Australian Government

Department of Home Affairs

The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Submission to the Independent National Security Legislation Monitor

September 2019

Contents

Introduction

1. The Department of Home Affairs (the Department) welcomes the opportunity to make a submission to the Independent National Security Legislation Monitor's review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Assistance and Access Act).
2. The Assistance and Access Act has created a modern framework for Australia's law enforcement, anti-corruption and intelligence agencies to seek technical support when exercising their investigative powers in fulfilment of their statutory functions. Combining additional powers to enable covert computer exploitation, augment existing search warrants to allow data collection and ensure appropriate penalties are available to access digital evidence, this legislation represents a comprehensive approach to address the diminishing abilities of agencies to interrogate secure communications as part of their investigations and operations.
3. This submission is divided into two parts. Part one responds to themes the Independent National Security Legislation Monitor has identified as the guiding principles for this review.[1] These themes are:
    - That law should in principle apply equally to the physical world and the virtual world,
    - That what the law permits and prohibits must be clear, and
    - That oversight and safeguards are vital.
4. These themes are critical to understand the environment in which the Assistance and Access Act was developed. These themes have not been fully discussed in other forums to date. Offering further facts on these themes, may present an opportunity to reset the debate that has surrounded this legislation and address the true need for the frameworks it introduced.
5. Part two of this submission responds to the Independent National Security Legislation Monitor's terms of reference for each of the powers contained in the Assistance and Access Act. These terms of reference are whether the power:
    - Contains appropriate safeguards for protecting the rights of individuals,
    - Remains proportionate to any threat of terrorism or threat to national security, or both, and
    - Remains necessary.
6. The Department has made detailed statements to explain the policy choices that underpin this legislation – most recently to the Parliamentary Joint Committee on Intelligence and Security's current, third review of the Assistance and Access Act. Many responses in part two of this submission have been taken from the existing material and reordered to more directly respond to this review's priorities.
7. Where any particular questions remain unaddressed, we refer any questions back to the Home Affairs Portfolio submission to the Parliamentary Joint Committee on Intelligence and Security review of the Assistance and Access Act made on 1 July 2019.

[1] Dr James Renwick CSC SC, speech to the Lowy Institute, Sydney, 12 June 2019.

Part One: Thematic Discussion

1.1 Applying laws equally in cyberspace

8. The Assistance and Access Act received significant, critical attention from interested parties during the period of its introduction and passage which has continued throughout subsequent reviews in 2019. This coverage has focused almost singularly upon Schedule 1 which contains the legislation's most complex and least easily explained framework. The complexity of the industry assistance framework introduced by Schedule 1 has resulted in significant misunderstanding and misapprehension of the legislation and its purpose.

9. While all schedules are consistent in their intention, the Assistance and Access Act's aim is most clearly demonstrated by the more straightforward measures contained in Schedules 3, 4 and 5. Among other things, those schedules ensure that police, intelligence and border authorities may obtain technical assistance to access evidence stored in a digital format. This occurs by allowing investigators to obtain an order that provides a legal incentive to compel knowledgeable persons to offer technical assistance.

10. These powers are largely indifferent to the type of technical impediment to access – whether the evidence is locked by a password held by an administrator or buried in a database that requires an expert to interrogate. What matters is that, as in the case of evidence kept on a locked premises and retrievable under a search warrant, where an investigator has lawful authority to collect evidence this authority must not be frustrated by technological innovation. To put another way, evidence must not be treated differently because of the type of lock a suspect has used to secure it – whether physical or technology-based.

11. Schedule 1 has the same objective and performs the same function as the later schedules but does so with respect to a wider variety of established investigative powers. For example, where lawful authority has been provided by a *Telecommunications (Interception and Access) Act 1979* (Telecommunications (Interception and Access) Act) power such as a section 46A named persons warrant but the interception product is unintelligible, Schedule 1 offers investigators the ability to approach industry members and seek their assistance to decipher it.

12. For these reasons it is incorrect to suggest that Schedule 1 provides a new source of authority to conduct electronic surveillance. Schedule 1 supports the use of existing, approved investigation methods and powers. The powers Schedule 1 is designed to support, and that permit privacy interference during a law enforcement, anti-corruption or national security investigation, were not created by the Assistance and Access Act.

13. The debate around the Assistance and Access Act has been largely shaped by a narrative which claims that the law is intended to 'break encryption' which in turn, would undermine cybersecurity and the use of strong encryption for legitimate purposes (for example banking). As proof of this narrative, reports have often relied upon the statements and evidence provided by some industry representatives. In some cases these industry parties are unaccustomed to – and confronted by – the notion of government introducing frameworks to regulate or affect their activities in this way. This effect is magnified in light of the precedent Australia's legislation may set for other countries.

14. This incorrect narrative has detracted from a discussion of the most salient question that the Assistance and Access Act has sought to raise for public debate. Indeed, this reform provides a proportionate response to a wicked problem which has impeded the work of investigators for many years and is only worsening.

15. The critical question for debate may be roughly summarised as follows. **Should the powers granted by Parliament to the agencies charged with enforcing the criminal law and protecting Australia's national security be nullified by advances in technology?**

16. The Assistance and Access Act's policy settings follow from answering this question with a firm 'no'. This Act represents a commitment to applying the law equally to all people regardless of their technical prowess and nous. To do otherwise would be to accept the presence of criminality so long as it meets a minimum threshold of digital sophistication. This plainly would be an unacceptable outcome.

1.1.1 Genesis of the Assistance and Access Act

17. The reputation of the Assistance and Access Act for undermining encryption is both unfortunate and untrue. Were the Act aimed at 'breaking encryption' or creating backdoors, it would not be an acceptable response to cyber lawlessness. However, the legislation was not developed with the aim of impacting encryption and, as enacted, does not have this effect. To explain that breaking encryption is not the focus of the Assistance and Access Act, and to appreciate the problem this Act seeks to address, it is useful to examine the history leading to the development of this legislation.

1.1.1.1 The obligation to give reasonably necessary help

18. The concept that communications providers have a key role in ensuring their networks are not abused for criminal purposes is not new and has existed in Australian law for several decades – beginning with section 26 of the *Telecommunications Act 1989* (now repealed). The most well-established manifestation of this idea is embodied by subsection 313(1) of the *Telecommunications Act 1997* (Telecommunications Act) which provides that carriers and carriage service providers must do their best to prevent telecommunications networks and facilities from being used in the commission of offences.

19. Alongside the standing obligation in subsection 313(1) sits subsection 313(3) of the Telecommunications Act – first introduced as subsection 47(2) of the *Telecommunications Act 1991* (now repealed) – which places a duty on carriers and carriage service providers to give such help as is reasonably necessary to Commonwealth, State and Territory authorities. Help may be sought under this provision for five purposes, including to enforce the criminal law and safeguard national security.

20. The industry assistance framework in Schedule 1 of the Assistance and Access Act stems from both the concept and construction of subsection 313(3) of the Telecommunications Act. Similarities include a no-profit-no-loss basis of compliance for compulsory assistance, a positive rather than standing obligation[2] and several common purposes for which assistance may be obtained. However, Schedule 1 refines the obligation in section 313 by providing a shorter set of purposes for which assistance may be sought than those available under subsection 313(3), specifying the agencies that may seek assistance, listing the types of assistance that may be sought and specifying which delegates may use assistance powers.

21. Compliance with section 313 is required as part of the general requirement to comply with the Telecommunications Act and is governed by the compliance part of the Telecommunications Act.[3] In practice, compliance action has rarely been necessary in relation to this section. A representative of the Australian Mobile Telecommunications Association told a parliamentary committee:

[2] A positive obligation is less onerous than a standing obligation as it only compels action following the decision of an empowered agency rather than requiring ongoing action.

[3] Mr Ian Robinson, Deputy Secretary, Infrastructure Division, Department of Communications, *Standing Committee on Infrastructure and Communications Hansard*, 18 March 2015, p. 5; Part 31-31A *Telecommunications Act 1991*.

> The mobile telecommunications industry and the telecommunications industry generally have a well-established and long-running cooperative relationship with law enforcement agencies and national security agencies. That relationship and the provision of assistance when needed is guided by legislation and regulation as well as the day-to-day operations and protocols in place for provision of assistance when it is necessary and as required under the law. That provision of assistance is sometimes given in times of emergency or natural disasters but also more routinely, and that is guided by regulations, legislation and government policy and guidelines that have been in place for many years.[4]

22. This tradition has continued throughout agencies' early experiences using the Assistance and Access Act with all assistance to date being provided under the voluntary technical assistance request power.[5] This suggests that industry members continue to share a willingness to cooperate with law enforcement and national security agencies under the new industry assistance framework.

23. Other praise for section 313 has highlighted the provision's flexibility and utility to adapt the law to technological advances. A representative of the Communications Alliance, speaking in the context of the use of subsection 313(3) to block websites, testified in 2015 that:

> In that broader context of law enforcement engagement, we consider that section 313 is a useful provision. It specifically allows providers to engage with law enforcement agencies when the matter does not fall under any of the other provisions in the act or in the Telecommunications (Interception and Access) Act. It is also a quite useful provision when the law has not kept up, understandably, with technological development. (emphasis added) That could, for example, be a denial-of-service attack or something like that, where a large institution is affected by that to the detriment of the economy. It would not fall under many other places, but it could fall under section 313, and it allows providers to help as reasonably necessary…
>
> … a more robust framework would certainly be desirable… Amongst other things, we would want it to contain clear accountabilities, to adequately limit the circuit of agencies that issue those requests and to establish a clear level of authority of the officer…[6]

24. The industry assistance framework in Schedule 1 addresses these issues by granting powers to a narrower set of interception and intelligence agencies than section 313, and creates a clear framework for dispute resolution and compliance. This has been achieved while maintaining the robustness present in section 313 and adding additional safeguards for industry by, for example, making explicit that assistance can only be required where it is within the power of the designated communications provider to offer.[7]

25. Where assistance is sought under Schedule 1, agencies are encouraged to seek an outcome rather than a prescriptive technical procedure. This emulates the flexibility of subsection 313(3) – endorsed above as an important feature for keeping pace with technological development. The drafting of section 313 has been described by the Department of Communications and the Arts as intended to confer volition upon carriers and carriage service providers to decide how best to give help:

> Essentially, the way carriage service providers assist law enforcement agencies and other government agencies is open to them. The section is drafted in a way that they can provide the assistance that they

[4] Ms Lisa Brown, Policy Manager, Australian Mobile Telecommunications Association, *Standing Committee on Infrastructure and Communications Hansard*, 6 March 2015, p. 8.

[5] Australian Federal Police submission to the *Parliamentary Joint Committee on Intelligence and Security Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, January 2019, p 4.

[6] Mrs Christiane Gillespie-Jones, Director Program Management, Communications Alliance, *Standing Committee on Infrastructure and Communications Hansard*, 6 March 2015, p. 8.

[7] Subsection 317L(2A) Schedule 1 Assistance and Access Act.

> are capable of providing—their best endeavours. If they have that flexibility then that also allows them to say back to the requester, 'Instead of doing it like that, we could do it like this.'[8]

26. The Department's *Administrative Guidance for the Use of Part 15 of the Telecommunications Act* (Administrative Guidance) reflects this understanding of section 313 in interpreting Schedule 1:

> Law enforcement, national security and intelligence agencies should approach preliminary engagement without expectations of the precise technical solution required to offer the assistance they require. Instead, providers should be approached regarding the desired outcome and allowed to advise of the easiest and safest technical pathway to attaining it.[9]

27. The existence of subsection 313(3) in some form for decades, with the support of the Australian communications industry, demonstrates that the Assistance and Access Act is based upon a well-established and well-respected principle of Australian telecommunications regulation. Despite the existence of an obligation to offer assistance to authorities for many years, concerns that subsection 313(3) put digital infrastructure at risk have not materialised and actual damage has not occurred. It follows that a more prescriptive, narrowly defined form of subsection 313(3) neither carries this risk.

1.1.1.2 Addressing the growth of unintelligible communications

28. The other foundational concept of the Assistance and Access Act is the challenge it was designed to address. Technological impediments to lawfully accessing communications have been the subject of considerable discussion over many years and many potential solutions have been proposed. Considering this history and its proposed solutions helps to demonstrate that this challenge has not been created by a single technology and explains why the Assistance and Access Act presents a balanced extension of real world laws to cyberspace.

2000s: the Blunn Report

29. An awareness of the problem technological growth and the appearance of over-the-top providers on Australian telecommunication networks was creating for investigators can be dated back to at least the 2005 *Report of the Review of the Regulation of Access to Communications* (Blunn Report) which stated:

> The ever increasing range of data products carried over networks, often as a service to other providers, means that that data is often not readily interpreted by the carrier. From the point of view of the intercepting agencies receiving the raw data is of little use and defeats the intention of the scheme which pre-supposes product in useable form.

30. The Blunn Report then made the following recommendation:

> One solution would be to maintain the obligation on [carriers and carriage service providers] by requiring them in turn to impose on service providers for whom they carry data the obligation to interpret that data (or at least the means to decode it) and to provide useable product. I recommend this be done.[10]

31. This obligation was never imposed. If implemented, this proposal would require all service providers – including the over-the-top-providers captured by Schedule 1 of the Assistance and Access Act – to either retain plain text versions of their users' communications or otherwise hold capability to decrypt any of their users' communications.

32. While this may have been impossible to predict at the time of this report, technical solutions to comply with such an obligation may have produced an effective mandate to introduce an

---

[8] Ms Trudi Bean, Deputy General Counsel, Department of Communications, *Standing Committee on Infrastructure and Communications Hansard*, 18 March 2015, p. 3.

[9] Available on the Department's website: <https://www.homeaffairs.gov.au/nat-security/files/assistance-access-administrative-guidance.pdf> p 10.

[10] *Report of the Review of the Regulation of Access to Communications,* August 2005, p 47.

exceptional access solution such as a 'backdoor' or have resulted in providers attempting to block the use of asymmetric encryption on their network. These outcomes may have stifled innovation and created cybersecurity vulnerabilities in the products of communication providers operating in Australia.

33. The Assistance and Access Act is designed to prevent these outcomes from the earliest possible point in time. The voluntary technical assistance request power and consultation requirements associated with mandatory assistance powers mean that the assistance sought by agencies will be guided by industry members best-placed to understand and secure their technology. Explicit protections against the imposition of these requirements provide a further layer of protection against the creation of security flaws. As a matter of law, Schedule 1 does not allow vulnerabilities that persistently weaken technological security to be created or introduced in any way.

2010s: 'going dark' and earlier proposals

34. In 2011, the United States Federal Bureau of Investigation used the term 'going dark' to describe the widening gap between their legal authority and the limitations of their technical capabilities.[11] This language is now widespread and continues to be used by American counterparts such as Attorney-General William Barr who described the deployment of "warrant-proof" communications technology during a speech in July 2019 calling for technical solutions to enable lawful access to data while preserving robust cybersecurity.[12]

35. The terminology has been adopted in the Australian context. In 2012, the Parliamentary Joint Committee on Intelligence and Security heard evidence from Victoria Police arguing that the problem had multiple sources:

> In terms of this concept of going dark, it is certainly something that is being increasingly discussed amongst the law enforcement fraternity and it is a recognition primarily of these new technologies that we are unable to intercept for a range of reasons.[13]

36. The Commonwealth Attorney-General's Department submitted to the same inquiry that this collection of challenges across multiple technologies meant that industry obligations would need to apply to all participants in the communications market:

> The Department considers that industry obligations should apply to all such industry participants so as to ensure both existing and emerging products and services are covered, and are not outside law enforcement's powers. This will ensure that people cannot 'technology shop' to avoid detection.[14]

37. The possibility of 'technology shopping' applies equally to providers as to technologies themselves – outlawing or crippling encryption, were this possible, would not prevent other technologies being used to conceal, deliberately or inadvertently, the content of communications. The Commonwealth Attorney-General's Department provided as an example of this the following:

> In IP-based communications, the content of communications is embedded in data packets in a form which is not readily able to be reconstructed and interpreted outside of the transmitting and receiving terminal devices and the applications running on them. Data used to route, prioritise and facilitate the communications is also embedded along with the content, in the communications packets. This means

[11] Ms Valerie Caproni, General Counsel, Federal Bureau of Investigation, *Evidence to the House Judiciary Committee Subcommittee on Crime, Terrorism, and Homeland Security, United States Congress*, 17 February 2011, p. 7.

[12] Attorney-General William P. Barr, Department of Justice, *Keynote Address at the International Conference on Cyber Security*, 23 July 2019.

[13] Detective Inspector Gavan Seagrave, Victoria Police, *Parliamentary Joint Committee on Intelligence and Security Hansard*, 5 September 2012, p 29.

[14] Attorney-General's Department submission to the *Parliamentary Joint Committee on Intelligence and Security Inquiry into Potential Reforms of National Security Legislation*, August 2012, p 6.

that agencies must further process communications accessed under an interception warrant to extract and reconstruct the content.[15]

38. This obfuscation is not deliberate but a feature of how data is transmitted that nonetheless dramatically reduces the value of interception product. Prior to the Assistance and Access Act there was no legal avenue to require entities other than carriers and carriage service providers perform interpretation of these data packets.

39. In response to this evidence in 2013, the Parliamentary Joint Committee on Intelligence and Security canvassed a proposal to create an offence of failure to assist in the decryption of communications. While the Committee's discussion was only preliminary, there are significant drawbacks in such a proposal.[16]

40. A decryption offence would detrimentally limit its focus to one particular way in which technology may create a barrier to lawful access. The failure to be technologically neutral would likely have incentivised bad actors to exploit the narrow scope of the law to conceal their communications with other methods. Schedule 1 of the Assistance and Access Act overcomes this problem by specifying in its list of acts or things at paragraphs 317E(1)(d) and (da) that providers may be asked to give information in a particular format or undertake activities to facilitate giving effect to a warrant or authorisation. These paragraphs will enable agencies to seek assistance to obtain intelligible forms of the data to which they have lawful access, regardless of the technology involved.

41. A decryption offence proposal also suggests an assumption that providers always have the ability to decrypt communications on their platform. This would either encourage industry members to build standing decryption capabilities or bear the burden of rebutting a presumption in a criminal proceeding. This is undesirable and risks penalising providers for activities where they may have little control. The civil penalties provided for under Schedule 1 of the Assistance and Access Act are a more appropriate compliance tool in this environment, as this may only be enlivened when a provider has the ability to assist but refuses to do so.

42. In its 2014 submission to the Senate Legal and Constitutional Affairs References Committee's *Inquiry into the comprehensive revision of the Telecommunications (Interception and Access) Act 1979*, the Commonwealth Attorney-General's Department refined this decryption offence proposal. They proposed creating a regime of 'intelligibility notices' that could be issued to service providers or other persons upon application to an independent authority and served as a new, additional source of lawful authority to access data.[17]

43. The intelligibility notices proposal provides a suboptimal answer to this challenge for the following reasons. In contrast to a general decryption offence, these notices were proposed to operate in a similar manner to the aforementioned section 3LA orders available under the *Crimes Act 1914* (Crimes Act) – requiring the recipient of the notice provide the information in an intelligible format. Unlike the Assistance and Access Act this approach may have existed as part of the Telecommunications (Interception and Access) Act's regime of interception powers, likely creating the inaccurate perception that a new investigative power had been established.

44. Intelligibility notices, which would have provided independent authority to seek deciphering of data, would have been regulatory instruments for providers rather than orders attached to criminal penalties. However, the regulatory nature of these powers would have been at odds with their authorisation by independent authority and potential position alongside other privacy-intrusive powers in the Telecommunications (Interception and Access) Act. Schedule 1 of the Assistance and Access Act's presence in the Telecommunications Act reflects that the powers are not an imposition

[15] Ibid, p 22.

[16] Report of the Inquiry into Potential Reforms of Australia's National Security Legislation, *Parliamentary Joint Committee on Intelligence and Security*, May 2013, p 59.

[17] Attorney-General's Department submission to the *Senate Legal and Constitutional Affairs References Committee's Inquiry into the comprehensive revision of the Telecommunications (Interception and Access) Act 1979*, March 2014, p 19-20.

but a collaborative framework and therefore resolves the tension between the regulatory nature of the power and the criminal matters to which they are applied.

45. The authorisation of intelligibility notices by an independent authority would also create overlap with existing powers such as the section 46 telecommunications service warrants in the Telecommunications (Interception and Access) Act which already provide agencies authorisation to view the content of communications. As such, it is unclear what the independent authority would be authorising or if the authorisation would overlap completely with the existing powers. Schedule 1 of the Assistance and Access Act addresses this by enabling agencies to internally authorise powers to seek intelligibility assistance from industry, subject to thresholds and safeguards including that authority already exists to view any content.

46. Intelligibility notices further fail to account for the many other ways technology can interfere with lawful authority to access data. Schedule 1 of the Assistance and Access Act will, for example, allow agencies to upgrade the facilities of telecommunications service providers to ensure their infrastructure accurately captures communications on the network. This could include ensuring that a telecommunications service provider has the technology to record Visitor Location Register Data that reveals the location of devices on the network when they are not communicating – information that service providers are not required to retain if their facilities lack the capability to generate it in the first instance.

1.1.1.3 Conclusion

47. The Assistance and Access Act builds on existing precedents in telecommunications law. Rather than creating an onerous standing obligation or decryption assistance offence, which would be both detrimental and have diminishing effectiveness, the Assistance and Access Act builds a balanced, flexible and robust framework that enables agencies that have already obtained the lawful authority to access communications to work with industry to ensure those particular communications are intelligible.

48. The history of this debate also demonstrates that encryption is only one aspect of a larger series of interferences created by new technology and explains why the approach taken by Schedule 1 of the Assistance and Access Act was assessed to be the most appropriate in terms of how it is constructed and authorised. Furthermore, the legislation's application to providers across the communications supply chain is justified by the need to prevent alternative pathways for obfuscation being created and prevent bad actors shopping between technologies and technology providers.

1.1.2 Arguments against applying law equally in cyberspace

1.1.2.1 Integrity of cybersecurity and public perception

49. The standard at which the Assistance and Access Act prohibits assistance being sought is reached when an action is likely to create a systemic weakness.[18] By this metric, unless it can be demonstrated that a systemic risk is the likely outcome of the legislation, the appropriate balance between the interests of national security and cyber safety has been struck. Absent this evidence, there is no reason for laws governing the real world not to apply equally in cyberspace.

50. It has been argued that Schedule 1 of the Assistance and Access Act is a greater threat to the nation than the crimes and threats it seeks to combat.[19] Prior to passage, submissions to the Parliamentary Joint Committee on Intelligence and Security warned that the legislation could

[18] Subsections 317ZG(1) and (4A) Schedule 1 Assistance and Access Act.

[19] Damian Cronan, 'Dangerous overreach on encryption leaves 'backdoor' open for criminals', *Sydney Morning Herald*, 15 December 2018.

weaken the banking system[20], interfere with human rights[21] and posed a "significant risk of destabilising the Australian communications infrastructure"[22].

51. One academic wrote that "If passed, then, the Bill will jeopardize the personal safety of countless people in other countries (including some in Australia's sphere of influence)."[23] Another academic has since claimed that Schedule 1 means "you now have no privacy when it comes to your online information and any technology you use."[24]

52. However, after nine months of operation, these claims have not been substantiated.

53. This has led some to acknowledge that their concern has shifted to the way in which the law has been perceived, and the potential impacts of this perception even if it does not match the reality of the legislation. For example, Senetas noted in their submission to the Parliamentary Joint Committee on Intelligence and Security's Review of the Assistance and Access Act in February 2019:

> The accuracy of any of the above [media reporting] is entirely irrelevant. It is now a fact that citizens, businesses and governments across the world believe that, by passing this legislation, the Australian Government has fundamentally compromised their interests. As a consequence, trust in Australian companies operating in this market has been severely damaged.[25]

54. Seeking to remedy this perception by rolling back these powers would be misguided and needlessly hinder the work of law enforcement and national security agencies. The problem identified by the above is not one that can be addressed through legislative reform because it was not created by the operation of the law.

55. The disconnect between the perceived and actual effect of the law means that pointing to negative perceptions, even where those are widely held, is not an argument against the underlying policy and therefore cannot influence a reform discussion.

1.1.2.2 Interference with 'privacy'

56. In *A Declaration of the Independence of Cyberspace*, a founding member of the Electronic Frontiers Foundation, John Perry Barlow wrote:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.[26]

57. Barlow's declaration reflects a common cultural understanding prevalent throughout discussions of government regulation of the internet. As touched on by the examples in 1.1.2.1 above, this argument against applying the law equally in cyberspace stems from the expectation that online activities may be carried out in a state of privacy free from government oversight. However, often what is meant by 'privacy' when these appeals are made is in fact a belief in the right to total anonymity and protection from real-world consequences for actions taken online.

---

[20] Australian Information Industry Association submission to the *Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, October 2018, p 12.

[21] Access Now submission to the *Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, October 2018, p 8.

[22] Communications Alliance, Australian Industry Group, Australian Information Industry Group and Australian Mobile Telecommunications Association joint submission to the *Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, October 2018, p 17.

[23] Riana Pfefferkorn submission to the *Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, October 2018, p 9.

[24] Damien Manuel, 'Why we need to fix encryption laws the tech sector says threaten Australian jobs', *The Conversation*, 29 March 2019; See the discussion at 1.1.2.2.

[25] Senetas submission to the *Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, February 2019, p 4.

[26] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, Davos, Switzerland, February 8, 1996.

58. There is no absolute privacy in real life, and we do not expect there to be. We understand that law enforcement officials may legitimately obtain judicial authorisation to investigate within private spaces including by entering private property, examining personal luggage in security zones, and examining our financial transactions where necessary in order to prevent criminal behaviour that an absolute right to privacy could be used to conceal. Without the ability to enter private spaces for lawful purposes the work of law enforcement and national security agencies would become impossible.

59. While our cultural expectations of privacy online may depart from what we accept in real life, there is little justification for this distinction. The internet may be used to commit crimes that are as serious as many only possible in real life. The internet can also facilitate these crimes on a greater scale than had ever been previously possible and provide opportunities for new kinds of criminal behaviour to be perpetrated for the first time. The Department does not accept that the distinction that treats criminal behaviour differently because it occurs online should be reflected in our law.

60. It is essential that when interferences with privacy occur – online or offline – they occur consistently with the rule of law set down prospectively to ensure the application of the rules is not arbitrary or capricious, and that procedural fairness and natural justice are afforded to those under investigation. The Assistance and Access Act – in so far as it facilitates lawful interference with privacy that is authorised by other investigative powers – is one aspect of the rule of law that makes it permissible to abrogate individual privacy for legitimate purposes.

61. This position finds precedent in international human rights law which recognises the right to privacy may be limited for the legitimate purposes of enforcing the criminal law, assisting the enforcement of criminal laws in a foreign country, the interests of national security, foreign relations or economic wellbeing. The Assistance and Access Act's safeguards and thresholds ensure that the law may only impose limitations on the right to privacy where it does so for one of these legitimate purposes.[27]

[27] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Explanatory Memorandum, p 9; See the discussion at 2.1.1.

1.2: What the law permits must be clear

62. The desire for clear law is one shared by the Department. Though the Assistance and Access Act's Schedule 1 is necessarily complex, it nonetheless creates clear and prescriptive tests to determine where it applies and what assistance may be required. The Department has provided detailed, public guidance material to users of Schedule 1 within government and industry and continues to refine this advice.

63. Criticism of the Assistance and Access Act which describes it as unclear has usually focused on the prohibition against the introduction of systemic weaknesses.[28] While this framework has complexities – both legal and technical – fundamentally the protections and prohibitions in this framework are clear, as discussed below. Also below is a discussion of how the protection against side-stepping warrants or authorisations may be improved.

1.2.1 Systemic weakness[29]

64. At present, the global protection against the introduction or creation of systemic weaknesses prevents assistance being sought where it is likely that this will weaken a form of electronic protection used by any person other than the targeted individual. The interaction of a number of provisions and definitions achieve this effect.

65. Subsections 317ZG(1) and (5) mean that any attempt to use Schedule 1 powers to seek the implementation or building of a systemic weakness into a form of electronic protection or to prevent the patching of an existing systemic vulnerability has no effect. Subsections 317ZG(2) and (3) specify that this also nullifies the effect of any attempt to seek the building of a decryption capability or any weakening of authentication, encryption or electronic protection.

66. 'Electronic protection' is defined inclusively by section 317B as authentication and encryption while the Explanatory Memorandum further provides that it includes password rate limits on devices.[30] Defining 'electronic protection' inclusively (and not exhaustively) is intended to confer a broad, technologically neutral scope that would not be provided by listing types or categories.

67. The starting position created by subsections 317ZG(1) and (5) is augmented by the definition of systemic weakness in section 317B which provides that a weakness is a systemic weakness if it affects an entire class of technology. Because of this, as the Supplementary Explanatory Memorandum provides, a systemic weakness is something that makes general items of technology less secure rather than a single, particular item. It then offers examples of 'technological classes' including mobile device models, carriage services, electronic services or software.[31]

68. The definition of systemic weakness further provides that a systemic weakness does not include a weakness selectively introduced in a target technology connected with a person. The definition of 'target technology' is also provided by section 317B as meaning a particular carriage service, a particular electronic service, particular software, a particular software update, a particular item of customer equipment or a particular data processing device where these things are used, or likely to be used, by a particular person. This allows a weakness to be introduced into these things where it is confined to a particular instance of the thing and does not affect a whole class of the technology.

---

[28] Chris Culnane and Vanessa Teague, 'Well-Intentioned Bill Might Overshoot Its Target And Claim Us All', *The Australian*, 29 November 2018.

[29] The Assistance and Access Act prohibits 'systemic weaknesses' and 'systemic vulnerabilities' equally. References to 'systemic weakness' throughout this submission should be read also to capture 'systemic vulnerabilities'.

[30] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Explanatory Memorandum, p 67.

[31] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Supplementary Explanatory Memorandum, p 15.

69. The circumstances where it is permissible to introduce a weakness into one of these target technologies are further specified by subsections 317ZG(4A) and (4B). These provide that for selectively introduced weaknesses, such as those contemplated by the latter part of the definition of systemic weakness, the general prohibition of paragraph 317ZG(1)(a) includes anything that is likely to jeopardise the security of information held by any other person – other than the target person.

70. Subsection 317ZG(4C) further specifies that the security of information is placed in likely jeopardy if a material risk is created that otherwise secure information can be accessed by an unauthorised third party. 'Material risk' is undefined.

1.2.1.1 Development of the prohibition

71. 'Systemic weakness' was not defined in the public exposure draft of the legislation. The Department argued in its October 2018 submission to the Parliamentary Joint Committee on Intelligence and Security on the legislation that the flexibility afforded by this approach would allow users of the Schedule 1 framework to better guard against cyber risks:

> The term [systemic weakness] has also not been exhaustively defined as it is anticipated that it will apply differently between [provider]s. Given the significant divergence in the sophistication and complexity of systems, the activities that a provider may have to undertake to facilitate access to communications will not be uniform. One provider 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.[32]

72. Following Recommendation 9 of the Parliamentary Joint Committee on Intelligence and Security's December Advisory Report[33], the Department added a definition of the term 'systemic weakness' and provisions to reflect that such a weakness would be created if the information of persons other than the target would be put in jeopardy by the action taken. These provisions were drafted to preserve the legislation's policy intention and fundamental technological neutrality while crystallising the concept of 'systemic weakness'. The Department also took this opportunity to introduce the 'reserve capability' concept into legislation by defining 'systemic weakness' to exclude weaknesses limited to a single instance of a target device or service.

73. This is consistent with the concept of systemic weakness as included in the public exposure draft legislation. The Department's October 2018 submission to the Parliamentary Joint Committee on Intelligence in and Security provides that a systemic weakness is a weakness that "would undermine the security of other interconnected items."[34] The Explanatory Memorandum that accompanied the exposure draft provides that technical assistance notices and technical capability notices may require providers to "enable access to a particular service, particular device or particular item of software, which would not systemically weaken these products across the market".[35]

74. The concept that the integrity of interconnected items must not be undermined is now reflected in the 'class of technology' construction in the section 317B definition of 'systemic weakness'. The concept of a 'reserve capability' – that particular instances of a device or service may be affected without creating a systemic weakness – is now stated in the section 317B definition of 'systemic weakness' and also relies on the new definition of 'target technology' in section 317B. Therefore,

---

[32] Department of Home Affairs submission to the *Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, October 2018, p 20.

[33] Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, *Parliamentary Joint Committee on Intelligence and Security*, December 2018, p xi.

[34] Department of Home Affairs submission to the *Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, October 2018, p 20.

[35] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Explanatory Memorandum, p 67.

while these concepts are now embedded in legislation – exchanging some flexibility for clarity – the concepts themselves have remained consistent throughout.

1.2.1.2 Alternative proposals

75. Alternative proposals of the global protection have been raised for consideration, most notably in the form of an amendment moved in the Senate but not passed in February 2019.[36] The Home Affairs Portfolio's July 2019 submission to the Parliamentary Joint Committee on Intelligence and Security provides its analysis of this alternative formulation and pointed to several potential issues.[37]

76. The issues the Department identified with the proposal included that the removal of references to 'electronic protection' made it unclear what exactly systemic weaknesses were prohibited from affecting, that the introduction of a construction of 'communicating directly' applied awkwardly to internet forums and broadcasts with multiple recipients, and that sharing technical capabilities between agencies would be inadvertently restricted. The Department also considers that raising the probability of creating cyber risk from 'will or likely' to 'may or may in the future' placed an impossible expectation upon decision-makers to foresee future outcomes.

77. The potential areas of ambiguity identified with the alternative proposals suggests that these alternatives may not be clearer than the existing construction. It may be that no formulation is possible that satisfies all stakeholders.

78. It has also been proposed that the ability to weaken particular instances of technology be excised from the legislation.[38] It is appropriate for agencies to have the ability to selectively weaken the target technologies of those under investigation. Provided that no other person is impacted, there is no difference between introducing a security weakness into a person's service or device and compelling that person to hand over their login credentials. Both methods of access reduce the target's security, they only differ in regards to the layer in which the security vulnerability is introduced.

79. It is appropriate that the present arrangement be retained and further efforts be made to educate stakeholders of the protection's operation. The Department has been working continuously to inform and educate users of the industry assistance framework and stakeholders more broadly since the legislation was enacted.

1.2.1.3 A world's first protection

80. One reason for the controversy surrounding the clarity of the systemic weakness prohibition is the provision's novelty, compared to other provisions on the Australian statute books and internationally.

81. The Assistance and Access Act is comparable in some respects to powers that exist in the law of the United Kingdom and New Zealand. The United Kingdom's *Investigatory Powers Act 2016* (Investigatory Powers Act) and New Zealand's *Telecommunications (Interception Capability and Security) Act 2013* allow their respective countries to require telecommunications providers to make encrypted communications intelligible. However, the relevant parts of these laws that provide this power are considerably less prescriptive than what is provided by Schedule 1 of the Assistance and Access Act. Further, neither of these laws contain an explicit prohibition against weakening cybersecurity.

---

[36] Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019, sheet 8642.

[37] Home Affairs Portfolio submission to the *Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, July 2019, p 18-19.

[38] Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019, sheet 8642; Senetas submission to the *Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, February 2019, p iii.

United Kingdom

82. The United Kingdom legislation sets out that a technical capability notice may impose obligations on telecommunications operators that fall within the categories of "relating to apparatus owned or operated by a relevant operator" and "obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data".[39] Activities within these categories, to be set down in regulation, may theoretically include an obligation to produce data in an intelligible format or construct decryption capabilities.

83. Because this power may be deployed against any type of unintelligible information – including kinds that cannot be decoded without an exceptional access mechanism – this creates potential circumstances where reducing the security of a system will be necessary to comply with an obligation.

84. This obligation may be issued where it is considered by the Secretary of State and Judicial Commissioner to be necessary to ensure the operator has the capability to provide the required assistance and the conduct required is proportionate to what is sought to be achieved, among other considerations.[40] In the case of obligations to remove electronic protection, the Secretary of State and Judicial Commissioner must particularly consider if the obligation is technically feasible.[41] These decision-making criteria – which are replicated by Schedule 1 of the Assistance and Access Act – represent the only legislative safeguard within the Investigatory Powers Act against the introduction or creation of a systemic weakness.

New Zealand

85. The New Zealand legislation places a duty upon network operators and service providers to provide technical assistance and take all reasonable steps to give effect to a warrant or lawful authority. Assistance is specified to include assistance to "decrypt telecommunications where the person has provided the encryption".[42]

86. Exceptions to this requirement prevent agencies from requiring decryption assistance from a person who has indirectly supplied the encryption by providing an incidental product or requiring the provider ensure the agency has the ability to decrypt any telecommunication.[43]

87. These activities are authorised upon presentation of a warrant or other lawful authority by the intelligence and security agency to the network operator or service provider. This aspect of the power is mirrored by the effect of section 317ZH of Schedule 1 of the Assistance and Access Act.

88. Neither the exceptions nor the authorisation requirements prevent the theoretical imposition of a requirement upon a service provider to decrypt asymmetric encryption where they have directly provided the technology. This can effectively produce a circumstance where a provider must introduce a measure that reduces general user security in order to decode a particular communication.

1.2.1.4 Conclusion

89. The Assistance and Access Act introduced a unique and comprehensive protection against cyber risk that balances the imperatives of flexibility, technological neutrality, clarity and operability. The Department considers it has achieved this difficult balance in a way that places consequential brakes upon the types of assistance that may be requested using Schedule 1's powers that do not exist in comparable legislation overseas.

---

[39] Subsection 253(5) *Investigatory Powers Act 2016* (United Kingdom).
[40] Subsections 253(1) and 255(3) *Investigatory Powers Act 2016* (United Kingdom).
[41] Subsection 255(4) *Investigatory Powers Act 2016* (United Kingdom).
[42] Paragraph 24(3)(vi) *Telecommunications (Interception Capability and Security) Act 2013* (New Zealand).
[43] Subsection 24(4) *Telecommunications (Interception Capability and Security) Act 2013* (New Zealand).

90. The prohibition against systemic weaknesses is one specific aspect of the legislation that is only likely to be encountered where many more accessible assistance types have first been exhausted. Most assistance will not be directed at technological modification to navigate security features and will not engage with the protection.

1.2.2 Section 317ZH

91. As mentioned above, section 317ZH exists to prevent Schedule 1 powers being used to obtain data – both content and non-content – without first having in place the lawful authority that permits access to that data. Effectively, the provision creates a requirement that Schedule 1 powers only facilitate viewing of content data and non-content data with a relevant warrant, authorisation, or ministerial approval.

92. The existing section 317ZH is the product of redrafting to meet the request of stakeholders and Recommendation 17 of the Parliamentary Joint Committee on Intelligence and Security's December 2018 report. Unforeseen consequences associated with these changes have created a conflict between the original policy intention and the legal operation of this provision. Ambiguity now exists regarding the use of technical assistance requests in extraterritorial jurisdictions in circumstances where Commonwealth telecommunications warrants are ineffective. The Department is also concerned that the legal test called for approaches impossibility – asking a decision-maker to consider every law of the Commonwealth, a State or Territory.

93. As in the case of the prohibition against systemic weaknesses, the relative clarity of the current law can be measured by comparison with alternative proposals. However, in contrast to the above discussion, the Department considers that a model for a clearer version of section 317ZH is provided by section 172 of the Telecommunications (Interception and Access) Act which prohibits disclosure of content data in the course of executing a telecommunications data authorisation. In addition to imposing a simpler test, amending this provision in these terms to exclude the possibility of providing content and non-content data without the relevant underlying authority would also help to address concerns that the purpose of section 317ZH is not immediately clear.

1.3: Comparative models of oversight and safeguards

94. Schedule 1 of the Assistance and Access Act is most commonly compared with the United Kingdom's Investigatory Powers Act during discussions of the mechanisms that should exist to govern the authorisation and oversight of its powers. However, substantial differences exist between the two schemes which challenge the efficacy of direct comparisons.

95. The differences that make the United Kingdom's approach inappropriate for this scheme are:

- The different powers created by each scheme,
- The different conventions of each country's executive landscape, and
- The different bodies that exist to authorise the use of powers in each country.

96. The following discussion touches on these themes in the context of the authorisation requirements and technical assessment provided by Schedule 1 of the Assistance and Access Act particularly for the issue of technical capability notices.

1.3.1 The powers provided by the schemes are different

97. The key safeguard in the Assistance and Access Act's Schedule 1 powers is that they cannot authorise access to data – content or non-content. This is also the key difference with the United Kingdom's Investigatory Powers Act which provides both powers to obtain access to data and technical assistance ancillary to those powers. Because Schedule 1 powers do not in and of themselves provide a new, independent source of authority to conduct interception activities, the Department did not consider it necessary that they generally be issued by an issuing authority responsible for warrant-based powers.

98. This means that while it is true that most Schedule 1 powers are not authorised by an independent authority, the access to any underlying data targeted by those powers remains subject to ordinary approval processes which vary between agencies but include, most notably, approval by judicial authority. It is then only the technical assistance aspect of accessing data that is available for internal authorisation.

99. For these reasons the double-lock mechanism is unnecessary in this regime as it was created to authorise more consequential powers than mere technical assistance. Nonetheless, the Department continues to hold to its previously articulated view that the use of a technical capability notice, where it is intended to access the content of a communication, is governed by an effective 'triple-lock mechanism' involving the issue of the technical capability notice by the Attorney-General, approval by the Minister of Communications, and the issuing of the underlying warrant.[44]

100. Applying this higher level of authorisation to technical capability notices is appropriate given their ability to compel assistance to build new capability. This would be an irrelevant process for a voluntary power such as a technical assistance request which includes the critical safeguard that providers may freely decide they do not wish to comply if they consider they cannot do so responsibly in light of cybersecurity concerns. This would also be an unnecessary gate when using technical assistance notices which cannot create new cyber risk by virtue of being limited to compelling assistance that the provider is already capable of providing.

[44] Home Affairs Portfolio submission to the *Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, July 2019, p 37.

101. As has been noted, technical assistance possible under Schedule 1 is also narrower than is possible in the United Kingdom Investigatory Powers Act because of the global protection against the introduction or creation of systemic weaknesses. This further limits what can be obtained under Schedule 1's assistance powers; preventing them being exercised to undermine the integrity of several well-known security technologies such as end-to-end encryption. Australian technical capability notices also carry the additional limitation of item 317T(4)(c)(i) of the Assistance and Access Act, the operation of which prevents Schedule 1 being used to compulsorily build capability to remove electronic protection applied by the provider subject to the notice.

1.3.2 Technical review is provided for contentious cases

102. Because of the unique global protection and overall narrower scope of available technical assistance, it was assessed that the Assistance and Access Act's Schedule 1 powers do not carry the same theoretical risk of jeopardising cybersecurity that is present with the United Kingdom's Investigatory Powers Act. The Department does not wish to suggest that the operation of the Investigatory Powers Act has or will ever create a systemic weakness, only that this risk is managed differently in the United Kingdom legislation – through the role of a technical advisory board rather than a legislative protection. And, it is for this reason that the creation of a standing technical advisory board to adjudicate the technical consequences of assistance was not considered necessary.

103. However, technical review is provided for as part of the consultation process that precedes a technical capability notice being issued – specifically to consider technical capability notices that the provider considers carry the risk of creating a systemic weakness. The Attorney-General is required to appoint an independent technical expert to conduct this assessment when a provider who has received a consultation notice under subsection 317W(1) gives the Attorney-General a written notice making this request under paragraph 317WA(1).

104. As described in the Department's Administrative Guidance, the process of appointing this person should occur in consultation with the provider to ensure conflicts of interest and any other concerns of the provider are addressed.

> Best practice further dictates that, while the identities of the assessors may not be made public, the relevant parties to the proposed assistance instrument will have insight into the assessors' appointment and be given the opportunity to independently vet their backgrounds and relevant experience.[45]

105. This effectively builds industry into the discussion of what security modifications will create a material risk that otherwise secure information will be accessed by a third party.

106. In addition, the Department understands that technical capability notices are likely to be used sparingly as agencies prefer to build capabilities within the cooperative environment provided by the voluntary technical assistance request power. Agencies have been further incentivised to use technical assistance requests in such circumstances given the onerous approval process required to issue a technical capability notice. The low numbers of technical capability notices that are likely to arise from this intentional design and resulting culture would makes the creation of a standing review panel a disproportionate response to a rare situation.

107. Instead, the targeted technical review mechanism provided here offers a streamlined version of the expertise made available by the United Kingdom's technical advisory board and ensures that persons of expertise relevant to the particular system in question can be called upon as appropriate.

[45] Available on the Department's website: <https://www.homeaffairs.gov.au/nat-security/files/assistance-access-administrative-guidance.pdf> p 20.

1.3.3 Ministerial approvals are used for similar Australian powers

108. When comparing legislative powers between jurisdictions it is important to consider differences in the legal environments. It is the case, for example, that Australian law provides precedent for a Minister to authorise the use of powers or make decisions that are similar in complexity, process and magnitude to the issuance of a technical capability notice. Considering these comparisons helps to demonstrate that existing powers held by Australian executive authorities are consistent with those created by Schedule 1 of the Assistance and Access Act.

109. The *Security of Critical Infrastructure Act 2018* empowers the Minister for Home Affairs to direct the owner or operator of a critical infrastructure asset (which are those assets considered to be critical in the electricity, gas, ports and water sectors) to manage a risk that is prejudicial to security. The directions power is a power of last resort when good faith discussions and reasonable attempts to resolve the issue have broken down and is subject to a range of safeguards before the Minister can exercise the power. Most importantly, before considering use of the power, the Minister must be furnished with an adverse security assessment prepared under Part IV of the Australian Security Intelligence Organisation Act. Further safeguards include the Minister being satisfied that the direction is proportionate, consultation has occurred and the impact of the direction has been considered.

110. Another example of a similar executive power is section 315B of the Telecommunications Act which allows the Minister for Home Affairs to give a carrier or a carriage service provider a written direction requiring them to do, or refrain from doing, a specified act or thing within the period specified in the direction, also subject to a range of safeguards including an Australian Security Intelligence Organisation adverse security assessment.

111. The Attorney General's power to issue a technical capability notice is a comparable executive action that will generally only be exercised when voluntary approaches have been unsuccessful or when a provider has indicated they would prefer to offer assistance after being issued a legal obligation. This power is also subject to mandatory consultation with the provider, including – as set out above – review by an independent technical expert and a retired judge in addition to direct exchanges between the Attorney-General, the requesting agency and the provider. As with the above examples, technical capability notices may also be subject to judicial review. These similarities demonstrate that Parliament has been consistent in regards to the scope of powers generally granted to executive decision-makers.

112. Please note this comparison relates to the scope of the executive powers in question rather than the nature of the orders that may be issued or their content, which differ significantly. The powers available under the Security of Critical Infrastructure Act and 315B of the Telecommunications Act relate to the management of vulnerability rather than the provision of capability.

Part Two: Review Terms of Reference

2.1: Appropriate safeguards

2.1.1 Schedule 1: Industry Assistance Framework

2.1.1.1 Safeguards common to Schedule 1 powers

113. In addition to the discussion of the global protection against the introduction or creation of systemic weaknesses in 1.2.1, and the discussion of the prohibition against side-stepping authorisation requirements in 1.2.2, the use of the Assistance and Access Act's Schedule 1 powers are subject to the following safeguards.

Assistance must be reasonable and proportionate

114. The legislation contains lists of criteria to determine whether a request or notice is reasonable and proportionate.[46] These criteria apply to the decision to issue all Schedule 1 powers. The interpretation of these criteria will be assisted by reference to the Administrative Guidance which provides relevant considerations against each criterion.[47]

115. Neither the legislation nor the Administrative Guidance prescribe a particular weighting to these criteria, and consistent with the principles of good decision making, it is for the decision-maker to determine what weight they give to each criteria and consideration in the circumstances. In this context, it is open to providers to put forward their legitimate interests, which could include particular commercial interests, which must be taken into account (and appropriately weighted) by the decision maker.

116. Criteria for determining if a request or notice is reasonable and proportionate provide a thorough and flexible set of considerations for decision-makers to scrutinise. The Department will continue to develop and refine its advice to decision-makers regarding the interpretation of these criteria in response to consultation with industry stakeholders through subsequent versions of the Administrative Guidance.

Compliance must be practicable and technically feasible

117. Unlike the weighting exercise that occurs when considering if a request or notice is reasonable and proportionate, practicable and technically feasible compliance is concerned with real-world barriers to execution. It follows that a request or notice that is impracticable or not technically feasible will be impossible to execute. Though these terms are undefined in the Assistance and Access Act, the Administrative Guidance – which reflects input from industry stakeholders – offers a description of when a request or notice may be impracticable or not technically feasible.[48]

118. Practicability is described as concerning the human, financial and organisational resources required to perform an assistance activity and their availability to the provider. An additional test for practicability asks if the assistance sought resembles an activity that is within the provider's typical capacity to perform. If it is, then this may also suggest that compliance is practicable.

119. An activity is described as being technically feasible by the Administrative Guidance where it depends upon the operation of a capability that is within the provider's ability to utilise or, where

---

[46] Sections 317JC, 317RA and 317ZAA Schedule 1 Assistance and Access Act.

[47] Available on the Department's website: <https://www.homeaffairs.gov.au/nat-security/files/assistance-access-administrative-guidance.pdf> p 4-5.

[48] Ibid, p 5-6.

permitted, build. An assistance request or notice will not be technically feasible when it is unclear what technical procedure would need to occur to provide the assistance or if no technical procedure exists that could produce the outcome that is sought. Technical feasibility is also limited by what is permitted within the legislation's prohibition of systemic weaknesses and other limitations.[49]

120. Criticism of the decision-making criteria – particularly of "reasonable and proportionate" – has argued that they are subjective and present an inadequate safeguard against the bias of the decision-making towards law enforcement and security. However, the reasonableness and proportionality test is balanced by the practicability and technical feasibility criteria that, as described above, relate directly to questions of provider resources and attainable outcomes.

Relevant objectives / purposes

121. The use of Schedule 1 powers are, in most cases, specific to the functions of the agency they concern. For example, for the Director-General of the Australian Signals Directorate to issue a technical assistance request the request must relate to the Australian Signals Directorate's function of "providing material, advice and other assistance to a person or body mentioned in subsection 7(2) of the *Intelligence Services Act 2001* on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means"[50].

122. For interception agencies and the Australian Security Intelligence Organisation, the relevant objectives are broader to accommodate the range of activities that would benefit from the technical support enabled by Schedule 1 powers. However, these relevant objectives are not arbitrarily broad and do not include all of the functions of the captured agencies.

123. As discussed above in 1.1.1.1, the obligation on carriers and carriage service providers to give help under section 313 of the Telecommunications Act – the provision which industry assistance powers were designed to reflect – provides a broader range of purposes for which help can be provided than is possible in the Assistance and Access Act. Therefore, these narrow objectives and purposes provide a safeguard against assistance being sought in cases concerning less serious investigation types.

Serious offence threshold

124. The reference to 'serious Australian offences' and 'serious foreign offences' as part of the relevant objectives of 'enforcing the criminal law' for domestic and foreign offences, also creates an offence threshold that limits the offences that may be investigated by interception agencies. These terms are defined by section 317B as offences punishable by a maximum term of imprisonment of three years or more or for life. This was introduced in response to Recommendation 2 of the Parliamentary Joint Committee on Intelligence and Security's December 2018 report.[51] This offence threshold sufficiently limits the availability of industry assistance powers to the investigation and prosecution of serious crimes such as terrorism, child sex offences and other severe offences such as using a carriage service to menace, harass or cause offence.[52]

125. The current three-year threshold is appropriate and that raising it would place the Assistance and Access Act out of step with the warrants and authorisations it is designed to support. Surveillance device warrants and stored communications warrants both have offence thresholds of at least three years' imprisonment. These thresholds have been determined by Parliament to be sufficient to actually authorise intrusion on privacy and the collection of personal data – something which

[49] Ibid, p 6.

[50] Paragraph 317G(5)(c) Telecommunications Act.

[51] Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, *Parliamentary Joint Committee on Intelligence and Security*, December 2018, p ix.

[52] Section 474.17 of *Criminal Code Act 1995*.

Schedule 1 does not do. Raising the offence threshold for using Schedule 1 powers would prevent its use in parallel with these other investigative tools and frustrate the legislation's policy intention.

Consultation requirements

126. The Department has sought to bridge any gaps in the technical knowledge of decision-makers by proposing a robust regime of consultation and engagement between providers and investigators that may be extended or truncated as required to gather the necessary technical information and make an informed decision. Consultation thus provides a key safeguard against the acquisition of unsafe assistance.

127. Consultation is a legislative requirement before issuing a technical assistance notice or technical capability notice – though exactly what is required differs. These requirements have been calibrated to ensure that assistance relationships governed by compulsory Schedule 1 powers begin with appropriately detailed consultation and set the conditions for constructive future cooperation.

128. The requirements are also flexible enough to ensure that consultation can be minimised for repetitive assistance types under subsequent technical assistance notices – for example, assistance converting subsequent documents to a readable format. This approach will mean that providers have prior opportunity to discuss unique technical assistance notices but are not burdened with prescriptive consultation requirements in repeat instances.

129. In the case of technical assistance requests, it is appropriate that there is no legislated consultation requirement of any kind. The ultimate discretion of providers to decide to comply with a technical assistance request ensures that sufficient consultation will occur. If a provider considers they have not been properly consulted prior to the issue of a technical assistance request they may choose not to comply with the request. Alternatively, where a provider welcomes the issue of a technical assistance request with minimal or absent consultation, it is appropriate they be able to make this choice.

Statutory time limits

130. The exercise of Schedule 1 powers is further constrained by limitations on the period during which they may remain in effect. Technical assistance notices lapse after 90 days unless an expiry date is specified in the notice and may run for a maximum of 12 months unless renewed while technical capability notices lapse after 180 days unless an expiry date is specified in the notice and may run for a maximum of 12 months unless renewed.[53] Technical assistance requests lapse after 90 days if no expiry date is specified. Technical assistance requests do not have a maximum time limit though an end date must be specified in order for a request to last longer than 90 days.[54] The Department considers these limitations are appropriate and afford a safeguard against obligations and related immunities remaining in effect beyond the time that is necessary.

131. Regarding the absence of a maximum period specifiable for technical assistance requests; what makes this discretionary approach appropriate is the provider's ultimate ability to control whether or not to provide the requested assistance. Where a provider wishes to provide assistance for the period specified by the technical assistance request, it is appropriate they be allowed to do so. Subject to any commercial or contract consequences, providers are also able to decide unilaterally to cease providing assistance under a technical assistance request at a later time and, from this perspective, the end date specified by the technical assistance request is not enforceable upon the provider.

132. The other rights and obligations potentially modified by technical assistance requests belong to those individuals and entities whose ability to file a civil suit against a provider for an action is barred by the civil immunity associated with action taken under the technical assistance request. Here it is

[53] Sections 317TA and 317MA Schedule 1 Assistance and Access Act.

[54] Section 317HA Schedule 1 Assistance and Access Act.

important to note that technical assistance requests only provide an immunity to civil liability for providers for acts done in accordance with, or in good faith purportedly in accordance with, a request. This means that immunities created by technical assistance requests are only available while activities consistent with the request remain to be performed and, therefore, effectively cease to be available for further conduct after the activity requested has been completed regardless of whether the technical assistance request remains in effect.

133. Therefore, where a technical assistance request seeks very limited and specific assistance such as increasing a customer's data allowance, the range of activities that attract civil immunity are limited to a very specific action and for a very limited time. That is, after the data limit has been increased, civil immunities are not available for further activities even before the technical assistance request's expiry date.

134. Providers are commercial entities that operate in competitive business environments. In order for a technical assistance request to be appealing to these companies, agencies must be able to offer the certainty that their agency will support the technical assistance request for the lifetime of any underlying commercial agreement. Providers engaging under technical assistance requests are already demonstrating a great deal of trust towards agencies. Further asking providers to trust a technical assistance request will be reissued after a period of some years is an unreasonable burden to place on businesses already accepting a level of commercial risk that may be unacceptable in their ordinary dealings.[55]

2.1.1.2 Additional technical assistance notice safeguards

Coordination of technical assistance notices by Australian Federal Police Commissioner

135. Section 317LA requires the Australian Federal Police Commissioner to approve the giving of a technical assistance notice by the chief officer of a State or Territory interception agency. The Australian Federal Police Commissioner's role is to reduce duplication present in overlapping technical assistance notices, and to enable the exchange of relevant information across jurisdictions and provide advice on the types and forms of assistance commonly requested. The Australian Federal Police Commissioner is not required to reassess the decision-making behind the issuing of these technical assistance notices.

2.1.1.3 Additional technical capability notice safeguards

136. The primary additional safeguards applied to technical capability notices are described above in 1.3.1 and 1.3.2.

Express prohibitions against certain activities

137. To provide clarity regarding the interaction between technical capability notices and topics of particular public anxiety, section 317ZGA sets out certain specific activities that cannot be performed using a technical capability notice. This section provides that a technical capability notice has no effect to the extent that it would:

- Create new interception capabilities,
- Build or extend data retention requirements to new providers, and
- Create capability to store the browsing history of internet users.

[55] Home Affairs Portfolio submission to the *Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, July 2019, p 35.

2.1.2 Schedule 2: Computer Access Warrants

138. Amendments made by Schedule 2 of the Assistance and Access Act make changes to the Australian Security Intelligence Organisation's computer access warrant power to allow for interception to occur where it is for the purposes of doing things specified in the computer access warrant and associated amendments, including the ability to conceal activities undertaken under a computer access warrant.

139. Schedule 2 also introduced computer access warrants into the *Surveillance Devices Act 2004* (Surveillance Devices Act) to allow their use by Commonwealth and State and Territory law enforcement agencies. The safeguards for this power are provided by the authorisation process before an eligible judge or Administrative Appeals Tribunal member.

2.1.2.1 Australian Security Intelligence Organisation Act Computer Access Warrants

140. Consistent with the existing provisions in the *Australian Security Intelligence Organisation Act 1979* (Australian Security Intelligence Organisation Act), Australian Security Intelligence Organisation computer access warrants are subject to strict legislative requirements and thresholds and must be signed by the Attorney-General. The Attorney-General may only issue a warrant if they are satisfied that there are reasonable grounds for believing that access to data held in a computer will substantially assist the collection of intelligence in respect of a matter that is important in relation to security.

2.1.2.2 Surveillance Devices Act Computer Access Warrants

141. 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.

142. Computer access warrants are issued by judges or Administrative Appeals Tribunal members. In deciding whether to issue a warrant, he or she must be satisfied of the grounds of the application. Under subsection 27C(2) a judge or Administrative Appeals Tribunal member must also have regard to, among other things:

- 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.

143. 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 relevant 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.

144. 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.

145. 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.

146. 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.

147. 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 Telecommunications (Interception and Access) Act.

2.1.3 Schedule 3: Law Enforcement Search Powers

148. Amendments made by Schedule 3 of the Assistance and Access Act primarily made adjustments to pre-existing powers in the Crimes Act and therefore rely upon the safeguards that already existed in respect to those powers. This is primarily the judicial approval requirement attached to section 3E search warrants and section 3LA assistance orders.

2.1.3.1 Modernised Crimes Act Search Warrants

149. Section 3E search 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 by, for example, overwriting existing metadata attached to relevant files, and
- Material loss or damage to other persons lawfully using a computer is prohibited.

2.1.3.2 Increased Crimes Act Assistance Order Penalties

150. A number of 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. These conditions include that the magistrate is satisfied that:

- There are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device,
- The specified person is connected to the device (for example, as the device owner or user), and
- The specified person has relevant knowledge to enable them to access the device.

151. The Assistance and Access Act did not amend these safeguards.

2.1.4 Schedule 4: Australian Border Force Powers

152. Amendments made by Schedule 4 of the Assistance and Access Act to the Customs Act provide extended timeframes for executing search warrants and allow officials to move computers for the purpose of their investigations; bringing the powers of the Australian Border Force into line with other law enforcement agencies. These changes are safeguarded by the pre-established judicial authorisation process. Amendments to the Customs Act also provided increased penalties for assistance orders. These changes are also safeguarded by the pre-established judicial authorisation process.

2.1.4.1 Modernised Customs Act Search Warrants

153. The amendments to the Customs Act are supported by robust safeguards to ensure a warrant is only issued to meet Australian Border Force 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 Australian Border Force'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, and
- 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.

2.1.4.2 Increased Customs Act Assistance Order Penalties

154. A number of conditions in subsection 201A(2) must be met before a magistrate grants an order to allow officials to compel a person to give assistance accessing data. These conditions include that the magistrate is satisfied that:

- There are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device
- The specified person is connected to the device (for example, as the device owner or user), and
- The specified person has relevant knowledge to enable them to access the device.

155. Australian Border Force applications for the use of this power consist of an affidavit setting out the reasons that the person's assistance is required.

156. The Assistance and Access Act did not amend these safeguards.

2.1.5 Schedule 5: Australian Security Intelligence Organisation Assistance Powers

157. Amendments made by Schedule 5 of the Assistance and Access Act introduced new powers to allow the Director-General of Security to issue voluntary assistance requests to persons or bodies that confer civil immunity for related activities and to allow the Attorney-General to issue assistance orders to require persons to provide assistance.

158. 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:

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

2.1.5.1 Australian Security Intelligence Organisation Act Voluntary Assistance Requests

159. The Director-General is responsible for issuing requests for assistance under section 21A of the Australian Security Intelligence Organisation Act. The Director-General has to be satisfied on reasonable grounds that the conduct is likely to assist ASIO in the performance of its functions.

160. In addition, subsection 21A(8) allows the Director-General to give an evidentiary certificate certifying the factual basis necessitating the assistance provided. This certificate will detail how the relevant conduct was likely to assist the Australian Security Intelligence Organisation in the performance of its functions.

161. The Director-General also has discretion to provide civil immunities for any assistance given under section 21A. Subsection 21A(1) sets out the thresholds for when civil liability immunity applies to persons or bodies:

- Has the Director-General requested the person or body to engage in certain conduct;

- Is the Director-General satisfied that, on reasonable grounds, the conduct is likely to assist the Australian Security Intelligence Organisation in the performance of its functions;
- Does the conduct involve a person or body committing an offence against a law of the Commonwealth, a State or a Territory; and
- The conduct would not result in significant loss of, or serious damage, to property.

162. These thresholds ensure that civil immunities are appropriate.

2.1.5.2 Australian Security Intelligence Organisation Act Assistance Orders

163. A section 34AAA order allows the Director-General to request the Attorney-General to make an order requiring a person to provide information or assistance to the Australian Security Intelligence Organisation that is reasonable and necessary to allow the Australian Security Intelligence Organisation to access, copy or convert data held in computers or data storage devices. As such, this means a section 34AAA order can only apply to a computer or data storage device already accessible to the Australian Security Intelligence Organisation pursuant to a warrant or authorisation.

164. 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.

2.2: Proportionality

2.2.1 Schedule 1: Industry Assistance Framework

165. Considerations of proportionality are required to exercise Schedule 1 powers as described in 2.1.1.1. The requirement to consider proportionality as part of the issuing criteria means that these powers cannot be exercised where proportionality is not considered.

2.2.2 Schedule 2: Computer Access Warrants

2.2.2.1 Australian Security Intelligence Organisation Act Computer Access Warrants

166. The exercise of intelligence-gathering powers by the Australian Security Intelligence Organisation must be proportionate as required by the Australian Security Intelligence Organisation's Attorney-General's Guidelines. Please see the discussion below in 2.2.5.

2.2.2.2 Surveillance Devices Act Computer Access Warrants

167. The threshold for obtaining a computer access warrants is proportionate as it is in line with the tests for an application for a surveillance device warrant in the Surveillance Devices Act.

2.2.3 Schedules 3 & 4: Crimes Act and Customs Act Search Powers

2.2.3.1 Modernised Crimes Act and Customs Act Search Warrants

168. The enhancements made to search warrants in both the Crimes Act and Customs Act directly reflect the realities of interrogating digital devices by allowing investigators longer periods to conduct forensic examinations, move computers offsite to use specialised hardware, and, if necessary to execute the warrant, add, copy, delete and alter data on the device. As these changes have been made to reflect modern technological realities, they are naturally proportionate.

169. Please see the related discussion of necessity below in 2.3.3 and 2.3.4.

2.2.3.2 Increased Crimes Act and Customs Act Assistance Order Penalties

170. Pre-existing provisions in the Crimes Act and Customs Act enabled law enforcement to compel certain persons (including owners and users of a device) to assist in providing access to data held in a device. Schedules 3 and 4 amended the law to ensure the penalties for non-compliance with an assistance order reflect the potential ramifications for the security of the community.

171. Under the previous regime, offenders frequently refused to comply with an assistance order in instances where the evidence on their device may lead to a more severe penalty than non-compliance with the order. For example, in 2016 an individual was prosecuted on 13 charges relating to the control of multiple child sexual abuse websites he used to distribute and facilitate the production of child pornography material. He received total effective sentence of 15 years and six months' imprisonment with a non-parole period of 10 years. For the offence under section 3LA of the Crimes Act, he was sentenced to six months' imprisonment, which must be considered in the context of the overall sentence.

172. Schedules 3 and 4 introduced a tiered approach to enforcement which ensures that the penalties are reflective of the gravity of non-compliance with an assistance order. The penalty for non-compliance in relation to a simple offence has been increased from two years imprisonment or 120 penalty units, to five years imprisonment or 300 penalty units, or both (see subsection 3LA(5) Crimes Act). Penalties in relation to simple offences in the Customs Act increased from six months imprisonment or 120 penalty units to five years imprisonment or 300 penalty units, or both (subsection 201A(3)).

173. The Assistance and Access Act also introduced a penalty for serious/aggravated offences of 10 years imprisonment or 600 penalty units, or both (see subsection 3LA(5) Crimes Act and subsection 201A(4) Customs Act). It is important to note that the aggravated penalty is only available where the underlying investigation relates to a serious offence (defined as an offence attracting two years' or more imprisonment) or serious terrorism offences.

174. This enforcement structure is proportionate and ensures that the penalties for non-compliance are reflective of the potential harm it may cause to innocent Australians.

175. The law also includes explicit protections for those persons that are required to provide assistance but are incapable of doing so. A person would be incapable of complying with an assistance order if, for example, the person is no longer able to provide the evidential material by virtue of not having access to the relevant device.

2.2.4 Schedule 5: Australian Security Intelligence Organisation Assistance Powers

176. The Attorney-General's Guidelines specify that any information obtained by the Australian Security Intelligence Organisation is to be obtained in accordance with several principles. These include that "any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence".[56] As information-gathering powers, both new powers provided by Schedule 5 of the Assistance and Access Act are subject to this direction.

177. Furthermore, the Department understands it is standard internal practice for issuing decisions by the Australian Security Intelligence Organisation to consider proportionality.

2.2.4.1 Australian Security Intelligence Organisation Act Voluntary Assistance Requests

178. The ability to provide civil immunities to persons and bodies that provide the Australian Security Intelligence Organisation assistance voluntarily is proportionate because the immunity is not available to activities which involve committing offences against the laws of the Commonwealth, a state or a territory, or conduct that results in significant loss or damage to property.

2.2.4.2 Australian Security Intelligence Organisation Act Assistance Orders

179. Assistance orders are directed towards the legitimate objective of ensuring that the Australian Security Intelligence Organisation can give effect to warrants which authorise access to a device. The Australian Security Intelligence Organisation'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.

[56] Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence), 10.4(a).

2.3: Necessity

2.3.1 Schedule 1: Industry Assistance Framework

180. The necessity of Schedule 1's powers is a major theme of this submission and is explored in 1.1.1.2 above. For operational examples of why these powers are necessary to agencies throughout the Home Affairs Portfolio and beyond, the Department refers to those agencies' submissions to this review.

2.3.2 Schedule 2: Computer Access Warrants

181. Schedule 2 of the Assistance and Access Act modernised the existing computer access warrant power in the Australian Security Intelligence Organisation Act to address operational challenges and replicated these updates while introducing the power into the Surveillance Devices Act. Computer access warrants are an important covert investigatory tool which allows law enforcement and the Australian Security Intelligence Organisation officers to search electronic devices and content on those devices. The Assistance and Access Act's amendments ensure these warrants continue to be operationally effective while respecting the need to appropriately limit access to intrusive powers.

Incidental interception

182. It is often necessary to undertake limited interception for the purposes of executing a computer access warrant. Schedule 2 amended the law to permit the interception of a communication passing over a telecommunication system, if the interception is for the purposes of doing anything specified in the computer access warrant. In other words, any interception of communications would be incidental to executing a computer access warrant, including the concealment of access, and cannot be used for independent evidence or intelligence collection.

183. This is consistent with the general exceptions to the prohibition against interception in section 7 of the Telecommunications (Interception and Access) Act. Paragraph 7(2)(ac) of that Act exempts a number of legitimate activities that require the incidental interception of communications, including "the interception of a communication where the interception results from, or is incidental to, action taken by an Australian Security Intelligence Organisation employee, in the lawful performance of his or her duties".

184. This framing means that the existing thresholds for interception are not lowered by Schedule 2. Though the same information is collected regardless of warrant-type, officers will require an interception warrant to deal with intercepted communications beyond what is required to give effect to a computer access warrant. The existing threshold for interception warrants is generally offences with a maximum seven years' imprisonment or more.

Concealment

185. Surveillance activities authorised by a computer access warrant may require the addition, copying, alteration or deletion of data.

186. The concealment of the execution of a computer access warrant is vital to the exercise of the powers under Schedule 2, and indeed, the pre-existing powers in the Australian Security Intelligence Organisation Act. Concealment of access is essential for preserving the covert nature of computer access warrants, and to protect law enforcement and intelligence technologies and methodologies.

Entry onto premises

187. Schedule 2 amendments allow officers to enter a premises for the purpose of concealing the fact that anything has been done under a computer access warrant. The law also provides scope for law enforcement and the Australian Security Intelligence Organisation to intercept communications for the purposes of gaining access to a premises. Any interception must be strictly related to the concealment of the execution of the warrant – in this case entering a premises. Officers may also rely on this power to retrieve a physically implanted computer access device from a computer which was required to give effect to the warrant. This acknowledges the importance of ensuring that agencies have the ability to determine when access to premises or to a device will best ensure the operation remains covert.

188. Similarly, Schedule 2 introduced provisions into the law to allow law enforcement agencies and the Australian Security Intelligence Organisation to use interception powers to facilitate entry to a premises, including third-party premises, to remove a computer or device for the purpose of concealing access. The ability to temporarily remove a computer from the premises is important in a number of operational situations, including those in which an agency may have to use specialist equipment to access the computer but cannot for practical reasons bring that equipment onto the premises in a covert manner.

189. In both these circumstances, the interception of communications is only permitted so far as it is required – either to enter a premises for concealment purposes or to temporarily remove a device to give effect to the warrant. Any limitations on this capability may disproportionately impact law enforcement agencies and the Australian Security Intelligence Organisation.

190. Officers cannot always reliably predict whether, or when, they will be able to safely enter a premises to retrieve devices or conceal access without compromising a covert operation. For example, a person may unexpectedly relocate their computer or device before it can be removed by law enforcement for concealment purposes. This may ultimately undermine an ongoing investigation. The ability for law enforcement and the Australian Security Intelligence Organisation to intercept communications pursuant to the purposes discussed above will allow officers to better predict when it is safe and appropriate to enter a premises.

Use of force

191. The use of force may be required as part of executing a computer access warrant due to the likely obstacles faced by officers while executing a warrant. For example, it may be necessary to use force against a door or a cabinet lock to access a thing on the premises or to use force to install or remove a computer. In the case of force against a person, its use is constrained by the legislation to circumstances where force is required to execute the computer access warrant. For instance, it may be necessary to use reasonable force if a person is obstructing a doorway into the warrant premises and an officer needs to move past them.

192. The absence of a power to use reasonable and necessary force could potentially lead to civil action or criminal charges should a law enforcement officer do acts or things against a person proportionate to what is contemplated by warrant. Reasonableness and necessity requires the use of force to be proportionate in all circumstances.

193. However, it is a long standing practice that entry onto premises may be necessary where it would be impractical or inappropriate to intercept communications in respect of a device otherwise than by using equipment installed on specified premises. This may be due to technical reasons connected with the operation of the service or the telecommunications system of which the service is part, or because the execution of the computer access warrant, as a result of action taken by an officer of a carrier, might jeopardise the security of the investigation. Accordingly, it is reasonable and necessary to ensure that law enforcement officers undertaking these activities can do so with appropriate authorisations around the use of force.

2.3.3 Schedule 3: Law Enforcement Search Powers

2.3.3.1 Modernised Crimes Act Search Warrants

194. Schedule 3 amends the 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.

Searching and seizing computers

195. Previously, the Crimes Act allowed law enforcement to obtain an overt search warrant (which must be issued to the relevant person) to seize and search computers. Schedule 3 modernised this power by allowing law enforcement agencies to remotely and overtly collect evidence using specialist equipment. This amendment reflects forensic best practices as it reduces the risk of altering, damaging or destroying evidence by using a suspect's computer, which was required under the previous search warrant provisions.

Account-based data

196. Schedule 3 also updated search warrants in the Crimes Act to reflect modern forms of communications. A new definition of 'account-based data' was inserted to ensure that accessing a computer under a search warrant also enables law enforcement officers to access information associated with an online account such as an email or social media account.

Extending timeframes for forensic examination

197. The previous provisions in the Crimes Act did 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 increased 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

Add, copy, delete or alter

198. Amendments made by Schedule 3 also enhance section 3E search warrants as necessary to make them compatible with the ordinary manner by which data is copied from a computer. Paragraph 3F(2A)(a) provides that officers may add, copy delete or alter data on a device uncovered during the execution of a search warrant if necessary to execute the warrant.

199. This amendment does not authorise officers executing a search warrant to destroy or modify the contents of documents on electronic devices. The power to 'add, copy, delete or alter other data' is used solely to obtain access to data held on a computer system.

2.3.3.2 Increased Assistance Order Penalties in the Crimes Act

200. The case for the necessity of the increased penalties for Crimes Act assistance orders aligns closely with the reasons why this increase is proportionate to the challenge. The Department refers to 2.2.3.2.

201. See also the Australian Federal Police's submission.

2.3.4 Schedule 4: Australian Border Force Powers

2.3.4.1 Customs Act Assistance Orders Increased Penalties

202. The case for the necessity of the increased penalties for Customs Act assistance orders aligns closely with the reasons why this increase is proportionate to the challenge. The Department refers to 2.2.3.2.

2.3.4.2 Customs Act Computer Access

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

203. Schedule 4 enabled judicial officers to issue warrants authorising the Australian Border Force 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.

204. Under previous laws, the Australian Border Force could only obtain a judicial authorisation for a search warrant relating to a search of premises. The amendments were made in recognition 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

205. Schedule 4 enabled the Australian Border Force 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 have enabled the Australian Border Force 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.

206. Previously, 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 they believes on reasonable grounds that the data constitutes evidential material. To use this power, an officer must be physically located at the warrant premises.

207. Subsections 199(4A) and 199B(2) now allow the Australian Border Force 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 power to move a computer or data storage device

208. Schedule 4 enabled 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 previous provisions for premises-based search warrants in the Customs Act, which allowed an executing officer to move evidential material or suspected evidential material found on a premises.

209. This power allows the Australian Border Force 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 created as a result is necessary and in the interests of law enforcement and national security.

210. Schedule 4 also amended timeframes for how long a device may be moved for analysis. Under the previous section 200 of the Customs Act, a thing moved from premises was required to be returned within 72 hours. Schedule 4 extended the time period for moved computers and data storage devices to 30 days and allows additional time extensions of 14 days. These timeframes allow the Australian Border Force adequate time to conduct the lengthy and intricate forensic processes necessary for investigation of electronic devices. The amendments ensure the Australian Border Force can fulfil its statutory functions with forensic best practice.

2.3.5 Schedule 5: Australian Security Intelligence Organisation Assistance Powers

2.3.5.1 Australian Security Intelligence Organisation Act Voluntary Assistance Requests

211. Section 21A established 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 the Australian Security Intelligence Organisation

212. Subsection 21A(1) provides that if the Director-General requests a person or body to engage in conduct that the Director-General is satisfied, on reasonable grounds, is likely to assist the Australian Security Intelligence Organisation 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.

213. The person or body is not subject to any civil liability for, or in relation to, that conduct.

214. This power is necessary to indemnify those persons or bodies who provide necessary technical assistance to the Australian Security Intelligence Organisation voluntarily and therefore addresses the need to incentivise knowledgeable persons and bodies to provide this important assistance.

Unsolicited assistance provided to the Australian Security Intelligence Organisation

215. Schedule 5 also provides protection from civil liability for persons or bodies making unsolicited disclosures of information to the Australian Security Intelligence Organisation. 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 the Australian Security Intelligence Organisation, or giving or producing a document to the Australian Security Intelligence Organisation, or making one or more copies of a document and giving those copies to the Australian Security Intelligence Organisation, and:

- The person reasonably believes that the conduct is likely to assist the Australian Security Intelligence Organisation 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.

216. 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 the Australian Security Intelligence Organisation, or the Australian Security Intelligence Organisation's functions.

2.3.5.2 Australian Security Intelligence Organisation Act Assistance Orders

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

218. Schedule 5 addressed this issue by allowing the Director-General to request the Attorney-General make an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the Australian Security Intelligence Organisation to do one or more of the following:

- 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.
- Copy data held in, or accessible from, a computer, or data storage device, described in paragraph (a) to another data storage device.
- Convert into documentary form or another form intelligible to an ASIO employee or ASIO affiliate:
  - Data held in, or accessible from, a computer, or data storage device, described in paragraph 34AAA(1)(a),
  - Data held in a data storage device to which the data was copied as described in paragraph 34AAA(1)(b),
  - Data held in a computer or data storage device removed from premises under a warrant under section 25, 26 or 27A, or
  - Data held in a computer or data storage device removed from premises under section 27D. [57]

[57] Paragraph 34AAA(1)(a) Schedule 5 Assistance and Access Act.

219. The types of assistance that the Australian Security Intelligence Organisation 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 Australian Security Intelligence Organisation officers to interrogate the relevant electronic database or use the relevant software so that they can obtain a copy of particular records or files.

220. This power enables the Australian Security Intelligence Organisation to compel those capable to provide the Australian Security Intelligence Organisation 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.