subsection 317T(6) of the legislation allows the Minister to make a legislative instrument (tabled in Parliament) listing items additional to what is already in proposed section 317E for which capabilities can be built. However, this determination making powers is subject to conditions and the Minister must have regard to a number of interests, like the impact on DCPs. To meet these conditions consultation with industry would be expected.

71. A full explanation of the items in proposed paragraphs 317E(1)(a) –(j) is listed in the Explanatory Memorandum to the Bill. Examples of activities that may be requested under each item can be found at **Attachments D and E.**

72. **Change from consultations:** In response to industry feedback, Home Affairs added proposed subsection 317E(2) to ensure that if a DCP is asked to conceal legitimate surveillance activities of an agency, they cannot be asked to make false or misleading statements or engage in dishonest conduct.

Further restrictions

73. In addition to not being able to require a DCP to remove a form of electronic protection, a TCN cannot require a DCP to build an interception capability, a delivery capability or a data retention capability. These restrictions are expressed in proposed subsections 317T(8) – (11) of the Bill. Core capabilities like interception or data retention have already been appropriately defined and limited by Parliament and it is not appropriate that a TCN be issued to modify this regime.

74. As highlighted below, the disclosure of communications content or data has not been included in the listed acts or things. The Explanatory Memorandum makes clear that this exclusion, in addition to the prohibition in 317ZH, is designed to ensure that a TAR, TAN or TCN cannot be used as vehicles for the collection of personal information.

A graduated approach to assistance

75. As indicated above, the Bill adopts an incremental approach to industry assistance, allowing agencies to issue three tiers of notice:

    a. **Technical Assistance Requests** (TAR) on a voluntary basis,

    b. **Technical Assistance Notices** (TAN) requiring a DCP do a thing they are already capable of doing, and

    c. **Technical Capability Notices** (TCN) requiring providers to build new capabilities.

76. **Attachment F** illustrates the operation of this graduated industry assistance process.

77. Australian agencies want to engage with industry collaboratively and constructively, and, in many cases, do. The expressed preference of Australian authorities is to work with providers on a

voluntary basis in the first instance. Recognising the value of that assistance, the TAR regime establishes an immunity for help given and allows a basis for agencies to contract commercially for services provided. A DCP that acts in good faith to voluntarily assist Commonwealth, State and Territory agencies should not be subject to civil liability.

78. However, where a DCP would prefer a clear legal obligation to assist, or is unwilling to provide the necessary assistance, coercive powers are available. A TAN or TCN can compel a DCP to do things they are already capable of doing. As discussed above, this type of assistance can be executed through using the capabilities they retain as a result of their business functions and, accordingly, does not require them to do anything extraordinary.

79. Where investigative demands cannot be met by a DCP's existing capabilities, a TCN may be issued to require the construction of a new capability. The fact that these activities go beyond business needs and may build functions dedicated to legitimate law enforcement or security purposes is reflected in the limitation, oversight and consultation arrangements associated with a TCN.

80. Compliance with a TAN or TCN attracts similar immunities to those available under a TAR (see proposed section 317ZJ).

81. The agencies allowed to issue each of these powers, the purposes for which they may be issued, and associated consultation requirements varies to reflect the scale of the obligations under which a DCP may be placed.

Relevant Agencies

Technical Assistance Requests

82. The TARs in Division 2 of the Bill allows select agencies to seek voluntary help from a DCP. In addition to interception agencies listed under the TIA Act, the Australia Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS) and the Australian Signals Directorate (ASD) can issue a TAR.

83. The inclusion of intelligence agencies ASIS and ASD in the TAR scheme is appropriate due to the voluntary nature of the requests. Consistent with Australia's broader legislative framework for intelligence agencies, these agencies are not able to issue coercive notices but will be empowered to bestow immunities on DCPs that assist them with the performance of their proper functions and in connection with the eligible activities of the DCP.

84. The extension of immunities for voluntary actions is civil only. This is more limited in scope than the civil and criminal immunity bestowed upon entities acting in support of these agencies by section 14 of the *Intelligence Services Act 2001* and is consistent with the immunities extended to carriers and carriage service providers that assist authorities under section 313 of the Telecommunications Act.

85. **Change from consultations:** Proposed section 317HAA was added to require explicit advice on the voluntary nature of a TAR to accompany any request.

Technical Assistance Notices

86. The TANs in Division 3 of the Bill may be issued directly by the chief-officer of an interception agency, the Director-General of ASIO or their respective senior delegates. The scope of agencies directly empowered by Division 3 is limited to Australia's key law enforcement, anti-corruption and security authorities that already have the ability to apply for, and execute, interception, stored communications and surveillance warrants. It also reflects the agencies able to authorise the disclosure of telecommunications data.

87. The agencies entitled to require assistance is significantly narrower than those captured by the existing 'reasonable assistance obligations' in section 313 of the Telecommunications Act. That section imposes an obligation on carriers and carriage service providers to give "officers and

authorities of the Commonwealth and of States and Territories such as help as is reasonably necessary" for listed purposes. This definition includes a broad swathe of Government entities across Australia, including the Australian Competition and Consumer Commission, sporting integrity bodies and councils. The more limited scope of the agencies empowered to seek assistance from the telecommunications industry under the Bill acknowledges the seriousness of the functions and investigative matters that these agencies deal with and their already sophisticated relationships with key players in the communications industry.

Technical Capability Notices

88. A TCN is issued by the Attorney-General, Australia's first law officer, on behalf of an interception agency or ASIO and in relation to the performance of those agencies under law. As noted below, Ministerial authorisations for administrative decisions of a law enforcement and national security nature is a common feature of the Australian legislative landscape. The Attorney-General, as first law officer, has a traditional role at maintaining the rule of law and, by virtue of recent changes in Government arrangements, more explicit integrity functions. Given the potentially more significant requirements under a TCN, it is appropriate that the ability to direct the construction of a new capability is reserved to the Attorney-General. This power is not delegable.

Purposes for which assistance may be sought

89. All assistance, under any power, must be related to the performance of a relevant agencies' function conferred by, or under, a law of the Commonwealth, State or Territory. The permissible objectives of the powers varies between TARs, TANs and TCNs.

Technical Assistance Notices and Technical Capability Notices

90. A TAN and TCN can be issued for the *relevant objectives* of:

- *Enforcing the criminal law:* This includes criminal investigations and prosecutions, as well as intelligence gathering activities to support prosecutions.
- *Laws imposing pecuniary penalties:* This encompasses civil penalties which are alternatives to criminal prosecutions but, as noted in the Explanatory Memorandum, is not intended to capture small-scale fines.[10] In Commonwealth, State and Territory legislation there are significant civil penalties for serious breaches of the law, including corporate misconduct.
- *Assisting the enforcement of the criminal laws in force in a foreign country:* This allows notices to be issued in support of Australia's international obligations. Australian agencies retain discretion to action these requests and any requests for content or personal information of persons need to be processed through established mechanisms for international cooperation, such as mutual legal assistance or through police-to-police assistance governed by Chapter 4 of the TIA Act.[11]
- *Safeguarding national security:* This reflects the national security function of the listed agencies and the reasons for which ASIO may issue a notice.

91. These relevant objectives are consistent with the reasons for which these same agencies may seek reasonably necessary assistance under section 313 of the *Telecommunications Act 1997* and for which they may authorise the disclosure of telecommunications data under Chapter 4 of the TIA Act. They are not arbitrary or unique purposes and demonstrate the key functions of interception

[10] Explanatory Memorandum p 44.
[11] See Chapter 4, Division 4A. Police-to-police based assistance is subject to a number of safeguards, for example an authorised officer of the AFP must be satisfied that the disclosure is reasonably necessary and appropriate in all the circumstances.

agencies. They have adequately governed the scope of industry assistance to date and largely met the investigative needs of agencies.

92. A fuller explanation of the relevant objectives is set out in page 44 of the Explanatory Memorandum.

Technical Assistance Requests

93. In addition to the above relevant objectives, a TAR can be issued in the interests of Australia's national security, foreign relations or national economic well-being. This reflects the inclusion of ASIS and ASD in the voluntary scheme and mirrors their functions under the *Intelligence Services Act 2001*.

94. **Change from consultation:** Following feedback from the public, protection of the public revenue was removed as a purpose for which a TAR, TAN or TCN may be issued. Although this is an established purpose for which the listed agencies may request assistance under the Telecommunications Act and authorise the disclosure of data, the Home Affairs, in consultation with agencies, considered that removing this purpose would better reflect the mandate of issuing agencies and the purposes for which the measures would be used.

Decision-making criteria and consultation requirements

95. Senior decision-makers within key national security and law enforcement agencies, and the Attorney-General, may exercise the proposed powers in Schedule 1. These decision-makers have an intimate knowledge of the operational challenges Australia's law enforcement faces and, in consultation with industry, are well-placed to determine **reasonable**, **proportionate**, **practical** and **technically feasible** means of achieving set investigative goals. The decision-maker would also have to consider whether the requirements in the notice was in prohibition of proposed section 317ZG.

96. **Attachment G** illustrates the decision-making process for each agency.

Technical Assistance Notices

97. Although there is no explicit consultation process for decision-makers to undergo before issuing a TAN, the practical effect of the legislation would require consultation in most cases before a notice is given to a DCP. A decision-maker must be satisfied that the requirements imposed by a notice are reasonable and proportionate and that compliance with the notice is practicable and technically feasible.

98. As **changes made as a result of public feedback** make clear, in deciding whether a notice is reasonable and proportionate, the decision-maker must have regard to the interests of the relevant DCP, the availability of other means to achieve the notice and the privacy and cybersecurity expectations of Australians (proposed sections 317RA and 317ZAA explains). These changes were made in response to public feedback for further clarification on the standards of reasonableness and proportionality (explained in detail in the Explanatory Memorandum)[12] and suggestions that a TAN should have a consultation component.

99. In most circumstances, it would be expected that a decision-maker would need to consult with the DCP in order to determine if the assistance requested is reasonable, proportionate, practical and technically feasible. For example, noting the technical nature of requirements in a notice, a decision-maker is unlikely to be satisfied of their technical feasibility without having a prior understanding of a DCP's system infrastructure and capabilities – information that would have to be gained through consultation with a DCP.

[12] See Explanatory Memorandum pp. 48-9

100. Given the need for operational flexibility, and the role of TANs in supporting dynamic and ongoing relationships between agencies and DCPs, it is not practical or desirable to establish a minimum consultation period.

Technical Capability Notices

101. The decision to issue a TCN has a mandatory consultation process that can only be waived in situations of urgency, impracticability or where a provider agrees to forgo consultation.

102. Proposed section 317W establishes a process through which the Attorney-General may issue a written notice setting out the proposal and inviting a DCP to make submissions. These consultations must run for at least 28 days.

103. **Changes made as a result of public feedback** allow, upon agreement, for a technical advisor to be appointed to carry out an assessment of whether the TCN would contravene proposed section 317ZG (the prohibition against building or implementing systemic weaknesses into forms of electronic protection). This provision in proposed subsection 317W(7) was introduced following concerns that external experts may need to be consulted to establish the security implications of proposed capabilities. Given the likely sensitivity of capabilities developed under a TCN (including commercially sensitive information), it is not suitable for these proposals to be made public. However, the mechanism allows experts trusted by both industry and Government to undertake a thorough examination of any security impacts where a provider has concerns.

104. The Attorney-General is subject to the same decision-making criteria as a chief-officer or the Director-General, although the thresholds of reasonableness and proportionality would increase with the potential gravity of requirements under a TCN. The Attorney-General's satisfaction of the decision-making criteria will need to be informed by any submissions received from a provider or a technical advisor as part of the consultation process**.**

Systemic weaknesses and vulnerabilities

105. A critical protection of the Bill is the prohibition against a TAN or TCN from building or implementing a "systemic weakness or systemic vulnerability" into a form of electronic protection expressed in proposed section 317ZG. As proposed subsection 317ZG(3) makes clear, this prohibition captures any effort that would make methods of encryption or authentication less effective. It also prohibits the construction of a decryption capability. Electronic protection is an expansive concept and, as the Explanatory Memorandum explains, includes password rate limits on a device. [13]

106. Proposed paragraph 317ZG(1)(b) explicitly prevents a TAN or TCN from preventing a provider from fixing a systemic weakness or vulnerability they have identified in a form of electronic protection. This means that decision-makers cannot request that providers refrain from taking steps to strengthen the security of their systems (for example, by patching a service to fix a flaw) - even if those steps frustrate lawful access to communications.

107. **Significant changes** were made to the original draft of this provision following industry consultation, namely:

- The prohibition was extended to include any weaknesses or vulnerabilities **implemented** as well as **built** into a form of electronic protection.
- The prohibition was extended to all forms of electronic protection.

[13] See explanatory memorandum pp. 67-8

- The prohibition included anything that would make forms of encryption or authentication **less effective** instead of **ineffective**.

108. Importantly, given that a TAN can only require a DCP to do a thing of which they are already capable of doing, these notices have no ability to introduce systemic weaknesses or vulnerabilities into a service or device. Regardless, the prohibition attaches to TANs given their compulsory nature.

109. For the purposes of proposed section 317ZG, the term 'system' encompasses interacting or interdependent items that form a unified whole. The term 'systemic' is intended to refer to matters 'relating to a system' rather than a particular part. However, it is not meant to capture systems isolated entirely to a single device, for example. The purpose and meaning of the provision is clear in the text of the Bill, and is further described in the Explanatory Memorandum to the Bill.

110. Proposed section 317ZG prevents a weakness or vulnerability from being built into a single item (like a target service or device) if it would undermine the security of other, interconnected items. That is, where the weakness in one part of the system would compromise other parts of the system or the system itself. The purpose of the provision is to protect the fundamental security of software and devices and not expose the communications of Australians to hacking. This would capture actions that impact a broader range of devices and services utilised by third parties with no connection to an investigation and for whom law enforcement have no underlying lawful authority by which to access their personal data. Accordingly, weaknesses that impact a range of devices across the market, requirements that force a provider to adopt a less secure means of encryption for its users, or capabilities that introduce a material 'hole' in the devices or services of innocent, third-party users, that could be exploited by malicious actors are covered by the prohibition.

111. The term has also not been exhaustively defined as it is anticipated that it will apply differently between DCPs. Given the significant divergence in the sophistication and complexity of systems, the activities that a DCP may have to undertake to facilitate access to communications will not be uniform. One DCP may be able to meet requirements without creating a systemic weakness, while others may not. Home Affairs considers that the prescriptive, inflexible application of the safeguard carries the risk of creating loop-holes and eroding the global protection it provides.

112. The prohibition, and the meaning of 'systemic', does not extend to access to a particular device or service. As noted in the Explanatory Memorandum:[14]

> "A [TAN] or [TCN] may, notwithstanding new paragraph 317ZG(1)(a), require a provider to enable access to a particular service, particular device or particular item or software, which would not systematically weaken these products across the market."

113. Accordingly, a TAN or TCN may require weaknesses or vulnerabilities to be implemented or built into the service or device of a target. Consistent with the long-standing principle that law enforcement and security agencies should, under warrant, be able to intercept and access target communications industry is expected to assist in these lawful surveillance activities.

114. It is important to note that the mere fact that a capability to selectively assist agencies with access to a target device exists will not necessarily mean that a systemic weakness has been built. The nature and scope of any weakness and vulnerability will turn on the circumstances in question and the degree to which malicious actors are able to exploit the changes required.

115. Significant public feedback focused on this aspect of the Bill and many public comments suggested that the Bill would still allow 'backdoors' or require providers to do things that would undermine the wholesale security of systems. Home Affairs reasserts that the limitation in proposed section 317ZG is global and applies to any compulsory aspects of the Bill, including any activity done consistent with the listed acts or things in items 317(1)(a) –(j). It is intended to prohibit **any** requirements in a notice

[14] Explanatory Memorandum p. 67

that weaken the security of systems or devices beyond the target/s and ensure that the integrity of communications remains intact.

116. If a provider formed an opinion that compliance with a TAN or TCN would create such a weakness or vulnerability, and they informed the decision-maker of this risk, then the decision-maker would need to take that into account when making the decision to issue a notice. If they failed to do so, they would not meet the thresholds of reasonableness or proportionality for issuing a notice. The addition of proposed subsection 317W(7) following public feedback is intended to allow external scrutiny of TCN requirements to ensure requirements do not contravene this prohibition.

117. A DCP that legitimately believes a TAN or TCN would contravene proposed section 317ZG has a firm basis for not complying with the requirements of a notice and could seek judicial review for the administrative decision. The presence of any systemic weakness or vulnerability could then be assessed by a court with the aid of expert testimony.

118. The sophistication of some forms of electronic protection and the wide application of encrypted systems, its inclusion means that, in many instances, Australian agencies will not be able to access encrypted communications as the only realistic means of doing so would make the communications of non-target persons vulnerable. Given the significance of the prohibition on the ability of agencies to access encrypted data, other aspects of the industry assistance framework have been designed to allow enforcement and security officers to effectively and flexibly seek meaningful assistance from the communications industry without affecting cybersecurity.

Restrictions on accessing personal content and data

119. The powers in Schedule 1 are not vehicles for evidence or intelligence collection in their own right and safeguards in the Bill prevent them from being used in substitute of an established warrant.

120. Proposed section 317ZH states that a TAN or TCN has no effect to the extent it requires a DCP to do an act or thing which would require a warrant or authorisation under the TIA Act, the *Surveillance Devices Act 2004* (SD Act), the *Crimes Act 1914*, the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), or the *Intelligence Services Act 2001* (IS Act) or State and Territory surveillance device legislation. While these laws contain the primary means for the relevant agencies to collect evidence or intelligence, in response to industry and public feedback this prohibition was extended to include **any** law of the Commonwealth or a law of a State or Territory. The effect and intent of this limitation is that the new powers in Schedule 1 cannot act as a substitute means of evidence or intelligence collection.

121. This means, for example, that a TAN or TCN cannot require a provider to intercept communications; an interception warrant under the TIA Act would need to be sought. However, a notice may require a provider to assist with the access to information or communications that have been lawfully intercepted.

122. Similarly, a TAN or TCN has no effect to the extent it requires a DCP to use a surveillance device or access data held in a computer where a State or Territory law requires a warrant or authorisation for that use or access.

123. The limitation reinforces a key purpose of the powers in Schedule 1. A TAN and TCN are intended to compliment the execution of warrants or authorisations and will be largely issued to support an underlying instrument that provides the authority to access communications, devices or data. This is why proposed subsections 317ZH(4) – (5) state that the limitation does not prevent a TAN or TCN from requiring a DCP to assist in, or facilitate, giving effect to a warrant or authorisation under a law of the Commonwealth, a State or Territory. Accordingly, the use of a TAN without an associated warrant will be limited to types of assistance that don't directly facilitate access to communications, such as the provision of technical information.

124. **Change from consultation:** This provision makes clear that any and all limitations in the Acts listed above apply to the operation of notices both within and outside Australia. This change was made in response to concerns expressed by offshore providers during industry consultation, who noted that they do not currently form part of Australia's domestic warrant framework. Subsequent changes were made to ensure that a notice cannot require a domestic or offshore provider to produce private communications or data.

125. Importantly, Schedule 1 powers are subject to the inherent territorial limitations of the underlying warrant. Many DCPs, including offshore providers, cannot under existing law be required to execute an interception warrant or disclose telecommunications data under authorisation. The powers in Schedule 1 do nothing to change this – rather, they provide the opportunity for agencies to work with these DCPs to assist in validly executed powers (like a warrant issued to an Australian carrier).

126. This express limitation should be read in connection with the listed acts or things in 317E. That list deliberately does not include the disclosure of personal information as a form of assistance. This intention is noted in the Explanatory Memorandum:[15]

> "technical information does not include telecommunications data such as subscriber details or the source, destination or duration of a communication for which an authorisation under the TIA Act would be required"

And:

> "requirements to decrypt or remove electronic protection under this subsection cannot oblige a provider to furnish the content or metadata of private communications to authorities. Consistent with the restrictions in new section 317ZH, agencies must access communications content and data through establish warrants an authorisations under the TIA Act…"

127. The inability of the new powers in Schedule 1 to act as a substitute for existing warrants or authorisations means that the ability of Australian law enforcement to receive communications content and data from offshore providers, like Facebook, is limited to either voluntary disclosures or information received through the mutual legal assistance process.

Oversight

128. Agencies empowered under Schedule 1 of the Bill are currently subject to extensive oversight by Commonwealth and State Ombudsman, the Inspector-General of Intelligence and Security and law enforcement integrity bodies. These organisations have a wide-remit to investigate agency misconduct and inspect agency records. Notably, legislation does not explicitly provide for these organisations to oversight existing requests for industry assistance tendered under section 313 of the Telecommunications Act.

129. Importantly, these bodies have established inspection and reporting functions in relation to the evidence collection powers that the new framework in Schedule 1 is designed to support.

130. The prohibitions in Schedule 1 limit TARs, TANs and TCNs from being used to intercept communications, authorise the disclosure of data, access stored communications or deploy surveillance devices. They are instruments to secure the necessary assistance from industry to enable agencies to access this information in a digital environment characterised by ubiquitous encryption and increasingly complex communications systems.

[15] See Explanatory Memorandum page 39

131. Accordingly, the existing regimes in the TIA Act and the SD Act establish oversight of the powers that will be used in conjunction with TARs, TANs and TCNs.

The Telecommunications (Interception and Access) Act 1979 (TIA Act)

132. A primary use of these powers will be in support of warrants and authorisations within the TIA Act.

133. The TIA Act and State and Territory legislation currently contains a range of oversight mechanisms in relation to agency use of powers under the TIA Act:

- The Commonwealth Ombudsman oversights Commonwealth agencies in relation to interception of content and all agencies with respect to stored communications.
- The Commonwealth Ombudsman oversights the use of telecommunications data and the data retention regime.
- The Commonwealth Ombudsman prepares annual reports regarding its oversight functions.
- State and Territory Ombudsmen and equivalent authorities oversight telecommunications interception by State and Territory agencies, pursuant to State and Territory legislation (for example, the *Telecommunications (Interception and Access) (New South Wales) Act 1987*).

134. The Commonwealth Ombudsman regularly prepares reports and undertakes inspections regarding agency activities under the TIA Act. These inspections and reports allow the Ombudsman to scrutinise interception warrants and data authorisations that are used in connection with TARs and TANs.

135. Home Affairs also compiles annual reports regarding interception, stored communications access and telecommunications data access, which are tabled in Parliament. TANs and TCNs were originally included in this requirement. **Following public feedback**, TARs issued by interception agencies must also be included in this report (see proposed section 317ZS).

136. Use and disclosure exceptions are included in the TIA Act to allow the Inspector-General of Intelligence and Security (IGIS) to effectively receive information relevant to their oversight of ASIO, ASIS and ASD.

The Surveillance Devices Act 2004 (SD Act)

137. The Commonwealth Ombudsman oversights the use of surveillance devices issued under the SD Act. This Act has extensive inspection and recording-keeping regime that provide the Ombudsman with powers to scrutinise the proper use of surveillance devices, including those that may be used in connection with a TAR, TAN or TCN.

138. The Commonwealth Ombudsman must report to the Minister for Home Affairs on the results of these inspections biannually. The Minister must table this report in Parliament.

139. The Department compiles annual reports regarding the use of surveillance devices. While these reports won't include the TARs, TANs and TCNs issued to assist in the execution of surveillance device warrants (those numbers will be included in the TIA Act annual report), the public has visibility of the use of surveillance devices by law enforcement.

140. State and territory surveillance device legislation, like the *Surveillance Devices Act 2007* (NSW) establishes similar inspection and reporting regimes for State law enforcement. For example, the Inspector of the Law Enforcement Conduct Commission must inspect the records of NSW law enforcement to determine compliance. A copy of the inspection report is tabled in the NSW Parliament.

Established Oversight Powers

141. Commonwealth, State and Territory oversight bodies have considerable powers to inspect and ensure the compliance of all agencies that are empowered under Schedule 1. This includes the ability to conduct compliance inspections on the use of covert and intrusive powers, require the production of agency information, hear complaints about agency activities and report to Commonwealth or State Parliaments.

142. Schedule 1 does not limit these functions. Proposed paragraph 317ZF(3)(c) creates an exception to the prohibition against unauthorised disclosure to allow the existing oversight roles of these bodies to operate smoothly in relation to agency functions under Schedule 1.

The Inspector-General of Intelligence and Security

143. The IGIS has extensive powers to oversight the limited functions of ASIS and ASD under new Division 2. Importantly, the IGIS has a statutory role to undertake comprehensive oversight of ASIO activities. IGIS functions include powers to obtain information, take sworn evidence and enter agency premises.

144. The IGIS will oversee the making and administration of TARs by ASIS and ASD, and the ASIO's functions under a TAN and TCN. In their submission to Home Affairs, IGIS acknowledged that their oversight role could include consideration of complaints from a DCP and others who may be affected by notices and requests.

145. To facilitate IGIS oversight, the use and disclosure provisions in paragraph 317ZF(3)(f) allows disclosure of information about a TAN, TAR or TCN to an IGIS official for the purpose of their exercising powers, or performing their functions or duties.

146. Given the extension in the oversight functions of the IGIS, Home Affairs, with Government and the Attorney-General's portfolio, will monitor the adequacy of IGIS resourcing. The implications on IGIS oversight will rest on the frequency, and manner, in which the new powers may be used.

Ombudsman and integrity bodies

147. Commonwealth and State Ombudsman, as well as integrity bodies such as the NSW Law Enforcement Conduct Commission have extensive powers to initiative investigations into the activities of the law enforcement agencies empowered under this schedule.

148. As noted above, the express exception to the offence against unauthorised disclosure has been made to facilitate the general inspection and oversight functions of these bodies. Paragraph 317ZF(3)(c) allows the disclosure of information relating to a TAR, TAN or TCN in accordance with any requirement imposed by a law of the Commonwealth, a State or a Territory – including notice to produce powers in the enabling legislation of oversight bodies.

Judicial Review

Depending on the issuing body, the *Constitution* and the *Judiciary Act 1903* provide clear avenues for judicial review of the exercise of powers under new Part 15 of the *Telecommunications Act 1997*. For example:

a. Issue of a TAN by a Commonwealth interception agency (i.e. the AFP) or a TCN by the Attorney-General would be reviewable by the High Court due to its constitutional power of review. The Federal Court may also review these powers through the *Judiciary Act 1903*.

b. Issue of a TAN by a State interception agency (i.e. NSW Police) would be reviewable by the Federal Court or State Supreme Courts through the *Judiciary Act 1903*.

c. Issue of a TAN by a Territory interception agency (i.e. NT Police) would be reviewable by the Federal Court through the *Judiciary Act 1903*.

149. Grounds for review are broad and may be on the basis that a requirement would create a systemic weakness into a form of encryption, contrary to the prohibition ,or that in the circumstances the decision-maker could not have been satisfied that requirements in the notice were reasonable, proportionate, practical or technically feasible.

150. The Bill does not provide for merits review of decision making and excludes judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act). This approach to review is consistent with similar decisions made for national security and law enforcement purposes – for example those made under the IS Act, ASIO Act, *Inspector General of Intelligence and Security Act 1986* and the TIA Act. Many ministerial decisions of national security and law enforcement nature are also expressly excluded from the ADJR Act regime, noting the severity and urgency of these decisions.

151. 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. As the publication notes, if decisions relating to investigations were subject to merits review the investigation of breaches, as well as the proper enforcement of the law could be jeopardised.[16]

152. Security and law enforcement agencies may require a technical assistance notice in order to access appropriate electronic evidence for an investigation that is underway and evolving. It is imperative that a TAN can be issued and used quickly. It would not be appropriate for a decision to issue a TAN to be subject to judicial review under the ADJR Act or merits review as review could adversely impact the effectiveness and outcomes of an investigation. Decisions by the Attorney-General to issue a TCN are particularly unsuitable for review as they are ministerial decisions to develop law enforcement and national security capabilities.

Ministerial Oversight

153. Consistent with established arrangements for administrative decision-making powers, the Attorney-General is the issuer of a TCN. This ensures that this significant power is subject to oversight at the highest levels of the Government and mirrors authorisation procedures for the issuing of warrants to intelligence and security services, and the making of ministerial directions to protect Australian telecommunications networks or facilities for unauthorised access.

154. Several key pieces of national security legislation provide for the exercise of ministerial authorisations, including (but not limited to):

- The *Telecommunications and Other Legislation Amendment Act 2017* (which amended the Telecommunications Act) enables the Attorney-General to issue a notice requiring a carrier to do a specified act or thing for the purpose of eliminating the risk of unauthorised interference with a network or facility.
    - Like TCNs, this direction power is subject to consultations, requirements and judicial review.

[16] Administrative Review Council (1999) "What decisions should be subject to merits review" at 4.31

- The issue of ASIO search warrants by the Attorney-General under section 25 of the ASIO Act.
- The issue of interception warrants by the Attorney-General under section 9 of the TIA Act.
- Ministerial directions under sections 8 and 9 of the IS Act.

Centralisation

155. Enforcement actions for non-compliance with a notice must be undertaken by the CAC, a central, statutory authority within Home Affairs. Division 5 of Schedule 1 designates the CAC as the applicant for proceedings related to civil penalties, enforceable undertakings and injunctions in the Federal Court. This will ensure that State and Territory agencies cannot commence actions against a DCP without Commonwealth involvement and allow the Commonwealth to take into account broader Australian interests before commencing an action.

156. The CAC also retains central oversight of the regime through the notification requirements in proposed subsection 317ZF(12). This requires that agencies utilising the powers notify the CAC before information about a TAN, TAR and TCN is disclosed.

Reporting

157. As mentioned above, the numbers of TARs, TCNs and TANs issued in a year by interception agencies must be tabled in Parliament in the report prepared under the TIA Act. Although this requirement originally included just the numbers of TCNs and TANs issued in a year, **following public consultation** a requirement was added to include TARs in annual report to increase transparency.

158. **Following industry consultation** changes were made to the unauthorised disclosure provisions in proposed section 317ZF to allow a DCP to disclose statistics about the total number of TANs, TARs or TCNs given to them during a period of the last six months. This change will allow DCPs to publish the level of their assistance in corporate transparency reports. To ensure that these transparency reports could not be linked to covert agency activities, these statistics must be published in the aggregate and cannot identify the agency that issued the notice or request.

Compliance, costs, terms and conditions

159. Acknowledging the value that agencies place on industry assistance, the Bill takes the default position that a DCP should be able to recover the reasonable costs of assistance (see proposed section 317ZK). The no-profit/no-loss basis is consistent with the terms that carriers and carriage service providers receive for assistance pursuant to section 313 of the Telecommunications Act. However, different costs arrangements may be agreed between Government and a DCP in appropriate circumstances. For example, commercial terms may be suitable in cases where agencies require a provider to develop a large bespoke capability that would ordinarily be the subject of a significant procurement. The availability of commercial terms will give an agency the flexibility to enter into an arrangement containing both financial incentives and risk-management measures to secure satisfactory and timely performance.

160. In limited circumstances a DCP may not be entitled to cover the costs of compliance. A decision-maker may invoke a public interest exception to the no-profit/no-loss rule if they meet strict thresholds and weigh the impact of such a decision with the regulatory burden on the provider. For example, full reimbursement may not be appropriate if a TAN or TCN has been issued to remediate a risk to law enforcement or security interests that has been recklessly or wilfully caused by a DCP.

161. The Bill allows the terms and conditions of a notice to be set flexibility between Government and a DCP, consistent with the existing framework for industry assistance in section 314 of the Telecommunications Act.

162. A DCP is only expected to comply with the requirements of a notice to the extent that they are capable of doing so. For example, if a DCP does not have the resources, or the means to acquire the resources, to comply with requirements they will not be expected to do so.

163. **Following public and industry feedback** a defence for non-compliance was inserted into proposed subsection 317ZB(5) of the Bill. If a DCP (who is not a carrier or carriage service provider) can prove that compliance with a TAN or TCN would cause it to contravene a law of a foreign country, it has a defence for non-compliance in a proceeding for a civil penalty order. Acknowledging the global reach of some providers that may be subject to these powers, Home Affairs agreed that a DCP should not be placed in a position where compliance with a TAN or TCN would cause the violation of the laws of another country.

Arbitration

164. In exceptional cases where DCPs and Government cannot agree on the terms and conditions for compliance with a notice, an independent arbitrator appointed by the Australian Communications Media Authority or the Attorney-General will determine terms and conditions under proposed subsections 317ZK(5) – (14). This mechanism is consistent with the method for resolving disputes on the terms and conditions of existing industry assistance under section 314 of the Telecommunications Act.

Comparison to the Investigatory Powers Act 2016 (UK)

165. Regular comparisons have been made between Schedule 1 of the Bill and the *Investigatory Powers Act 2016* (UK) (IPA). The IPA is the UK's principle source of investigatory powers and contains a comprehensive suite of measures for UK law enforcement and national security agencies, including:

- revised powers for targeted interception, data collection and computer network exploitation,
- bulk powers which enables the surveillance of multiple communications,
- a new data retention scheme, and
- the introduction of Technical Capability Notices (UK TCN) to solicit industry assistance.

166. While Home Affairs notes that comparisons between regulatory regimes in different jurisdictions is a complex exercise, it emphasises that no direct comparison can be made between the size and scope of the IPA Act and this Bill. The IPA is vastly larger in scope and application. This Bill **does not** provide for:

- interception, bulk or otherwise[17]
- bulk equipment interference
- disclosure of communications data

[17] Limited Interception for testing purposes or where it is ancillary to the execution of computer access warrants in Schedule 2 is permissible. Schedule 2 restricts the interception activities to those necessary for executing a computer access warrant itself (see proposed section 27E(2)(h))

- the retention of personal data sets, including internet collection records, or
- multiple other powers in the IPA.

167. The above powers are substantial and their Australian equivalents, where there are equivalents, are located in a number of separate pieces of established legislation that have been modernised over the years through separate Acts. For example, targeted interception powers and data retention are regulated by the TIA Act and data surveillance devices can be issued, under warrant, via the SD Act. These Acts, and other relevant statutes, contain their own safeguards including judicial oversight arrangements, independent oversight by the IGIS and Ombudsman and reporting requirements.

168. As a source of criticism to the Bill, a number of public submissions noted that the European Court of Human Rights made a ruling in September 2018 against UK's IPA powers. This ruling chiefly related to the use of bulk surveillance powers in another, older piece of legislation the *Regulation of Investigatory Powers Act 2000* (RIPA) which has largely been replaced by the UK IPA. The Bill does not allow for the kinds of powers that were subject to the challenge.

169. The measures in this Bill contain some similarities to the UK TCN provisions. While both measures are intended to solicit industry assistance with access to communication, there are significant differences. Notably, the UK TCN has a more expansive scope. Unlike the proposed powers in Schedule 1, Home Affairs understands a UK TCN can:

- Compel the creation of a capability to remove a form of electronic protection, including decryption capabilities.
    - A TCN in this Bill cannot require DCPs to build such a capability and the inclusion of requirements to build a decryption capability is expressly prohibited by proposed subsection 317ZG(2).
    - The IPA Act leaves the door open to requiring companies to retain a capability to decrypt communications where reasonably practicable.
- Require a provider to establish an interception capability.
    - Mandatory interception capabilities are limited and regulated by Part 5-3 of the TIA Act.
    - Proposed subsections 317T(8) – (11) expressly exclude the use of TCNs for this purpose.
- Require a provider to establish a delivery capability.
    - Mandatory delivery capabilities are limited and regulated by Part 5-5 of the TIA Act.
    - Proposed subsections 317T(8) – (11) expressly exclude the use of TCNs for this purpose.
- Require a provider to establish bulk collection capabilities.

170. Notably, the UK TCN framework **does not**:

- Contain an express prohibition against the building or implementation of systemic weakness or vulnerabilities or an equivalent provision.
- List the obligations that may be set in a notice in primary legislation; this is instead specified through regulations.

171. The presence of the 'double-lock' regime in the UK IPA whereby a Secretary of State and a Judicial Commissioner approve a TCN is a feature of the Investigatory Powers Commissioner's broader function to approve warrants issued under that Act. Home Affairs will not comment on its

appropriateness but maintains that the scope of potential activities under a UK TCN is more expansive and may have more significant impacts on DCPs than a TCN proposed by this Bill. This assessment is particularly based on the ability of a UK TCN to remove electronic protection and the use of UK TCNs to mandate core surveillance capabilities, like interception.

172. The Technical Advisory Panel established by the IPA Act, while commenting on regulations relevant to a UK TCN, has broader functions relating to the exercise of the extensive powers contained in the IPA (powers that are not present in the Bill). Further, the Department understands that the panel have a role on assessing core capabilities that may be developed under a UK TCN which TCNs under the Bill cannot mandate.

173. As discussed elsewhere in this submission, ministerial authorisations like the Attorney-General's ability to issue a TCN are an established aspect of the Australian regulatory regime that operate effectively, and appropriately, to discharge and monitor national security and law enforcement powers.

Warranted computer surveillance – Schedule 2

Purpose

174. Schedule 2 modernises legislation to allow Commonwealth, State and Territory law enforcement agencies to obtain a warrant to covertly search electronic devices and access content. Data surveillance powers that already facilitate access to a computer are available to law enforcement in existing legislation through the SD Act.

175. However, the capacity of these powers are limited and increasingly unsuitable for modern investigations. Currently, a surveillance device warrant permit 'view only' access on a device and does not permit the remote searching of a device (e.g. searching folders where it becomes clear that those folders will contain child sexual exploitation).

176. The *computer access warrant* will allow for agencies to access content at a point where it is not encrypted (e.g. where a communication is in plain text on the device but then encrypted once sent over a network). This ensures agencies are able to view communications without unnecessarily compromising encryption technologies on a device when lawfully obtaining evidence for investigations or prosecutions.

177. The Bill allows the execution of a computer access warrant covertly and remotely to limit interference with property and risk of harm to law enforcement officers. Similarly, the Bill allows agencies to conceal access to devices to preserve the effectiveness of covert warrants and operational integrity.

178. Schedule 2 also amends legislation to ensure Australia continues to meet its international agreements and cooperatively work with international partners as required.

What is computer access?

179. Computer access involves collecting information directly from end-point (target) electronic devices, either remotely or physically, acknowledging that the end-point device needs to decrypt content to enable the user to interpret it, and that modern encryption provides an effective means of preventing eavesdropping or access to content whilst in transit.

Law enforcement and ASIO warrants

180. Schedule 2 amends the SD Act to allow for Commonwealth, State and Territory law enforcement agencies to obtain computer access warrants when investigating a federal offence punishable by a maximum of three years imprisonment or more.[18]

181. Amendments to the SD Act ensure that the criteria for issuing a computer access warrant is consistent with existing surveillance devices warrants and authorisations. The SD Act has also been amended to strengthen safeguards and limitations that ensure agencies are only able to issue a computer access warrant when required.

182. Schedule 2 also provides for a number of new powers for law enforcement agencies and amends the ASIO Act to address a range of operational challenges associated with the use of existing computer access powers, including by:

- Enabling the interception of communications for the purpose of executing a computer access warrant, removing the need to obtain a second warrant for that purpose.
- Permitting the temporary removal of a computer or thing from a premises (for example, to a vehicle or nearby premises that has more sophisticated equipment to enable access to the computer), for the purpose of executing a warrant, and to return the computer or thing.
- Enabling agencies to take steps to conceal its access to a computer, following the expiry of the warrant, to address situations where an agency no longer has access to the computer at the time the warrant expires and discovery may compromise a covert investigation.

183. Collaboration between providers and agencies in the testing or developing of interception technologies is critical. Schedule 2 amends the TIA Act to permit the head of a security authority to request the Attorney-General to authorise the security authority to work with a carrier in order to test or develop interception technologies. This ensures that carriers are able to provide assistance to agencies under Schedule 1 when required.

184. The Bill also updates provisions in the TIA Act to allow security agencies to test their capabilities either independently or with the assistance of a carrier. Currently, the TIA Act only allows testing by employees of a security authority. The amendments will allow carriers to work with security authorities under authorisation, reflecting the practical operation of interception capabilities.

185. Investigations and prosecutions frequently involve criminal use of the internet and cross border storage of information. Australia's mutual assistance framework is critical in enabling Australian and foreign authorities access to information necessary to investigate and prosecute serious crime.

Mutual legal assistance and assistance to foreign partners

186. Foreign countries will be able to request through Australia's mutual assistance framework for the Australian Federal Police to seek a computer access warrant and execute on behalf of a foreign country. Evidence obtained as a result of that warrant will then be provided through the mutual assistance process.

187. Computer access warrants are a critical new tool to combat not only serious domestic crime but also serious crime that is transnational in nature. Accordingly, it is necessary and a logical step to allow foreign countries to request these powers under mutual assistance to combat serious transnational crime.

188. The mutual assistance framework will provide safeguards, including mandatory and discretionary grounds of refusal (identified above in regards to Schedule 1). An additional safeguard will be direct

[18] Commonwealth agencies may apply for warrants to investigate State offences with a federal aspect.

ministerial oversight requiring the Attorney-General to authorise the AFP to apply to an eligible Judge or nominated AAT member to obtain a computer access warrant.

Safeguards and limitations

189. Similar to the thresholds that apply to surveillance devices warrants, law enforcement officers can only seek a computer access warrant for relevant offences if the officer has reasonable grounds to suspect that:
    - a relevant offence (generally an offence attracting punishment of three years or above) has been or will be committed
    - an investigation is or will be underway, and
    - access to data is necessary to obtain evidence of the offence or information about the offenders.
190. Computer access warrants are issued by judges or AAT members. In deciding whether to issue a warrant, he or she must be satisfied of the grounds of the application. Under proposed subsection 27C(2) judge or AAT member must also have regard to:
    - the nature and gravity of the alleged offence
    - the likely evidentiary or intelligence value of any evidence that might be obtained
    - any previous warrant sought
    - the extent to which the privacy of any person is likely to be affected, and
    - the existence of any alternative means of obtaining the evidence or information.
191. A computer access warrant must specify the things that are authorised under the warrant, which may include:
    - entering premises for the purposes of executing the warrant
    - using the target computer, a telecommunications facility, electronic equipment or data storage device in order to access data to determine whether it is relevant and covered by the warrant
    - adding, copying, deleting or altering data if necessary to access the data to determine whether it is relevant and covered by the warrant
    - using any other computer if necessary to access the data (and adding, copying, deleting or altering data on that computer if necessary)
    - removing a computer from premises for the purposes of executing the warrant
    - copying data which has been obtained that is relevant and covered by the warrant
    - intercepting a communication in order to execute the warrant, and
    - any other thing reasonably incidental to the above things.
192. Interference is not authorised when executing a computer access warrant. Specifically, the warrant does not authorise the addition, deletion or alteration of data, or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. However, there may be addition, deletion or alteration of data where necessary for the execution of the computer access warrant. Moreover, the warrant does not authorise the material loss or damage to other persons lawfully using a computer, except where necessary for concealment.

193. The chief officer of the law enforcement issuing agency must revoke the warrant if it is no longer required to obtain evidence of the offence. The chief officer also has an obligation to ensure that access to data is discontinued.

194. Unauthorised disclosure of information about, or obtained under, a computer access warrant is an offence. 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.

195. The use, recording and communication of information obtained in the course of intercepting a communication in order to execute a computer access warrant is restricted. Where agencies want to gain intercept material for its own purpose, they must be issued with, an interception warrant under Chapter 2 of the TIA Act.

Oversight

196. The Bill includes strong reporting requirements to provide assurance to Parliament and the Australian community that the powers are being used only as required.

197. The chief officer of a law enforcement agency must report to the Minister for Home Affairs on every computer access warrant issued and include the following high-level detail:

- whether the warrant or authorisation was executed
- the name of the person primarily responsible for the execution
- the name of each person involved in accessing data
- the name of any person whose data was accessed
- the location at which the computer was located, and
- details of the benefit to the investigation.

198. Agencies must report annually on the number of warrants applied for and issued during the year and the number of emergency authorisations.

199. Agencies must keep records about computer access warrants, including in relation to decisions to grant, refuse, withdraw or revoke warrants and how the information in the warrant has been communicated.

200. This information will also allow the Commonwealth Ombudsman to review the performance of the computer access warrant and determine compliance with law. The Ombudsman will report their results to the Minister biannually. The Minister must table Ombudsman reports in the Parliament.

Enhancing existing channels of access to data – Schedules 3, 4 & 5

Enhanced search warrants under the *Crimes Act 1914* – Schedule 3

Overview and purpose

201. Schedule 3 amends the *Crimes Act 1914* (Crimes Act) to enhance the ability of criminal law enforcement agencies to collect evidence from electronic devices found during a search warrant. Specifically, these amendments modernise the existing search warrant powers and assistance orders to account for modern technology such as smart phones and the complexity of modern communications systems.

Computer access

202. Currently, the Crimes Act allows law enforcement to obtain an overt search warrant (which must be issued to the relevant person) to seize and search computers. Schedule 3 modernises this existing power by allowing law enforcement agencies to remotely and overtly collect evidence using specialist equipment. This amendment is in keeping with current forensic best practices as it reduces the risk of altering, damaging or destroying evidence by using a suspect's computer, which is required under the current search warrant provisions.

203. Schedule 3 ensures the computer access warrants in the Crimes Act reflects modern forms of communications. A new definition of *account based data* will be inserted to ensure that accessing a computer under a search warrant enables law enforcement officers to access information associated with an online account such as an email or social media account.

204. The current provisions in the Crimes Act do not take into account the length of time that forensic examination of electronic equipment commonly takes, particularly where encrypted content is located. The amendments in Schedule 3 will increase the time that an electronic device found while executing a warrant can be moved to another place to determine whether it contains evidential material from 14 days to 30 days.

Safeguards

205. Computer access warrants are supported by strong safeguards to ensure they are only issued to meet legitimate law enforcement objectives and that law enforcement do not adversely affect privacy and the integrity of the data or device. These safeguards include:

- Warrants require the approval of an independent issuing officer employed by the court.
- The issuing officer must be satisfied that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, evidential material on the premises or person.
- The warrant must be executed within seven days after it is issued.
- The person executing the warrant must make details of the warrant available to the occupier of the premises or person.
- A warrant does not authorise the addition, deletion or alteration of data, or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. An exception to the limitation is where the actions are necessary to execute the warrant.
- Material loss or damage to other persons lawfully using a computer is prohibited.

Assistance orders

206. The Crimes Act includes important powers that allow law enforcement to compel a person to provide assistance in certain circumstances. Under the current section 3LA, a magistrate can compel certain persons (including owners and users of a device) to assist in providing access to data held in, or accessible from, a device that has been seized, moved or found in the course of a search authorised by a warrant. An order may also require a person to assist in copying data to another device and converting data into an intelligible form. Section 3LA also imposes an obligation, in limited circumstances, upon a person with knowledge of a computer or a computer system to assist law enforcement for the purposes of accessing the computer or computer system.

207. However, recent law enforcement experiences have highlighted that current assistance order powers are outdated as they can only be issued pursuant only to a premises search warrant. Law enforcement can't compel that assistance in relation to a device, such as a mobile device, found on

their person. Schedule 3 amends the Crimes Act to address this gap and to ensure existing assistance orders reflect the prevalence of devices such as smart phones and tablets being carried by people.

208. To reflect the importance of assistance orders to investigations and the deficiencies in the current regime, Schedule 3 also increases the penalties for not complying with orders from a judicial officer requiring assistance in accessing electronic devices where a warrant is in force. The Crimes Act assistance order will now be subject to a tiered penalty. Firstly, the existing penalty (lower offence) will increase from a maximum of two years imprisonment to a maximum five years imprisonment for a 'simple' offence. A second higher offence of up to ten years imprisonment will be introduced for contravention of a 'serious offence' or a 'serious terrorism offence'.[19]

209. The increase in penalty is a necessary incentive. Often people who are suspected to be involved in serious criminal activity will accept the current two year penalty rather than provide information held on a device that could be used in evidence in prosecution of a more serious offence. For example, a sentence of two year imprisonment is significantly lower than the 15 years or more attached to certain child sex offences. If a suspect held child exploitation material on their device, there is little incentive to cooperate with an order for access.

210. The use of a 3LA assistance order is an essential tool in the investigation of serious criminal activity to ensure that either law enforcement have access to devices subject to protections such as passwords, or there is criminal accountability in the event a person refuses and a prosecution is in the public interest. An example is the 2016 prosecution of Matthew Graham who was convicted of 13 charges relating to the control of multiple child sexual abuse websites on the 'dark web' which he used to access a network where he controlled, distributed and facilitated the production of child pornography material. He received total effective sentence of 15 years six months' imprisonment with a non-parole period of 10 years. For the offence under section 3LA, he was sentenced to six months' imprisonment, which must be considered in the context of the overall sentence.

211. Where a section 3LA offence is being sentenced alongside more serious offences such as child sexual abuse online, a penalty of two years imprisonment also fails to attract the clear serious criminal accountability expected for noncompliance with the court order. Increasing the penalty goes a long way to recognise this deficiency and signals Parliament's intention that non-compliance must attract a higher penalty to ensure criminal accountability reflects the seriousness of the crimes.

212. Assistance orders do not threaten the privilege against self-incrimination. The orders require a person to provide the necessary information to enable a law enforcement officer to access the computer, not the information within the computer itself. This is an important distinction. Existing search warrants can require a person to give access to a premises which may hold information of evidentiary value; the assistance orders (already established under the Crimes Act) require a person to give access to a lawfully seized device that may hold information of evidentiary value.

213. There must be reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device. The new thresholds represent the maximum penalty that may be imposed and courts retain the discretion to impose a lower penalty in appropriate circumstances.

Safeguards

214. Currently, the Crimes Act requires law enforcement officers to apply to a magistrate for assistance to access a device. Before a Judge or AAT member issues a person-based warrant, subsection 3E(2) states that they must be satisfied that there are reasonable grounds for suspecting that the person has in his or her possession, or will within the next 72 hours have in his or her possession, any

[19] A serious offence means an offence punishable by imprisonment for two years or more.

evidential material. Evidential material is anything relevant to an indictable offence or summary offence that has been or will be committed.

215. A number of additional conditions in subsection 3LA(2) must be met before a magistrate grants an order to allow enforcement to compel a person to give assistance accessing data. The person must be connected to the device (for example, as the device owner or user) and have the relevant knowledge to enable them to access the device. This bill does not amend the existing robust safeguards.

Enhanced search warrants in the *Customs Act 1901* – Schedule 4

Overview and purpose

216. Similar to Schedule 3, the Bill amends the *Customs Act 1901* (Customs Act) to allow the Australian Border Force to collect evidence from electronic devices under a search warrant. Specifically, these amendments modernise existing computer access warrants and assistance orders to account for modern technology such as smart phones and the complexity of modern communications systems.

Computer access

The power to search persons who may have computers or storage devices

217. Schedule 4 enables a judicial officer to issue a warrant authorising the ABF to search or frisk a person if they are satisfied that there are reasonable grounds for suspecting that the person possesses, or will possess in the next 72 hours, a computer or data storage device that is evidential material. Evidential material is anything relevant to an indictable offence or summary offence.

218. Under existing laws, the ABF could only obtain a judicial authorisation for a search warrant relating to a search of premises. The amendments recognise that information is often stored on devices, held physically by persons, and that an inability to access this information may impede legitimate investigations and prosecutions.

The power to remotely access computers

219. Schedule 4 enables the ABF to access private communications and other information on a device using a range of methods. Amendments to the search warrant framework in the Customs Act will enable the ABF to use electronic equipment, data storage devices and telecommunications facilities where a search warrant is in force in order to obtain access to data held in the computer or device, or account-based data accessible by the device.

220. At present, under section 201 of the Customs Act, the executing officer of a search warrant in relation to premises or a person assisting, may operate electronic equipment at the warrant premises to access data if he or she believes on reasonable grounds that the data constitutes evidential material. To use this power, an officer must be physically located at the warrant premises.

221. Proposed subsections 199(4A) and 199B(2) will allow the ABF to access data without having to physically be on warranted premises. The amendments provide that a search warrant relating to a premises authorises the officer or assisting person to use a computer, data storage device found in the course of a search, or a telecommunications facility, or other electronic equipment or a data storage device to obtain data on the computer, or a data storage device found in the course of a search to determine whether the data on it is evidential material. The provisions also allow for data to be added, copied, deleted or altered where reasonable to do so. The warrant can be used to access account-based data of a person who is the owner or lessee of the computer, who uses the computer or who has used the computer.

The power to move a computer or data storage device in the course of a search under a warrant

222. Schedule 4 enables a person-based search warrant to authorise the movement of a computer or data storage device in the course of a search to another location in order to determine whether the computer or data storage device constitutes evidentiary material that should be seized. The executing officer must believe on reasonable grounds that the computer or device is evidential material in relation to an offence to which the warrant relates, and the movement is necessary to prevent its concealment, loss or destruction or its use in committing an offence. These amendments reflect the current provisions for premises-based search warrants in the Customs Act, which allow an executing officer to move evidential material or suspected evidential material found on a premises.

223. This power will allow the ABF to analyse the computer or data storage device for evidence, enhancing their ability to conduct investigations and assist prosecutions. Any limitation or interference with the right to privacy is necessary and in the interests of law enforcement and national security.

224. The Bill also includes amendments to timeframes for how long a device may be moved for analysis. Under the current section 200 of the Customs Act, a thing moved from premises must be returned within 72 hours. These amendments will extend the time period for moved computers and data storage devices to 30 days and allow time extensions of 14 days. These timeframes will allow the ABF adequate time to conduct the lengthy and intricate forensic processes necessary for electronic devices. The amendments ensure the ABF can fulfil its statutory functions with forensic best practice.

Safeguards

225. The amendments to the Customs Act are supported by robust safeguards to ensure a warrant is only issued to meet ABF objectives and, that in executing a warrant, law enforcement do not adversely impact privacy and the integrity of the data or device. These safeguards include:

- Warrants are authorised by a judicial officer to ensure a warrant is issued only when necessary to meet the ABF's objectives and is proportionate to the potential offence.
- The amendments provide a strict time limit of seven days to undertake a search authorised by the warrant.
- The executing officer must believe on reasonable grounds that the computer or data storage device is evidential material and that the seizure is necessary to prevent the concealment, loss or destruction of that item.
- The addition, deletion or alteration of data is not authorised when those actions are likely to interfere with communications in transit or the lawful use by other persons of a computer, unless specified in the warrant. The addition, deletion or alteration of data is also not authorised when those actions are likely to cause any other material loss or damage to other persons lawfully using a computer.

Assistance orders

226. The Customs Act includes important powers that allow law enforcement, under judicial authorisation, to compel a person to provide assistance in certain circumstances. Schedule 4 will increases the penalties for not complying with orders from a judicial officer requiring assistance in accessing electronic devices where a warrant is in force. The penalty under the Customs Act will increase from a maximum of six months imprisonment to a maximum five years imprisonment or 300 penalty units for a 'simple' offence, and up to ten years imprisonment or 600 penalty units for contravention of a new 'aggravated' offence where the investigation of a serious offence or a serious terrorism offence.

227. Like orders under the Crimes Act, the increased penalty is a necessary incentive. A sentence of six months imprisonment is significantly lower than the 15 or more years attached to certain trafficking offences. If compromising material was held on a device, there is little incentive to cooperate with authorities for access.[20]

228. These amendments will assist the ABF to access information held directly on a computer or data storage device, which may otherwise be inaccessible or unintelligible.

Safeguards

229. The requirement for a magistrate to authorise warrants provides an important safeguard for person-based search warrant powers. To grant an order, the magistrate must be satisfied of a number of things set out in the legislation, including that: there are reasonable grounds for suspecting that evidential material is held in, or accessible from, the computer or device; that the person is connected to the computer or device (for example, as the owner or user); and that the person has relevant knowledge to enable access to data held in, or accessible from, the computer or device. These existing robust safeguards have been retained.

ASIO assistance powers – Schedule 5

Overview and purpose

230. Schedule 5 amends the ASIO Act to allow ASIO to seek voluntary or compulsory assistance to gain access to data. These amendments facilitate ASIO in achieving its objective of gathering information and producing intelligence which is critical to national security matters.

Voluntary assistance

231. Proposed section 21A establishes two frameworks which provide protection from civil liability for voluntary assistance provided in accordance with a Director-General request and for unsolicited disclosure of information.

Servicing a voluntary request from ASIO

232. Proposed subsection 21A(1) provides that if the Director-General requests a person or body to engage in conduct that the Director-General is satisfied is likely to assist ASIO in the performance of its functions and:

- the person engages in the conduct in accordance with the request
- the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory, and
- the conduct does not result in significant loss of, or serious damage to, property.

233. The person or body is not subject to any civil liability for, or in relation to, that conduct. The requirement for the Director-General to be satisfied that the conduct is likely to assist ASIO in the performance of its functions is intended to provide greater legal certainty to recipients of requests, by allowing them to rely on the Director-General's satisfaction.

Unsolicited assistance provided to ASIO

234. Schedule 5 also provides protection from civil liability for persons or bodies making unsolicited disclosures of information to ASIO. The amendment provides that a person or body is not subject to civil liability for, or in relation to, conduct that consists of, or is connected with giving information to

[20] See above discussion.

ASIO, or giving or producing a document to ASIO, or making one or more copies of a document and giving those copies to ASIO, and:

- the person reasonably believes that the conduct is likely to assist ASIO in the performance of its functions
- the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory
- the conduct does not result in significant loss of, or serious damage to, property, and
- a Director-General request discussed above does not apply to the conduct.

235. Given this amendment relates to unsolicited help, the policy intention is to ensure that someone who reasonably believes that their help will assist benefits from the immunity, even if they are mistaken about what may assist ASIO, or ASIO's functions.

Compulsory assistance

236. The rapidly evolving nature of technology, including the prevalence of encryption, is impacting ASIO's ability to gain access to data stored on computer devices and networks. This data is critical for ASIO to better understand the national security threat environment.

237. Schedule 5 addresses this issue by allowing the Director-General to request the Attorney-General to make an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow ASIO to do one or more of the following (proposed section 34AAA):

- Access data held in, or accessible from, a computer or data storage device that:
    - is the subject of a warrant under section 25A, 26 or 27A
    - is the subject of an authorisation under section 27E or 27F
    - is on premises in relation to which warrant under section 25, 26 or 27A is in force
    - is on premises in relation to which an authorisation under section 27D or 27F is in force
    - is found in the course of an ordinary search of a person, or a frisk search of a person, authorised by warrant under section 25 or 27A
    - is found in the course of an ordinary search of a person, or a frisk search of a person, authorised under section 27D
    - has been removed from premises under a warrant under section 25, 26 or 27A
    - has been removed from premises under section 27D; or
    - has been seized under section 34ZB.

238. The types of assistance that ASIO may seek under this power include compelling a target or a target's associate to provide the password, pin code, sequence or fingerprint necessary to unlock a phone subject to a section 25 computer access warrant. Another example is where a specialist employee of a premises subject to a section 25 search warrant could assist ASIO officers to interrogate the relevant electronic database or use the relevant software so that they can obtain a copy of particular records or files.

239. This power enables ASIO to compel those capable to provide ASIO with knowledge or assistance to access data on computer networks and devices to do so. As noted above, similar powers are available to the police under section 3LA of the Crimes Act and equivalent powers in the Customs Act.

Safeguards

240. The amendments in Schedule 5 are supported by robust safeguards to provide the appropriate level of oversight, ensure requests are only issued if necessary and ensure protections are available for assistance provided. These safeguards include:

- Assistance requests are issued by Australia's highest law officer, the Attorney-General, which ensures there is appropriate oversight and that requests are only issued if necessary.
- Lawful protections are available for those that satisfy a voluntary request from ASIO, or that disclose information unsolicited.

241. ASIO must seek an order from the Attorney-General to require a person to provide assistance. The Attorney-General must be satisfied that the device is subject to an issued ASIO warrant. This means that the thresholds of the particular warrant have been met. For example, under a computer access warrant, access to data must substantially assist the collection of intelligence in accordance with the ASIO Act in respect of a matter that is important in relation to security.

242. The person who is to be given the order must also be reasonably suspected of being involved in activity prejudicial to security, or a person who is otherwise connected to the device. The person must also have relevant knowledge of the device or computer network.

243. The measures are directed towards the legitimate objective of ensuring that ASIO can give effect to warrants which authorise access to a device. ASIO's inability to access a device can frustrate operations to protect national security. The measures are a reasonable and proportionate response to the challenges brought about by new technologies, including encryption.

Outcome of consultation

244. Home Affairs has already conducted significant consultation on the entire Bill amongst Government, industry, civil society groups and the public. Consultations can be divided into three distinct stages:

- Preliminary industry consultations (July 2017 – June 2018)
- Targeted industry consultations (28 June 2018 – 14 August 2018)
- Public consultations (14 August 2018 - 10 September 2018)

245. Significant changes have been made to the Bill on the basis of feedback received in both industry consultations and public consultations. The key concerns raised in consultations, and the Department's response to them, are outlined below.

246. **Attachment H** contains a full summary of amendments made to the Bill following both consultation periods.

Preliminary industry consultations

247. Industry has been aware of, and consulted on, the development of a legislative response to the problems associated with encryption for more than a year. On 14 July 2017, then Prime Minister Malcolm Turnbull announced the development of a legislative package to assist Australia's law enforcement and security authorities with access to encrypted messages.

248. Immediately following this announcement, the Attorney-General's Department (AGD), then responsible for the reforms, began engaging with key industry stakeholders to discuss the proposals. As the Bill was developed, AGD and then Home Affairs presented the intention, and broad operation,

of the industry assistance framework (Schedule 1) to select domestic and offshore providers. Officers at both departments received and incorporated the preliminary feedback from industry when developing draft legislation.

249. Significant engagement also occurred at the Ministerial level with then Attorney-General George Brandis and former Minister for Law Enforcement of Cyber Security, the Hon Angus Taylor MP, meeting with senior industry representatives on the proposed reforms a number of times.

250. Over 25 separate meetings were held with industry members at the departmental and ministerial level during this period.

Targeted industry consultations

251. On 28 June 2018 the then Minister for Law Enforcement and Cyber Security, the Hon Angus Taylor MP, hosted a roundtable for a number of key companies potentially affected by the legislation. A full exposure draft of the Bill was released at this roundtable, along with extensive explanatory materials to assist industry with their scrutiny of the legislation. The roundtable was confidential for both industry and Government participants. It was important that industry and Government were able to engage in an open and frank discussion about the proposed legislation, without prejudicing any final position.

252. At the roundtable, and in the weeks following, these companies provided substantive, and constructive, feedback on the exposure draft. Home Affairs held 10 separate meetings to discuss possible amendments on the Bill, engaging with 11 key providers. These consultations continued throughout July and early August and progressive changes were made to the draft legislation during this time.

253. While the details of the conversation are confidential, in general terms, the primary pre-occupations of industry regarded the security of their customers' data and privacy as well as the Bill's potential regulatory burden. As a result of these discussions Home Affairs made significant changes to the Bill, specifically:

- Strengthening the prohibition against building a systemic weakness or vulnerability into a form of electronic protection in proposed section 317ZG.
- Extending the limitations in proposed section 317ZH that prohibit the new powers from being used in substitution of an existing warrant or authorisation.
- Ensuring providers can publish statistics on requests and notices in corporate transparency reports.
- Requiring the Minister for Home Affairs to consider set criteria before specifying additional types of assistance.
- Setting an expiry time on notices and requiring that all requests and notices are given in writing by default.

254. Further detail on the amendments made following industry consultation is listed in **Attachment H.**

Public consultations

255. On 14 August 2018 the then Minister for Law Enforcement and Cyber Security released an exposure draft of the Bill for public comment by 10 September 2018, accompanied by extensive explanatory materials which included factsheets and a preliminary Explanatory Memorandum. The exposure draft that was released was amended following the outcomes of industry consultation.

256. Home Affairs received approximately 15,990 submissions during the consultation period. Of these submissions approximately:

- 15,130 were classified as standard campaign responses.
- 743 were unique individual responses classified as appropriate for consideration.
- 55 were considered substantive submissions from industry groups, civil society, government bodies and individuals.
- 62 were deemed inappropriate for publication due to the inclusion of offensive content.

257. The overwhelming majority of public submissions related to Schedule 1 of the Bill. All submissions received with consent to publish are available on the Department's website.[21]

258. In addition to reviewing the submissions received, Home Affairs held meetings with civil society groups like the Law Council of Australia and the Australian Human Rights Commission to discuss the measures in detail. Further, departmental representatives heard formally from representatives from digital rights bodies like the Electronic Frontiers Foundation and Internet Australia at conferences discussing the Bill and the broader question of exceptional access.

259. An exposure draft of the Bill was released on 14 August 2018, following by significant media reporting and public commentary. From the initial release of the exposure draft, Home Affairs maintained extensive coverage of the exposure draft's treatment in the media – including critical commentary and the key concerns of industry, civil society and interested academics.

260. Before the close of public consultations on the 10th of September 2018 the Department had drafted preliminary changes to the exposure draft in response to public commentary, continuous meetings with stakeholders and the submissions received before the deadline. Many of the final submissions were consistent with earlier commentary and confirmed the appropriateness of the changes. **Attachment I** notes the key concerns raised during this consultation process and Home Affair's response.

- requiring decision-makers to consider set matters, including privacy and cybersecurity, when deciding whether a notice is 'reasonable and proportionate'
- allowing the Attorney-General and a provider to appoint a technical expert to examine potential security impact of a TCN
- requiring decision-makers to explain to a provider their obligations under a request or notice
- removing 'protecting the public revenue' as a reason for which notices may be issued
- strengthening the limitation that prevents notices from being issued in substitution of an existing warrant or authorisation
- establishing a defence for providers where there may be a conflict of laws
- requiring the number of TARs issued to be reported, and
- clarifying that courts may protect national security, law enforcement and commercial information under a notice in relevant hearings.

261. A detailed list of the above changes is at **Attachment H**.

[21] https://www.homeaffairs.gov.au/about/consultations/assistance-and-access-bill-2018

Conclusion

262. The Bill is a necessary and proportionate response to the impact of technologies, such as encryption. These have significantly degraded law enforcement and national security agencies' ability to investigate and prosecute serious crimes, and combat threats to Australia's national security. Encryption is critical to protecting and securing information and communications, and is a vital part of internet, computer and data security. However, the evolving digital environment, including the growing use of encrypted technologies by terrorists and criminals, presents an increasing challenge for law enforcement and national security agencies.

263. Law enforcement and national security agencies have the ability to seize devices and access communications such as phone calls, provided there is a warrant issued by a judge or similar independent authority. However, lawfully intercepted or accessed communications are difficult or impossible to decrypt and use operationally. The inability of agencies to use lawfully obtained communications has a significant impact on public safety and national security.

264. The Bill does not provide law enforcement and national security agencies with any additional, unfettered powers but addresses the issues caused by technologies such as encryption and ensures agencies are able to give effect to warrants obtained under existing frameworks.

265. A key part to the Bill is strengthening existing relationships of cooperation between agencies and industry which have traditionally been important to addressing the issues caused by technologies when executing a warrant. Schedule 1 enhances the existing obligations of DCPs to aid agency investigations and, for the first time, extends assistance obligations to offshore providers. The communications industry designs, builds and operates the services and devices used to perpetrate crime and avoid detection and persons throughout the communications supply chain are in a unique position to assist agencies with the effective execution of warrants for lawful surveillance activities.

266. The prevalence of encryption highlights the legislative limitations which have impacted the ability of agencies to access communications for the collection of evidence and intelligence that may help to protect Australians. The Government determined that alternative collection capabilities must be available to allow agencies to access information at points where it is in an accessible form. Schedule 2 establishes a new computer access warrant regime for law enforcement and enhances ASIO's existing computer access powers, modernising the evidence and intelligence collection capabilities of Australia's key agencies and facilitating access to data in an accessible state.

267. Similarly, advice received from agencies was that existing search warrant frameworks required modernising to reflect the prevalence of modern technologies such as smart phones. Schedules 3, 4 and 5 augment the ability of agencies to access data in an accessible form by strengthening search and seizure powers for computers other devices such as mobile devices.

268. These schedules are supported by strong safeguards and oversight measures to ensure that the integrity of Australia's personal information, devices and communications are not compromised. Importantly, the Bill explicitly prohibits the creation of any systemic weaknesses or backdoors to encryption.

269. The Bill is consistent with overseas approaches to the challenges imposed by technological environment to law enforcement and national security agencies.

270. The Bill reflects the outcome of an extensive two-stage consultation process which allowed the Government to engage with industry on a confidential basis and provide key public stakeholders with an opportunity to provide comment. This process was productive and led to significant amendments to the Bill to address key concerns raised and reinforce the policy intent of the Bill.

271. The Home Affairs Portfolio acknowledges the importance of the Committee's review process and would like to thank members for scrutinising the Bill.

Australian Government
Department of Home Affairs

CHALLENGES FACED BY STATE LAW ENFORCEMENT AGENCIES - ATTACHMENT A

Victoria

This example relates to a high risk Registered Sex Offender (RSO). He was placed on the register for raping a 16 year old female, served 9 years imprisonment and is now monitored by Corrections via 2 ankle bracelets whilst out on parole. Police received intelligence that he was breaching his RSO and Parole conditions by contacting a number of females typically between 13 and 17 years of age. Police enquiries showed that he was contacting these females, offering them drugs and asking for sexual favours in return. On 25th June 2018 police executed a search warrant and arrested him. His mobile phone was seized and despite legislative requirements, has refused to provide his passcode. Due to an inability to access his phone as well as the fact that he used encrypted communication methods such as Snapchat and Facebook Messenger, police were unable to access evidence which would secure a successful prosecution or help identify further victims and offences. These are high victim impact crimes that are being hindered by the inability for law enforcement to access encrypted communications.

Western Australia

In a drug investigation case police recovered a Blackberry device which was found to be operating the Phantom Secure, P2P encryption software. When seized the device was locked with the encryption key. The arrested person cooperated with police and afforded access to the device. Having access to the device enabled investigators to: identify the safe house; the safe house occupier and the overall supplier/coordinator of half a kilogram of methylamphetamine; make a series of further arrests and refer further charges. Given that the drug syndicate felt confident in the encryption software the content of the messages was very matter of fact and forms a significant part of the brief of evidence against the accused persons. Without access to this encrypted device the overall supplier would never have been identified, let alone charged.

Following the arrest of a homicide suspect, attempts were unsuccessful to download encrypted 'Whats App' messages that were used by her to communicate with her co-accused during the time of the murder. It is believed that this encrypted data contained a confession by one of the co-accused however this could not be retrieved once the messages were deleted from the phone within the application.

South Australia

A significant investigation into child exploitation and related sex offences was conducted and quickly became national news regarding abuse in State care. An online associate of the principal target was actively involved in the possession and dissemination of Child Exploitation Material (CEM) and was charged and convicted for related offences. During the course of the investigation the exhibits seized from this associate were either encrypted or

forensically wiped, so no data could be obtained from these devices despite specialist analysis by an eCrime specialist. The associate later provided passwords through his lawyer, but these passwords did not work on the computers and as a result he was sentenced on his admissions to what was on the drives and on the basis he never provided useful passwords to police. Investigators are of the firm belief that the encrypted data holds further significant CEM that the offender does not want accessed. It isn't only the desire of police to identify further offending committed by the associate but more importantly to identify further victims who likely require support and help as a result of the abuse they have suffered.

Australian Government
Department of Home Affairs

FIVE EYES STATEMENT OF PRINCIPLES ON ACCESS TO EVIDENCE AND ENCRYPTION – ATTACHMENT B

Preamble

The Governments of the United States, the United Kingdom, Canada, Australia and New Zealand are committed to personal rights and privacy, and support the role of encryption in protecting those rights. Encryption is vital to the digital economy and a secure cyberspace, and to the protection of personal, commercial and government information.

However, the increasing use and sophistication of certain encryption designs present challenges for nations in combatting serious crimes and threats to national and global security. Many of the same means of encryption that are being used to protect personal, commercial and government information are also being used by criminals, including child sex offenders, terrorists and organized crime groups to frustrate investigations and avoid detection and prosecution.

Privacy laws must prevent arbitrary or unlawful interference, but privacy is not absolute. It is an established principle that appropriate government authorities should be able to seek access to otherwise private information when a court or independent authority has authorized such access based on established legal standards. The same principles have long permitted government authorities to search homes, vehicles, and personal effects with valid legal authority.

The increasing gap between the ability of law enforcement to lawfully access data and their ability to acquire and use the content of that data is a pressing international concern that requires urgent, sustained attention and informed discussion on the complexity of the issues and interests at stake. Otherwise, court decisions about legitimate access to data are increasingly rendered meaningless, threatening to undermine the systems of justice established in our democratic nations.

Each of the Five Eyes jurisdictions will consider how best to implement the principles of this statement, including with the voluntary cooperation of industry partners. Any response, be it legislative or otherwise, will adhere to requirements for proper authorization and oversight, and to the traditional requirements that access to information is underpinned by warrant or other legal process. We recognize that, in giving effect to these principles, governments may have need to engage with a range of stakeholders, consistent with their domestic environment and legal frameworks.

Principles

The Attorneys General and Interior Ministers of the United States, the United Kingdom, Canada, Australia and New Zealand affirm the following principles in relation to encryption.

1. Mutual Responsibility

Diminished access to the content of lawfully obtained data is not just an issue for Governments alone, but a mutual responsibility for all stakeholders.

Providers of information and communications technology and services - carriers, device manufacturers or over-the-top service providers -– are subject to the law, which can include requirements to assist authorities to lawfully access data, including the content of communications. Safe and secure communities benefit citizens and the companies that operate within them.

We are always willing to work with technology providers in order to meet our public safety responsibilities and ensure the ability of citizens to protect their sensitive data. Law enforcement agencies in our countries need technology providers to assist with the execution of lawful orders. Currently there are some challenges arising from the increasing use and sophistication of encryption technology in relation to which further assistance is needed.

Governments should recognize that the nature of encryption is such that that there will be situations where access to information is not possible, although such situations should be rare.

2. Rule of law and due process are paramount

All governments should ensure that assistance requested from providers is underpinned by the rule of law and due process protections.

The principle that access by authorities to the information of private citizens occurs only pursuant to the rule of law and due process is fundamental to maintaining the values of our democratic society in all circumstances – whether in their homes, personal effects, devices, or communications. Access to information, subject to this principle, is critical to the ability of governments to protect our citizens by investigating threats and prosecuting crimes. This lawful access should always be subject to oversight by independent authorities and/or subject to judicial review.

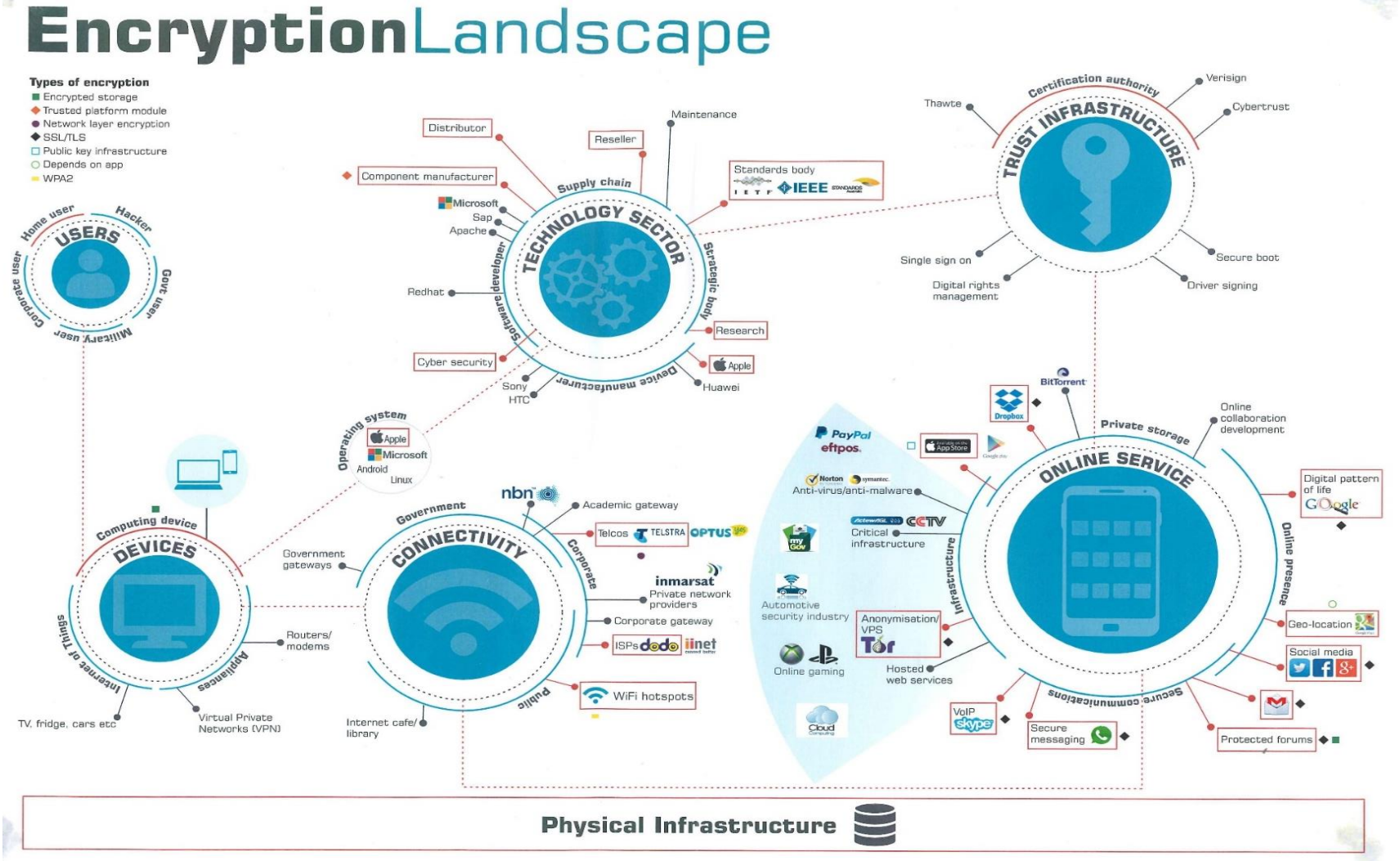
3. Freedom of choice for lawful access solutions

The Governments of the Five Eyes encourage information and communications technology service providers to voluntarily establish lawful access solutions to their products and services that they create or operate in our countries. Governments should not favour a particular technology; instead, providers may create customized solutions, tailored to their individual system architectures that are capable of meeting lawful access requirements. Such solutions can be a constructive approach to current challenges.

Should governments continue to encounter impediments to lawful access to information necessary to aid the protection of the citizens of our countries, we may pursue technological, enforcement, legislative or other measures to achieve lawful access solutions.

Australian Government
Department of Home Affairs

ENCRYPTION DIAGRAM – ATTACHMENT C



EXAMPLES – INDUSTRY ASSISTANCE SUPPORTING AGENCIES – ATTACHMENT D

Assistance in generating an historical online presence

Policing Dark Net environments increasingly requires an ability to engage in online forums and illegal markets. To do this successfully considerable resources are invested in developing covert strategies to ensure authenticity of any engagement. The support of online providers to establish an authentic online presence can substantially assist in disrupting the trade in illegal goods and services, the exchange of child exploitation material and the identification of those encouraging others to radicalise and participate in terrorist activities. In this example, a technical assistance notice may be issued. Where existing systems require some modification, the Attorney-General may issue a technical capability notice.

Ability to monitor the location of a phone

The ability to find the location of a mobile phone is a valuable investigative tool for law enforcement. For instance, where a child has been abducted by a relative, location tracking provides valuable information which can further inform investigators and assist physical surveillance activity. However, at present only some Australian telecommunications carriers have the network infrastructure to support the AFP in providing this near real time location information. For those instances where the suspect has a mobile service on one of the Australian telecommunications carriers without this capability, use of a technical capability notice would be extremely beneficial and would help ensure the child could be recovered prior to being removed from the state or country. Tracking of targets would be supported by data authorisations under the *Telecommunications (Interception and Access) Act 1979*.

Ability to degrade or migrate a deliberate encrypted communication device to another network

Recent media coverage around the disruption of Phantom Secure, who provided modified Blackberry's to facilitate criminal activity, highlighted that Australia had the highest level of usage of these devices in the world (at over 10,000). This proliferation of use in Australia is perpetuated by the inability of Law Enforcement to secure the support of telecommunications carriers to degrade, block or track these devices. With these devices employing international roaming SIM cards they roam between telecommunications carriers including to those that cannot provide real-time location monitoring to support alternative surveillance activities. A technical assistance notice or technical capability notice would assist in securing the support of telecommunications companies to provide increased identification, monitoring and tracking of these devices.

Ability to access cloud based services

The increasing use of cloud services to communicate, store and backup information makes access to these cloud services a valuable source of evidence. The ability to directly access

these services during the search of a premise pursuant to a lawful search warrant is a power that is already conferred to the AFP. Perpetrators, including those who are part of paedophile networks, organised crime syndicates or terrorist cells, are not always willing to furnish the passwords to provide access, even when served with an order to do so. A technical assistance notice could assist by the communications provider re-setting a password to facilitate timely access to cloud based backups, data and communication services (including closed forums). This could enable the identification of evidence, other participants and even disrupt planned activity.

Australian Government

Department of Home Affairs

EXAMPLES – TYPES OF INDUSTRY ASSISTANCE THAT CAN BE REQUESTED UNDER 317E – ATTACHMENT E

Operational examples from law enforcement agencies:

Sub section 317E(1)	Listed act or thing	Examples
(a)	Removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider.	- Requesting an ISP provide the password they have enabled on a customer supplied home modem to facilitate a review of its logs during a search warrant to identify connected devices. - Requesting a cloud storage provider changes the password on a remotely hosted account to assist with the execution of an overt account based warrant.
(b)	Providing technical information	- An application provider providing technical information about how data is stored on a device (including the location of the encryption key) to enable forensically extracted data to be reconstructed. - An international cloud hosted storage provider providing details of where a customer's data is hosted to enable a

Sub section 317E(1)	Listed act or thing	Examples
		MLAT process to be progressed to the host country seeking lawful access. - A mobile device provider providing a copy of their WiFi AP location maps generated through bulk analysis of customers data to correlate with location records extracted during a forensic examination of a device.
(d)	Ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format.	- Requesting a cloud service provider provide a copy of the contents of a hosted account in a particular format pursuant to the execution of an overt account based warrant. - Requesting that data held in a proprietary file format extracted from a device during a forensic examination pursuant to an overt search warrant is converted into a standard file format.
(e)	Facilitating or assisting access to that which is the subject of eligible activities of the provider including, a facility, customer equipment, an electronic service etc.	- Requesting a shared data centre provide access to customers computer rack to enable the execution of a computer access warrant or installation of a data surveillance device under warrant.
(f)	Assisting with the testing, modification, development or maintenance of a technology or capability.	- Requesting that a social media platform assist with testing or development of a tool to automate the creation of online personas and historical content to facilitate online engagement.
(g)	Notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes	- Requesting an ISP advise of any technical changes to their network which could impact on an existing interception.

Sub section 317E(1)	Listed act or thing	Examples
	are relevant to the execution of a warrant or authorisation.	
(h)	Modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider.	- Requesting a carrier increase the data allowance on a device that is subject to a surveillance device warrant to enable the surveillance device to be remotely monitored without consuming the targets data. - Temporarily blocking internet messaging to force a device to send the messages as unencrypted SMS's.
(i)	Substituting, or facilitating the substitution of, a service provided by the designated communications provider for: another service provided by the provider; or a service provided by another designated communications provider.	- Requesting a carrier force a roaming device to another carriers network to enable the enhanced metadata collection capabilities of the new carrier to collect information pursuant to a prospective data authorisation.
(j)	An act or thing done to conceal the fact that anything has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to: - enforcing the criminal law and laws imposing pecuniary penalties; or - assisting the enforcement of the criminal laws in force in a foreign country; or	- Requesting that the provider not inform the customer of the assistance provided to enable a computer access warrant. - Requesting that the provider delete an audit log in a customer's device relating to a computer access warrant. - Requesting a provider restore a password that was temporarily changed to enable a computer access warrant. - Requesting a provider allocate a specific dynamic IP address relating to remote access pursuant to a computer access warrant to conceal the access.

Sub section 317E(1)	Listed act or thing	Examples
	- the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.	

Operational examples from intelligence agencies

Sub section 317E(1)	Listed act or thing	Examples
(a)	Removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider.	ASIO establishes physical access to a target's mobile phone and manages to acquire a copy of the phone's contents. The opportunity is rare and unique in that the target normally employs fairly good security awareness and tradecraft. Stored within the database of an application on the phone are historical conversations with other subjects of interest that indicate the group are in the initial stages of planning a mass casualty attack at an upcoming music festival. Unfortunately the copy of the phone's contents only reveals a snapshot in time of the targets' intentions and ASIO cannot formulate an informed assessment of the group's intended activities. The application used by the group stores messages on a server in the cloud and makes use of various authentication mechanisms to authorise access to user accounts, limiting ASIO's ability to establish contemporary coverage of the group. On seeking appropriate warrants authorising ASIO to lawfully gain coverage of the target's communications, ASIO seeks out the designated communications provider (DCP) with capacity to deactivate the relevant authentication mechanisms allowing, ASIO to authenticate the target's account to provide up-to-date and ongoing coverage of the group's intentions and threat to Australia's security.
(b)	Providing technical information	In the example above, once ASIO overcomes the relevant protection mechanisms to access the relevant communications, without further technical assistance from the DCP, ASIO could expend significant time and resources attempting to understand the structure of the database associated with the chat application. The database may be complex with messages, parties to a conversation and associated attached media all stored in different portions of the database making an assessment of the subjects involved in the plan and

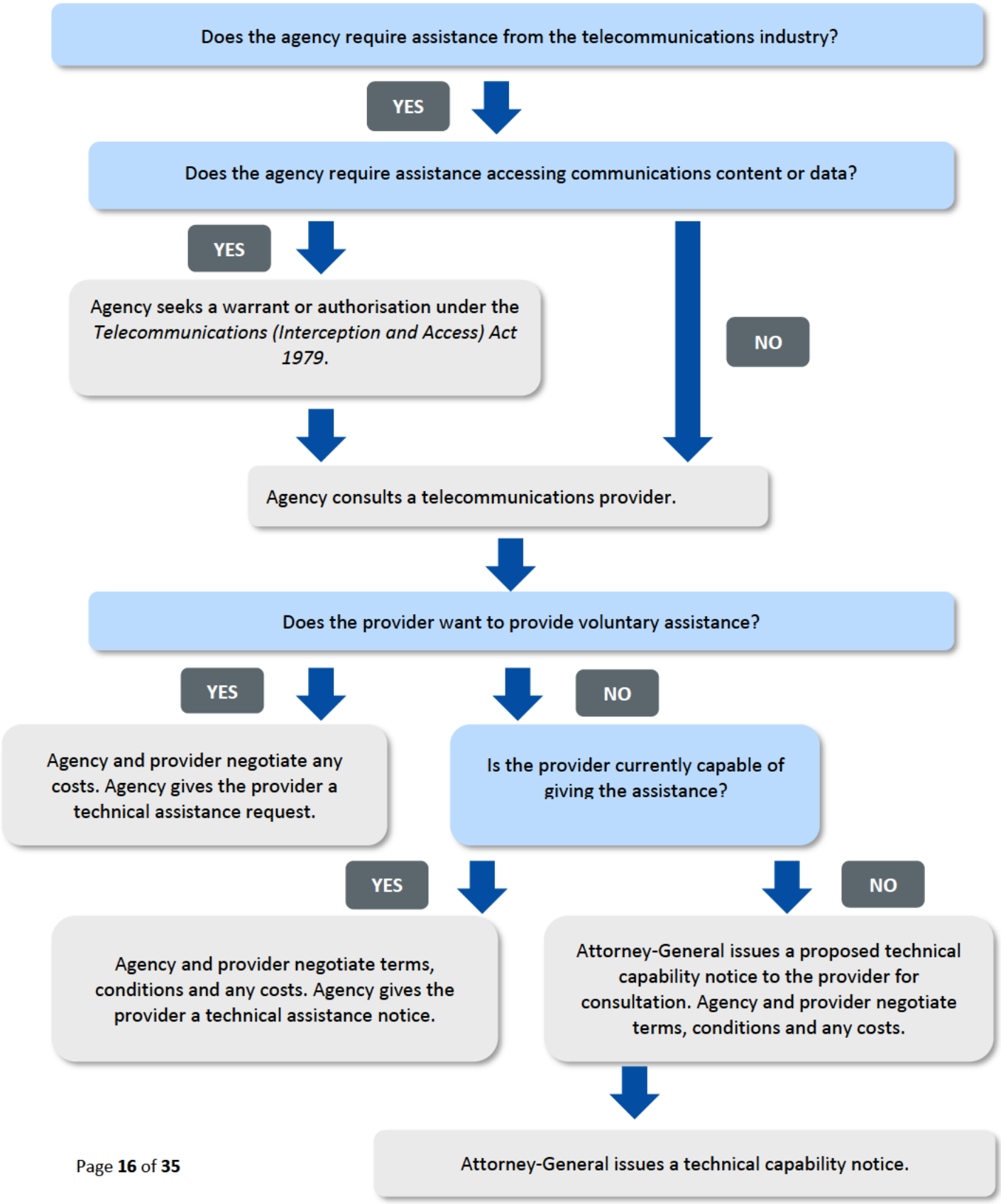
Sub section 317E(1)	Listed act or thing	Examples
		their intentions quite difficult. It could take ASIO months to organise the data in a legible format. Using a Technical Assistance Notice, ASIO would seek out the DCP responsible for the application to gather technical information about how the application makes use of a database to store local copies of communications that have been sent and received by the application, enabling efficient and timely analysis of the relevant communications.
(C)	Installing, maintaining, testing or using software or equipment	An anonymous call is placed to the National security Hotline indicating that a Terrorist cell is planning a bombing attack against the SMH Fun run in Sydney. ASIO receives this tip-off just two weeks before the event and only knows one of the group members involved. To avoid detection the group do not communicate via phone calls or face to face meetings but instead plan their attack online using application that encrypts messages as they are sent by users. Sent messages are received by the application's central server where they are decrypted and then re-encrypted with the intended recipient's key before being delivered to the intended recipient's device. ASIO secures an appropriate warrant and asks the communications provider to store copies of the target's communication before they are re-encrypted with recipient keys. To facilitate this, ASIO works with the DCP to install ASIO-controlled equipment that stores the communications. Interestingly, ASIO would store the communications in an encrypted format to prevent unauthorised access to the warranted material prior to it being disseminated back to ASIO.
(d)	Ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format.	ASIO may require that information data obtained by a carrier in response to a warrant be provided in a format that is compatible with ASIO's systems and allows for appropriate analysis.

Sub section 317E(1)	Listed act or thing	Examples
(e)	Facilitating or assisting access to that which is the subject of eligible activities of the provider including, a facility, customer equipment, an electronic service etc.	Further to the example above, ASIO, in conjunction with the DCP, identifies a physical data centre that represents the best location to acquire copies of the target's unencrypted communications; however, the data centre is owned and operated by a third-party company. ASIO in conjunction with the chat application DCP work with the data centre DCP to arrange appropriate rack space, power and cabling for the ASIO server equipment.
(f)	Assisting with the testing, modification, development or maintenance of a technology or capability.	Further to the example above, ASIO assesses that any perceivable impact on the target's electronic service (the chat application) may result in an acceleration of the target's attack planning because ASIO assess the target exhibits a heightened level of paranoia, is erratic and prone to violence. ASIO works carefully with the DCP to ensure that the installed equipment has no perceivable effects on the target's usage of the app and is entirely covert in its operation.
(g)	Notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation.	In the above example, the DCP intends to change the physical location of their infrastructure and notifies ASIO in advance of the change so ASIO can plan for the relocation of the ASIO equipment to ensure coverage of the target's communications is maintained.
(h)	Modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider.	It's feasible, in the example above, that ASIO's work with the DCP, ensuring that the installed equipment has no perceivable effects on the target's usage of the application, could require some modification, or substitution of, characteristics of a service provided by the DCP – or indeed, substitution of the service itself - in order to ensure the ongoing covert nature of ASIO's operation.
(i)	Substituting, or facilitating the substitution of, a service provided by the designated communications provider for: another service provided by the provider; or	

Sub section 317E(1)	Listed act or thing	Examples
	a service provided by another designated communications provider.	
(j)	An act or thing done to conceal the fact that anything has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to: - enforcing the criminal law and laws imposing pecuniary penalties - assisting the enforcement of the criminal laws in force in a foreign country; or - the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.	Further to the above example, it's also feasible that various other activities would be required to ensure the ASIO's operation remains covert, including: - Requiring that the assistance provided is kept confidential by the provider. - Asking the staff involved in providing the service to sign confidentiality agreements. - Requesting that a cover story to be adopted when explaining the nature of assistance being provided. - Adjusting billing, account access, data transfer logs etc. to hide evidence of access to a target device or service. - Facilitating covert physical access to a facility.

Australian Government
Department of Home Affairs

INDUSTRY ASSISTANCE FLOWCHART – ATTACHMENT F



Australian Government
Department of Home Affairs

DECISION-MAKING PROCESS – INDUSTRY ASSISTANCE – ATTACHMENT G

DECISION MAKING PROCESS – INDUSTRY ASSISTANCE							
		Voluntary / compulsory	**Decision maker**	**Purpose**	**Considerations as part of the decision-making process**	**Statutory limitations**	**Consultation / costs**
ASSISTANCE TYPE	***Technical Assistance Request (TAR)***	**Voluntary *(must advise that compliance with the request is voluntary)***	Chief officer of an interception agency (e.g. AFP Commissioner); Director-General of ASIS, ASD or ASIO	May ask the provider ***to do acts or things on a voluntary basis*** that are directed towards ensuring that the provider ***is capable of giving certain types of help*** in relation to '***relevant objectives***': i. Enforcing the criminal law and laws imposing pecuniary penalties; or ii. Assisting the enforcement of the criminals laws in force in a foreign country; or	Is the targeted provider a *'designated communications provider'*? Does the assistance requested relate to one or more: a. '*Relevant objectives*'? b. '*Listed act or things*'? Is the requested assistance in connection with any or all of the '*eligible activities*' of the provider? Does the assistance relate to the functions or powers of the agencies conferred under a law of the Commonwealth, State or Territory?	Must only be voluntary Immunities granted limited to civil actions and the '*eligible activities*' of the provider.	Law enforcement agencies may enter into contractual arrangements, including contracts of a financial nature.

				iii. The interests of Australia's national security, foreign relations or interests of Australia's economic well-being			
	Technical Assistance Notice (TAN)	**Compulsory**	Chief officer of an interception agency (e.g. AFP Commissioner) or the Director-General of ASIO.	May give a provider a notice which **requires** the provider to **do one or more specified acts or things that they can already do in relation to a function or power** which relates to '***relevant objectives'***: i. Enforcing the criminal law and laws imposing pecuniary penalties; or ii. Assisting the enforcement of the criminals laws in force in a foreign country; or iii. Safeguarding national security; or iv. Matter that facilitates, or is ancillary or incidental to, a matter covered under (i) – (ii).	Is the targeted provider a *'designated communications provider"*? Does the assistance requested relate to one or more: a. '*Relevant objectives"*? b. '*Listed act or things"*? Is the requested assistance in connection with any or all of the '*eligible activities'* of the provider? ***The decision-maker must not give a TAN unless they are satisfied that (Specific decision making criteria – s 317P):*** a. The requirements are '*reasonable*' and '*proportionate*'; and b. Compliance is '*practicable*' and '*technically feasible'*. In determining if a requirement is 'reasonable and proportionate', **must have regard** to (**s 317RA**): a. The interests of national security; b. The interests of law enforcement; c. The legitimate interests of a designated communications provider to whom the notice relates; d. The objectives of the notice; e. The availability of other means to achieve the objectives of the notice;	**Cannot require** a provider to implement or build a systemic weakness or vulnerability etc into a form of electronic protection. **Cannot prevent** a provider from rectifying a systemic weakness or vulnerability in a form of electronic protection. **Cannot require** a provider to do an act or thing for which a warrant or authorisation would be required under Commonwealth or State/Territory laws (e.g. provide content data which would usually be provided under a stored communications warrant).	Consultation would occur for a decision-maker to meet the thresholds o reasonableness, proportionality, practicability and technical feasibility. Must explain to a provider their obligations under a notice (**s 317MAA**) Law enforcement agencies may enter into contractual arrangements, including contracts of a financial nature.

					f. The legitimate expectations of the Australian community relating to privacy and cybersecurity; Any such other matter relevant as the case requires.		
	Technical Capability Notice (TCN)	**Compulsory**	Ministerial authorisation (Attorney-General)	May give a provider a notice which **requires** the provider to **do one or more specified acts or things in relation to a function or power of an agency** which relates to **'relevant objectives':** i. Enforcing the criminal law and laws imposing pecuniary penalties; or ii. Assisting the enforcement of the criminal laws in force in a foreign country; or iii. Safeguarding national security.	Is the targeted provider a *'designated communications provider'*? Does the assistance requested relate to one or more: a. *Relevant objectives'*? b. '*Listed help*? Is the requested assistance in connection with any or all of the '*eligible activities'* of the provider? ***The decision-maker must not give a TCN unless they are satisfied that (Specific decision making criteria – s 317V):*** a. The requirements are *'reasonable and proportionate'*; and b. Compliance is '*practicable*' and *'technically feasible'*. In determining if a requirement is 'reasonable and proportionate', **must have regard** to (**s 317RA**): a. The interests of national security; b. The interests of law enforcement; c. The legitimate interests of a designated communications provider to whom the notice relates; d. The objectives of the notice; e. The availability of other means to achieve the objectives of the notice;	**Cannot require** a provider to implement or build a systemic weakness or vulnerability etc into a form of electronic protection. **Cannot require** a provider to build a capability for the purpose of removing a form of electronic protection. **Cannot prevent** a provider from rectifying a systemic weakness or vulnerability in a form of electronic protection. **Cannot require** a provider to do an act or thing for which a warrant or authorisation would be required under Commonwealth or State/Territory laws (e.g. provide content	**Must not give a TCN** unless the AG has undertaken a **consultation process** and considered a submission from the provider and any technical expert engaged. Must explain to a provider their obligations under a notice (**s 317TAA**) Law enforcement agencies may enter into contractual arrangements, including contracts of a financial nature.

					f. The legitimate expectations of the Australian community relating to privacy and cybersecurity; g. Any such other matter relevant as the case requires. Consultation is part of the decision-making process.	data which would usually be provided under a stored communications warrant).	
					Ministerial declaration for '*listed help*' The Minister may, by legislative instrument, determine one or more kinds of '*acts or things*'. In making a determination, the Minister must have regard to: a. The interests of law enforcement; b. The interests of national security; c. Objects of the Telecommunications Act; d. Likely impact of the determination on a provider; Other such matters (if any) considered relevant.		

Australian Government
Department of Home Affairs

REVISIONS MADE FOLLOWING CONSULATION – ATTACHMENT H

Industry Consultation		
Issue	***Recommendation***	***Change***
Systemic weakness	Strengthen the limitation against building a systemic weakness ('backdoor').	The Bill was amended so that providers cannot be asked to build or *implement* a systemic weakness into *any* form of electronic protection. The Bill now clarifies that building a systemic weakness includes any action that would make systems of authentication *less* effective.
Limitation on content or data	Clarify that a notice cannot require any provider (foreign or domestic) to produce telecommunications content or data without a warrant or authorisation under the existing regime.	The Bill was amended to ensure that the limitations agencies are subject to in Australian law applies also to their dealings with offshore provides.
Transparency	Allow companies to publish statistical information about notices for transparency reports.	The Bill was amended so that it is an exception to the unauthorised disclosure offence for a company to disclose the number of notices given to the company.
Standards and benchmarks	Remove the provisions that allows the Minister for Home Affairs to determine standards and benchmarks to address interception capability standards. Existing mechanisms can address substandard interception capabilities.	Provisions that allowed the Minister for Home Affairs to determine standards and benchmarks to address interception capability standards have been removed from the Bill.
Ministerial determinations of additional types of assistance	Include conditions on the Minister for Home Affairs' ability to specify additional types of assistance that an agency may seek under a notice.	The Bill has been amended so that the Minister is required to consider a number of factors before making a legislative instrument determining a new type of assistance that may be required by agencies under a notice. The Minister must consider: • The interests of law enforcement • The interests of national security • The objects of the *Telecommunications Act 1997* • The likely impact on providers

Oral requests and notices	Ensure that notices and requests are given in writing except in emergency circumstances.	The Bill has been amended to require requests and notices to be in writing. They can be provided orally if an imminent risk of harm to a person exists and the request or notice is necessary to deal with the risk.
Notice expiry	Ensure that the requirements under a notice cannot continue indefinitely.	The Bill has been amended to provide that a technical assistance notice expires after 90 days unless otherwise specified. The Bill has been amended to provide that a technical capability notice expires after 180 days unless otherwise specified.

Public Consultation		
Issue	***Recommendation***	***Change***
Reasonable and proportionate	Specify what the agency must consider in deciding whether a notice is 'reasonable and proportionate.'	The Bill has been amended so that an agency must consider the following matters in deciding whether a notice is 'reasonable and proportionate': • The interests of law enforcement • The interests of national security • The legitimate interests of the provider • The objectives of the notice • The availability of other means to achieve those objectives • The legitimate expectations of Australians relating to privacy and cybersecurity
Powers of a court	Ensure courts may make any orders to protect information under a notice.	The Bill has been amended to reflect the discretion of the court to make orders to protect information if the court is satisfied it is in the public interest to make such orders (which includes the commercial interests of providers).
Technical advice	Enable independent technical experts to scrutinise a technical capability notice to provide advice on whether it may cause a systemic weakness.	The Bill has been amended to enable the Attorney-General and provider to, by agreement, seek the technical advice of an expert in the consultation period for the purpose of determining whether the requirements of a notice may cause a systemic weakness.
Helping providers by explaining obligations	Ensure that the Bill does not disadvantage smaller providers who may not understand their legal obligations under a notice.	The Bill has been amended to require agencies to explain a provider's obligations under a notice. Where an agency makes a voluntary request, the agency must advise the provider that compliance is entirely voluntary.
Protecting the public revenue	Amend the Bill to remove 'protecting the public revenue' from the list of	'Protecting the public revenue' has been removed from the list of objectives for which a notice may be issued. Notices may only be issued for the

	relevant objectives for which a notice may be issued.	purposes of enforcing the law and protecting national security.
Annual Reports	Require the reporting of the number of Technical Assistance Requests in the financial year to be included for annual reporting purposes.	The Annual reporting section of the Bill has been amended to add Technical Assistance Requests to the requirement for Technical Assistance Notices and Technical Capability Notices which are required to be reported in the *Telecommunications (Interception and Access) Act 1979* Annual Report
Extraterritorial effect	Introduce a provision that deals with the potential for a company to face a conflict in complying with a notice and the laws of a foreign jurisdiction	The Bill was amended so that a defence is available where a company is prosecuted for non-compliance with a notice and, at the time the notice was given, the company would have breached foreign laws in order to comply with the notice
Limitation on content or data	Remove the ambiguity over whether the new powers may be used to require a provider hand over personal information or do a thing that a warrant or authorisation would be required for.	The Bill was amended to extend the limitation in section 317ZH to include any law of a Commonwealth, State or Territory. The result is that the new powers in Schedule 1 will have no effect if a warrant or authorisation would otherwise be required under an Australian law.

Australian Government
Department of Home Affairs

CONSULTATION THEMES AND DEPARTMENT RESPONSE – ATTACHMENT I

This document summarises the main concerns identified during the public consultation process and notes the response from the Department of Home Affairs. These concerns were overwhelming targeted at Schedule 1 of the Bill. Specific themes include:

1. The risk of so-called 'backdoors'
2. Oversight arrangements
3. Decision-making criteria for exercising the powers
4. Protections against unauthorised disclosure
5. Purposes for which the powers may be exercised
6. Scope of providers captured
7. Impact on privacy

1. The risk of so-called 'backdoors'

A number of public submissions received during the consultation process highlighted key concerns around the fact that section 317ZG of the draft Bill provided that a TAN or TCN must not require a DCP to implement or build a systemic weakness or systemic vulnerability into a form of electronic protection. The most commonly cited concern on this proposed section of the Bill centred on the notion that a clear definition of 'systemic weakness' is not included within the text of the Bill itself.

This concern was specifically raised by the United Nations Special Rapporteur on the Promotion and protection of the right to freedom of opinion and expression, the Australian Human Rights Council, Access Now, the Office of Australian Information Commissioner, the Office of the Victorian Information Commissioner, the Communications Alliance, the Internet Architecture Board, the University of Melbourne and a joint submission compiled by Digital Rights Watch. These submissions were often accompanied with a recommendation that the legislation be redrafted to include a clear, precise and broad definition of 'systemic weakness'.

Another concern common to multiple submissions was the belief that any capability to facilitate access amounts to a systemic weakness, by definition. These concerns were specifically raised by Cog Systems and MIT's Internet Policy Research Initiative, which were also accompanied by security concerns over the overall impact of the Bill. These concerns were mirrored in a variety of ways by many other submissions received. MIT was specifically concerned that the lack of transparency surrounding TCNs would impede the public's ability to evaluate if a notice requires systemic weaknesses or vulnerabilities to be installed.

Some public submissions also noted that the Bill's section 317ZG provision prohibiting systemic weaknesses and vulnerabilities being built does not apply to TARs. These submissions considered that the prohibition should be expanded to include TARs for the purpose of ensuring the integrity of encryption systems is maintained regardless of the voluntariness of the provision of technical assistance. Submissions made by Internet Australia and the University of Melbourne also included these concerns.

Response

For the purposes of proposed section 317ZG, the term 'system' encompasses interacting or interdependent items that form a unified whole. The term 'systemic' is intended to refer to matters 'relating to a system' rather than a particular part. The purpose and meaning of the provision is clear in the text of the Bill, and is further described in the Explanatory Memorandum to the Bill. As the ordinary meaning reflects the appropriate operation of the limitation, it is not necessary to establish a definition.

Proposed section 317ZG prevents a weakness or vulnerability from being built into a single item (like a target service or device) if it would undermine the security of other, interconnected items. That is, where the weakness in one part of the system would compromise other parts of the system or the system itself. The term 'systemic' does not include weaknesses or vulnerabilities that could be isolated to a particular device (access to which would be subject to an underlying warrant). Rather, the provision prohibits a TAN or a TCN that purports to impact forms of electronic protection on non-target services and devices.

The term 'electronic protection' captures encryption methods, password protections and other forms of security. As the meaning of the term is clear in the text of the Bill, and is further described in the Explanatory Memorandum to the Bill, it is not necessary to establish a definition.

While Home Affairs considers that a DCP itself is best placed to determine what changes to their systems would have the potential to create a systemic weakness or vulnerability, the need for external evaluation of a TCN was acknowledged. Accordingly, a new provision was introduced (proposed subsections 317W(7) – (11)) to allow the Attorney-General and a DCP to jointly appoint a person with technical expertise to undertake an assessment of whether the requirements in a TCN would contravene proposed section 317ZG. The intent of the change was to facilitate scrutiny by the technical community whilst appropriately protecting sensitive law enforcement and national security capabilities as well as sensitive commercial information that will relate to a TCN. In any case, if a DCP believes that a notice would contravene proposed section 317G they may refer the decision to issue a TCN for judicial review which would provide an opportunity for expert evidence to be tendered regarding the cybersecurity implications of compliance.

Home Affairs also notes that the prohibition in proposed section 317ZG is complimented by two key limitations in both the TAN and TCN provisions. A TAN cannot require a provider to do a thing they are not already capable of doing, therefore its potential to implement systemic weaknesses in a system is limited by the fact that these weaknesses would likely need to be created by a new capability. A TCN cannot require the construction of a capability to remove a form of electronic protection and is thus limited in the requirements it may impose that cause direct flaws in forms of electronic protection.

Given their voluntary nature, and the changes made that require a decision-maker to notify a receiving DCP of the voluntary nature of a TCN, it was not considered necessary to extend the prohibition in proposed section 317ZG to TARs.

2. Oversight arrangements

During the consultation several industry and civil society groups raised concerns that the Bill lacks oversight of the technical assistance powers it grants to law enforcement. Of the kinds of oversight mentioned, most frequently submissions were concerned with the lack of a

requirement to seek judicial authorisation before a notice could be issued. This issue was raised by the UN Rapporteur on Freedom of Expression who is concerned that the lack of a "warrant or oversight process" for the issuance of a notice in Schedule 1 creates broad discretion for the exercise of these powers. The desire for an independent judicial authority to authorise notices was also shared by DIGI.

Similarly the Australian Human Rights Commission and a joint submission compiled by Digital Rights Watch considered that there was insufficient justification for the lack of a warrant regime or independent oversight over the power to issue notices. Additionally, Salesforce.com was concerned that the provider be given an avenue to challenge the issuance of a notice.

Some submissions, those by Human Rights Watch, the Australian Human Rights Commission, the Australian Information Commission, the Office of the Victorian Information Commissioner, the (Queensland) Office of the Information Commissioner, the Communications Alliance, Digital Rights Watch and Ai Group were also concerned that the lack of 'judicial oversight' of the Bill departed from the standard set by the UK IPA which some bodies considered to provide similar powers to British government agencies. The UK IPA created an independent statutory agency with judicial functions to authorise the issuance of notices and this is the approach preferred by some of the bodies consulted.

The express exclusion of merits review of decisions made under the Bill was criticised by Human Rights Watch and the Australian Human Rights Commission who were concerned that judicial review's limited ability to review the character of a decision would not provide a sufficient avenue to properly appeal a decision made under the Bill. Human Rights Watch considered that the legal protections available at judicial review are not broad enough to protect rights infringed by the Bill's new powers. The Australian Human Rights Commission was further concerned that the exclusion of judicial review under the legislative pathway provided by the ADJR Act makes judicial review less accessible and efficient than might otherwise be possible.

The Commonwealth Ombudsman noted the autonomy of law enforcement to make decisions under the Bill and suggested that "independent oversight" of the powers be provided for potentially by the Commonwealth Ombudsman acting in a role similar to their oversight of the metadata retention regime. The (Queensland) Office of the Information Commissioner suggested independent oversight could also be provided by appointing a Public Interest Monitor or engaging the Independent National Security Legislation Monitor.

The Australian Human Rights Commission suggested that more extensive reporting requirements be implemented to provide a "disaggregated summary of notices that is sanitised or redacted as necessary" and suggested this include the numbers of notices in force and expired and the number of notices varied, and indicate if any notices are facing legal challenge. The (Queensland) Office of the Information Commissioner suggested extending reporting to include areas contemplated by the UK IPA, namely: "errors; the number and type of all TARs, TANs and TCNs; and purpose, nature, source of authority and outcomes of TARs, TANs and TCNs". Similar suggestions were made by Future Wise.

The Commonwealth Ombudsman suggested that an exception be created to the non-disclosure provisions to allow the Ombudsman to review "information" regarding Schedule 1 requests and notices. A joint submission from Digital Rights Watch and another joint submission from the Communications Alliance both suggested the number of TARs be

published alongside TAN and TCN data in the annual report alongside information indicating how many TARs are complied with and how many are “escalated” to a notice.

Response

Home Affairs reinforces the distinction between technical assistance and the collection of personal information, including private communications and data. Through the combined operation of proposed section 317ZH, the limits on the things listed in proposed section 317E, the decision-making criteria and the interpretive capacity of the Explanatory Memorandum, the Bill creates a clear prohibition on a TAN or TCN from being able to act in substitution of a warrant or authorisation used to undertake otherwise unlawful collection of personal information. It is appropriate that the ability to access content in a device or service remain subject to judicial oversight which is well-placed to make determinations as to privacy and proportionality.

In contrast (and consistent with established obligations for industry assistance in section 313 of the *Telecommunications Act 1997*), technical assistance and core considerations regarding national security and law enforcement needs are appropriately determined by senior administrative decision-makers. Judicial officers do not have a dedicated role to assess and decide technical administrative decisions, many of which are anticipated to be of a complex, mechanical nature. Further, ministerial authorisations for national security decisions are an established feature of the Australian legislative landscape and, for example, govern decision to issue intelligence collection warrants or make determinations regarding the security of telecommunications systems (see item 13, section 315B of the *Telecommunications and Other Legislation Amendment Act 2017*). As noted elsewhere in this submission, decision-makers must meet significant thresholds and their decisions are subject to numerous limitations and global safeguards.

The similarities and differences between the UK IPA and the Bill are discussed extensively above, including the reasons behind why the Home Affairs has decided not to adopt a ‘double-lock’ approach.

As discussed elsewhere in this submission, a DCP is able to seek judicial review of any administrative decision to issue a notice. There are therefore multiple grounds by which to challenge a notice, including where a TAN or TCN creates broader vulnerabilities in networks or where it is infeasible that the decision-maker could consider requirements to be reasonable or proportionate. Depending on circumstances, a State court, the Federal Court or the High Court may preside over a review of the lawfulness of a decision.

Requirements under a TAN or TCN and the circumstances in which they are issued will involve sensitive information relevant to ongoing investigations. It is an established principle that national security and law enforcement decision-making are unsuitable for merits review. This has been recognised by the Administrative Review Council in its publication *What decisions should be subject to merits review?* The express exclusion of review under the ADJR Act is consistent with the existing exclusion of other national security and law enforcement legislation, like the TIA Act and ASIO Act and reflect the serious circumstances in which these powers are used and the need for timely execution.

As noted elsewhere in the submission, the Bill allows for the disclosure of information about the scheme to allow the Commonwealth Ombudsman, State Ombudsman and integrity bodies and the IGIS to discharge their existing oversight functions. These bodies retain the capacity to initiate investigations on their own volition into agency misconduct and the underlying legislative regimes that these powers will be used in connection with these

powers, such as the TIA Act, are already subject to extensive independent oversight. The Independent National Security Legislation Monitor's (INSLM) function is to review the operation of legislation upon referral by Government. If this Bill is passed, it is then open to the Government to refer it for INSLM review.

The TIA Act and SD Act establish extensive reporting and inspection requirements for the use of powers that will be supported by Schedule 1 of the Bill, including interception, the use of surveillance devices and stored communications warrants, as well as authorisations for telecommunications data. These reports must note numbers, errors and other warrant details (including warrants issued as a result of mutual assistance applications). As noted above, this Bill is not a mirror of the UK IPA. That Act sets out an extensive range of electronic investigative powers, the Australian equivalents of which are spread across a range of Acts that each provide for their own safeguards, oversight and reporting arrangements.

The Bill provides for both transparency reporting by DCPs in receipt of a TAN, TAR or TCN as well as annual reporting of the same notices. TARs were included in the annual reporting scheme in response to public feedback.

3. Decision-making criteria for exercising the powers

A number of public submissions made reference to the decision-making criteria employed when an interception agency issues a TAN or TCN to a DCP. Submissions received by both Human Rights Watch and DIGI Group both asserted that the decision-making process should be conducted by an independent judge rather than those decision-makers referred to in the Bill.

Additional decision-making criteria were suggested in a variety of submissions. The Law Council of Australia and Australian Human Rights Commission argued that costs accrued on behalf of the DCP should be taken into account as an independent criterion. The Australian Human Rights Commission also argued that decision-makers be required to consider the impact a notice will have on the 'right to privacy'. The Australian Human Rights Commission and a joint submission compiled by Digital Rights Watch argued that the decision-making criteria should include consideration of the public interest as well as the impact on the integrity of Australia's digital infrastructure, and should provide for the decision-maker to consult with technical professionals with suitable qualifications in making such a decision.

Submissions received by the United Nations Special Rapporteur on the Promotion and protection of the right to freedom of opinion and expression, the Office of the Victorian Information Commissioner, The Software Alliance and Kaspersky Labs all argued that the subjective nature of the decision-making process afforded decision-makers with unbounded discretion. They argue this impugns the integrity of the process of issuing notices under the Bill. The Software Alliance and Cog Systems both expressly stated that the subjectivity of decision-making was inappropriate for the circumstances laid out in the draft legislation.

Submissions from the Australian Human Rights Commission, the Office of Australian Information Commissioner and a joint submission compiled by Digital Rights Watch also asserted that the decision-making criteria attached to TANs and TCNs should also apply to voluntary TARs.

A joint submission compiled by the Communications Alliance as well as submissions received from Future Wise and Kaspersky Labs cited concerns that the consultation process

required when issuing a TCN was loosely defined. It was argued that this would lead to a lack of transparency and effective communication between interception agencies and DCPs.

Optus recommended that decision-makers be required to have regard to information submitted by a service provider in forming judgements about whether the decision-making criteria of "reasonable, proportionate, practicable and technically feasible" are met for each type of assistance request or notice.

Response

Decision-making under Schedule 1 of the Bill is restricted to senior government officials or occurs at a Ministerial level. A TAN is issued by the chief officer of an interception agency, the Director-General or their delegate (the list of delegates in proposed section 317ZR ensures that only senior executives in an organisation may be a delegate). The decision to issue a TCN is exercised by the Attorney-General. It is not common place for the judiciary to make administrative decisions of a national security and law enforcement nature that go to the technical requirements of an agency and investigation.

The type of judgments that may go to forming the requirements in a notice will require a deep appreciation for the current threat environment, the limitations in agency capabilities, agency operating budgets, the political and strategic context of the investigation and well as other tangible challenges. The direct purpose of a TAN or TCN is to meet investigative needs and senior decision-makers or a responsible Minister are recognised as being best placed to determine the most reasonable and proportionate means of achieving an effective outcome.

The subjective nature of the decision making requires the decision-maker to actually be satisfied that the requirements imposed by a notice are reasonable and proportionate and that compliance with the notice is practicable and technically feasible. Case law notes that this satisfaction must be informed on the correct understanding of the law – decision-makers cannot take into account matters which would be extraneous to any objects the legislature could have had in view.[1] This is not unbounded discretion - if, for example, a DCP provided clear and timely information that requirements in a notice were not technically feasible or the impact of the notice was unduly severe and the decision-maker ignored those concerns, a cogent case could be made in review that the decision-maker did not in fact reach the requisite state of mind.

Given the need for a decision-maker to have actually formed a state of mind as to the reasonableness and proportionality of the notice, it is unlikely to expect that a decision-maker could have considered the interests of the DCP without prior consultation. Further, given the technical nature of requirements, a decision-maker could not be satisfied that requirements are technically feasible without having a prior understanding of a DCP's system infrastructure and capabilities – information that would have to be gained through consultation with a DCP.

Section 313 of the *Telecommunications Act 1997* establishes an objective standard for industry assistance. As noted in the above submission, this objective standard has led to notable cases of uncertainty and frustrated legitimate investigations because it places members of industry in a position to determine what is reasonably necessary for a criminal or national security investigation. Home Affairs suggests that industry expertise rests in

[1] *Minister for Immigration and Multicultural Affairs v Eshetu* (1999) 193 CLR 611 at 651-654; *Water Conservation and Irrigation Commission (NSW) v Browning* (1947) 74 CLR 492 at 505.

commercial operations and technical competency – it does not extend to evaluating the threat environment and determining the necessity of agency actions.

Given the voluntary nature of TARs, Home Affairs does not consider it necessary to apply the strict decision-making thresholds of a TAN or TCN to its exercise. The request itself is bounded by the proper functions of the issuing agency, restricted to set activities of a provider and limited to the prosecution of an agency's core purposes as established by statute. Amendments made as a result of public consultations require an issuer to explicitly note that a TAR is voluntary (see proposed section 317HAA).

As changes made as a result of public feedback make clear, in deciding whether a notice is reasonable and proportionate, the decision-maker must have regard to the legitimate interests of the relevant DCP, the availability of other means to achieve the notice and the privacy and cybersecurity expectations of Australians (proposed sections 317RA and 317ZAA explain).

4. Protections against unauthorised disclosure

Stakeholders have raised concerns that the Bill does not provide protections or exemptions for the disclosure of information in certain circumstances particularly those that relate to the public interest. These concerns primarily relate to proposed section 317ZF which creates an offence when certain persons, including DCPs and their employees, disclose information in relation to TARs, TANs and TCNs.

The University of Melbourne and the Australian Human Rights Commission suggest that criminal penalties only attach to the intentional unauthorised disclosure of information that harms, or that is reasonably likely to harm, an essential public interest. The Australian Human Rights Commission considered that less serious conduct can be addressed by less restrictive measures such as administrative or contractual remedies. The Australian Human Rights Commission also recommends the Government include exemptions for the disclosure of information in relation to human rights violations and to allow for lawful public interest disclosures in relation to activities of agencies that do not fall within the scope of the IGIS Act. The University of Melbourne recommends for the Bill to be amended to allow for whistleblowing in cases of the improper use of those powers in Schedule 1.

Response

Home Affairs notes that proposed section 317ZF has been drafted to protect the commercially sensitive information of DCPs as well as the operations of law enforcement and security agencies. This provision reflects the outcome of consultations with industry who strongly recommended for the Government to restrict the disclosure of commercially sensitive information particularly in relation to the measures in Schedule 1. For example, a DCP would be reluctant to have the details of a TAN disclosed publicly as it may include technical information about a product or service. Given the law enforcement and national security material that will be regularly distributed under TARs, TANs and TCNs, it appropriate that robust protections apply to information which may pertain to investigations and agency capabilities more broadly.

Courts retain sentencing discretion to appropriately account for the circumstances of any unauthorised disclosure.

Following industry consultation, the unauthorised disclosure offence was extended to Government authorities that disclose DCP information received under a TAR, TAN or TCN.

This change underscores the commitment of Government to protect commercially sensitive information.

Home Affairs notes that the *Public Interest Disclosure Act 2013* has been established to govern the disclosures that would be in the public interest, subject to the limitations and conditions deemed appropriate by Parliament.

5. Purposes for which the powers may be exercised

The Bill limits the use of TARs, TANs and TCNs for the purpose of helping a relevant agency to perform its functions or exercise powers conferred by or under a law of the Commonwealth, a State or a Territory, so far as the function or power relates to a relevant objective.

Stakeholders have raised concerns that the definition of 'relevant objective' is disproportionately broad or otherwise unnecessary to serve the aims of the legislation. As a result, stakeholders are concerned that these powers will be used for purposes that are not within the policy intent of the Bill.

Access Now and Human Rights Watch expressed concerns that the relevant objectives allows for these powers to be used to investigate relatively minor offences. These submitters argued that the relevant objectives are broad enough to assist in the collection of fines or pursue minor tax evasion, and investigate incidents of public drunkenness. Future Wise suggested that the relevant objectives are wide enough to investigate "almost any regulatory offence."

The Law Council of Australia and Access Now criticised the inclusion of *safeguarding national security* as a relevant objective, claiming that it may inadvertently create violations of human rights. The Law Council of Australia further claimed that this purpose may be invoked without specifying any particular legislation as a source of power.

Access Now and Future Wise suggest that the powers in Schedule 1 should only be available for agencies to comply with foreign laws that comply with human rights standards. The Law Council of Australia submitted that the "fundamental human right to privacy" should be balanced with the purposes for which the powers in Schedule 1 may be authorised. As a result, notices should only be available to investigate cases involving "serious criminal offences."

The Law Council of Australia also recommended that any use of the powers in Schedule 1 to assist with *the enforcement of the criminal laws in a foreign country* have consideration for the "mandatory and discretionary grounds for refusing a mutual assistance request under section 8 of the *Mutual Assistance in Criminal Matters Act 1987 (Cth)*".

The Law Council of Australia also considered the relevant objective of *protecting the public revenue* had not been fully discussed in commentary surrounding the Bill and provides unfettered powers to access encrypted data conditional only on the suspicion that the data might provide evidence of taxation liability. Future Wise also considered that this purpose was beyond the stated "terrorism and national security" aims of the Bill.

Response

The definition of 'relevant objective' provides a reasonable and proportionate limitation on the use of a TANs and TCNs. The definition is also consistent with the established purposes for which a broader variety of agencies can currently seek assistance from the domestic

industry under section 313 of the *Telecommunications Act 1997.* They are also akin to the purposes for which for telecommunications data under Chapter 4 of the TIA Act can be made. These definitions are not arbitrary or unique and have been suitable to address the investigative needs of agencies to date.

The reference to 'pecuniary penalties' relates to penalties for breaches of Commonwealth, State and Territory laws that are not prosecuted criminally or that impose a penalty which serves as an administrative alternative to prosecution (often referred to as civil or administrative penalty provisions). As the Explanatory Memorandum makes clear, pecuniary penalties for the purposes of this provision are not intended to encompass small-scale administrative fines.[2] In Commonwealth, State and Territory legislation there are significant pecuniary penalties for serious breaches of the law, particularly laws regarding corporate misconduct.

Schedule 1 does not provide agencies with any additional powers which can be used to circumvent any human rights agreements. Instead, the powers furnish agencies with the ability to fulfil a warrant issued under existing frameworks. Broadly speaking, these existing frameworks are supported by safeguards and limitations to ensure human rights are not unnecessarily compromised. Agencies will also give consideration to human rights when deciding to issue notices under Schedule 1 to assist in enforcing the criminal laws in a foreign country. Where a TAN, TAR or TCN is issued in support of a mutual assistance request, agencies will consider the grounds of refusal under the *Mutual Assistance in Criminal Matters Act 1987.* For example, agencies are required to refuse providing assistance (unless there are 'special circumstances') where a person has been charged, arrested, detained or convicted of an offence that could result in the death penalty.

Importantly, the list of DCPs in items 1-15 of proposed section 317C are required to have a jurisdictional 'nexus' to Australia. The 'eligible activities' of each provider are connected to things and activities in Australia. The purpose of this connection is to limit the assistance requested to matters relevant to Australian authorities, or activities in their jurisdiction. There is also the additional requirement that notices be exercised consistent with the powers or functions of the relevant agency, listed in their enabling statues and limited appropriately.

As a result of feedback received through public consultations, the protection of the public revenue was removed as a purpose for which a TAR, TAN or TCN may be issued. While this objective remains an important part of law enforcement functions (as reflected by its inclusion in the other statutes mentioned above), Home Affairs considered that limiting the scope of purposes better reflected the core criminal law and security functions of the agencies listed.

6. Scope of providers captured

Stakeholders raised concerns that the definition of DCPs is too broad and places unnecessary obligations on a range of providers and related companies. Specifically, concerns were raised that the Bill may apply to companies and individuals that contribute to the communications supply chain such as manufacturers and relatively small scale providers that may not be able to meet the obligations in the Bill.

The Law Council of Australia considered that the Bill could impose assistance obligations on companies that operate a manufacturing facility or manufacture electronic components

[2] See Explanatory Memorandum, p. 44

without having responsibility for encrypted information. Similar concerns were raised by the Software Alliance and the Communications Alliance joint submission. As a result, the Law Council suggested that the definition of providers be limited to entities that control and have access to encrypted information.

Access Now raised concerns that the compliance obligations under the Bill could be prohibitively expensive, particularly for smaller entities. To this end, Access Now suggested that the definition of 'DCPs' be limited by a company's financial ability to comply with a notice and by the 'tangibility' and 'directness' of the company's connection with Australia. Internet Australia also suggested that the definition of 'DCPs' be narrowed by reference to the financial value of a company and the Software Alliance similarly suggested the Bill narrow its definition of provider by reference to a connection with Australia.

The Software Alliance, Internet Australia and the Communications Alliance joint submission raised concerns that the obligations in the Bill may apply to companies at any point in a supply chain of electronic equipment. Internet Australia suggested a provision be included to exempt those entities from being considered to DCPs if they "play no useful part in facilitating access to encrypted communications." Internet Australia further suggested that component manufacturers be removed from the list of providers.

Response

The definition of 'DCPs' is deliberately broad to reflect the range of entities that make up the modern communications environment. The provisions will apply to companies and individuals who contribute to the communications supply chain including carriers and carriage service providers, and developers of software and manufacturers of devices and components. The ability to secure assistance at different points in the communications supply chain is important to ensure law enforcement and national security agencies can target requests at those best placed to assist. Criminals will also often target small providers on the basis that their regulatory obligations will not be robust. As a result, it is no longer practical, efficient or fair to place obligations only on large domestic carriers. An extensive rationale for the scope of the definition is established in the above submission.

The powers in Schedule 1 are primarily designed to furnish law enforcement and national security agencies with the capacity to fulfil the requirements of a warrant issued under existing frameworks. The Bill will not allow agencies to serve interception warrants on overseas providers. This point has been further clarified with the inclusion of proposed subsection 317ZH(2) in the Bill following feedback received during consultations with industry. This provision ensures that TANs and TCNs cannot be used to require offshore providers to do things that would require a warrant or authorisation if they were a carrier or carriage service provider. For example, a TAN cannot compel the production of telecommunications data, as this would require an authorisation under the TIA Act if the DCP were a carrier.

A DCP that applies encryption is just one piece of the communications ecosystem that agencies need to work with to effectively discharge their established powers. Limiting assistance to providers that can control and access encryption would dramatically undermine the utility of the proposed new powers. Providers increasingly apply encryption schemes that they themselves are unable to break.

The Bill provides at proposed subsection 317ZK(3) that compliance with the requirements of a notice is to occur on the basis that DCPs neither profit nor bear the reasonable costs of complying with a notice. In appropriate circumstances, commercial terms may be available.

This ensures that DCPs of smaller financial means will not be adversely affected by complying with requirements under a notice. Requirements in proposed sections 317HAA, 317MAA and 317TAA ensure that authorities support smaller providers who may be subject to a request or notice.

The 'eligible activities' of providers are connected to Australia. Each item in proposed section 317C provides a 'nexus' to activities in Australia to ensure that the powers cannot be used to investigate matters wholly unrelated to investigations or matters at home.

7. Impact on privacy

During the consultation several social interest groups and stakeholders raised concerns that the Bill infringes upon both the privacy of specific users of encrypted communication and society more generally.

The United Nations Special Rapporteur on the Promotion and Protection of the right to the freedom of opinion and expression considered that privacy, as guaranteed by encryption, is a "gateway to the enjoyment of other rights" such as freedom of opinion and expression. Therefore, the Bill's potential to affect encryption infringes articles 17 and 19 of the ICCPR which guarantee rights to privacy and expression free from interference. The Rapporteur considered that restrictions on encryption imposed by the Bill do not respond to a legitimate interest, and disproportionately affect the rights of targeted persons and the broader population – the test for creating an exception to human rights. Concerns that the Bill's operation is contrary to the ICCPR were also shared by the Australian Lawyers for Human Rights and the law firm Nyman Gibson Miralis.

Human Rights Watch was similarly concerned that the decision-making criteria for consideration before issuing a notice are not sufficiently prescriptive to meet the standards of necessity and proportionality required to limit privacy. The Law Council of Australia, the Office of the Australian Information Commissioner and a joint submission from Digital Rights Watch suggested that the right to privacy form part of a decision-maker's considerations when evaluating if a notice is reasonable and proportionate. The Australian Human Rights Commission, the (Queensland) Office of the Information Commissioner and Future Wise suggested decision-makers be required to consider if the effect of the giving of a notice upon privacy is necessary and proportionate.

The Australian Human Rights Commission and the Office of the Australian Information Commissioner suggested the Bill require that the Minister consider privacy before making a legislative instrument to expand the definition of 'acts or things' available under a TCN.

General concerns that the Bill balance any curtailing of privacy rights against the needs of law enforcement were raised by the (Queensland) Office of the Information Commissioner, the Law Council of Australia and Optus. The Information Technology Professionals Association submitted that the Bill did not strike this balance appropriately. The Software Alliance described the choice between privacy and security as a "false" dichotomy.

The Communications Alliance recommended an independent privacy impact assessment be conducted of the Bill's application and the privacy protections available under the Privacy Act.

The Australian Human Rights Commission suggested that computer access warrants only be available to provide access where the issuing authority is convinced the warrant is necessary and after consideration of the likely effect on the right to privacy of any relevant

third parties. A joint submission from Digital Rights Watch recommended a requirement that computer access warrants sought by the Director-General of ASIO be granted by judicial authorisation in order to minimise the effect on privacy rights.

Response

The Bill's Explanatory Memorandum includes a statement of compatibility with human rights and engages with both Articles 17 and 19 of the ICCPR. Both of these rights can be permissibly limited to prevent appropriate interference from being deemed unlawful within the words of the ICCPR. For a limitation to be permissible it must pursue a legitimate objective and only impose a proportionate impact upon rights.

The legitimate objective pursued by the Bill is the protection of Australia's national security and public order by granting law enforcement, security and intelligence agencies the ability to respond to the use of encrypted communications and devices, and effectively access information which will assist investigations and prosecutions. National security is widely recognised as a legitimate objective of limiting human rights and it is broadly accepted that surveillance may be one measure which serves that objective.

When issuing a TAN or TCN, rights are protected by the requirement that the decision-maker be satisfied that the obligations imposed are reasonable and proportionate. In considering this, the decision-maker must evaluate the individual circumstances of each notice and the broader interests of the public. Within these broader interests, it is incumbent upon the decision-maker to consider the legitimate expectations of the Australian community as they relate to privacy and cybersecurity. Because of these criteria, any impact upon rights must be proportionate to the aim of the notice. This change was made following public feedback.

Decision-makers are required to consider the legitimate expectation of privacy within the broader Australian community when considering if a notice is reasonable and proportionate. The suggested criteria of 'necessity' is unnecessary because a consideration of that criteria naturally involves a decision-maker asking if a provider's obligations under a notice are proportionate to the notice's legitimate aim. This includes considering the availability of other means to achieve the objectives of the notice. Where proportional, a notice will naturally be of necessity.

Furthermore, the power to grant TANs and TCNs do not interfere with privacy because the notices cannot require a DCP to reveal content or data or grant access to underlying communications. Access to the content of an encrypted communication or device is conditional upon an underlying warrant being granted by a judicial body or other third-party.

The computer access warrants provided for under the Bill's Schedule 2 provisions require that the issuing authority, a judge or AAT member, consider the existence of alternative means of obtaining the evidence or information and the extent to which any person's privacy is likely to be affected. These considerations are targeted to discharge concerns that computer access warrants will be employed needlessly or impose a disproportionate violation upon privacy. The power of the Director-General of ASIO to seek a computer access warrant from the Attorney-General, Australia's highest law officer, predates the powers created by this Bill and it would be inappropriate for ASIO to seek judicial authorisation for the purposes of their investigations.