

Submission to the Parliamentary Committee on Intelligence and Security Review

Review of The Assistance and Access Bill 2018



Introduction

Thank you for the opportunity to make a submission to the PJCIS review of the Assistance and Access Bill 2018 ("Bill"). We note the relatively short time frame available for submissions and trust that submissions received will be given due consideration.

We are deeply concerned with the Government's engagement in the process of putting together this Bill and the speed with which it has been rushed through Parliament. The Department of Home Affairs requested submissions on the proposed legislation giving a very short time frame for those submissions. Still, nearly 15,000 submissions were received by the Department, yet the legislation was passed through the lower house with minimal changes less than two weeks after the close of submissions. This makes a mockery of the consultation process, making it seem like little more than a box ticking exercise for the Department. We also note that submissions were not made publicly available by default which is not in line with the normal process in these cases.

This submission is on behalf of and jointly authored by Future Wise.¹ We are a group of Australian professionals of varied backgrounds who seek to promote ideas which improve the long-term direction of Australia, particularly in the areas of technology, health and education. More information about Future Wise is available on our website.² We are happy to provide further clarification of any of the points in the submission, or for one of the authors to attend the hearing in person if required.

Summary of Submission

Our concerns with the Bill include:

1. Its constitutional validity, there being no clear head of power that will support the scheme.
2. Despite assertions as to the need for the enhanced powers granted by the Bill, security responses to 'terror threats' still need to be weighed up as a necessary and proportionate response in light of the imperatives of privacy, transparency, and the overarching functionality of encrypted online services. The latter values are not adequately addressed in the Bill.
3. There is little to no oversight of these new powers. Interception agencies can issue requests without judicial oversight, or even oversight of the Attorney General.
4. The Bill exhibits overreach as to:
 - a. the purposes of the scheme, which extend well beyond the security concerns cited;
 - b. those who are covered by the scheme, where the scheme's scope encompasses almost any person broadly engaged in common uses of hardware and software;
 - c. the mandating of private sector capability-building which is not proximate to an instance of alleged potential harm, or activities that are sufficiently removed from harm as to call into question the urgency of the security imperative.
5. Despite asserting a prohibition on 'backdoor' systems, the scheme necessarily involves creation of encryption backdoors. Further, there is no identified threshold of singular backdoors which collectively would create a 'system'. This will result in unintended consequences that undermine information security.

¹ This submission complements the joint submission by the Australian Privacy Foundation, Digital Rights Watch, Electronic Frontiers Australia, the Queensland Council for Civil Liberties, the New South Wales Council for Civil Liberties, Access Now, and Blueprint for Free Speech.

² <https://www.futurewise.org.au>

6. The language of freedom is used to mask the coercive effect of the scheme which is disingenuous at best, and at worst, generates ambiguity in the meaning and operation of the Bill.
7. The interception agencies covered by the scheme are too broad.
8. The process of decision-making lacks accountability.
9. Penalties are not proportionate or reasonable.

The issues identified with this bill and its far-reaching impact on citizens, including those who may unwittingly become communication providers, and the relationships between the government and these groups mean that the Bill should at the very least, undergo a far more extensive and rigorous discussion in the public domain. Of particular concern, the foundation of the Bill lies in the power of the government to command private sector to provide access to endpoints with decrypted information. Realising that breaking encryption itself is untenable, the Bill attempts to make an end-run around encryption. Despite the assertion that the government 'has no interest in undermining systems that protect the fundamental security of communications',³ this is exactly the intent of the Bill. Even a single instance of a backdoor undermines information security that supports the online infrastructure of government services, the market, and society.⁴ Furthermore, these powers affect not just the intended target, but every user of a system an enforcement agency has requested to be compromised.

In the case of systems which have been developed with security and privacy by design, the technical capabilities notice provided by the Bill has potential for significant unintended consequences. Not only would the party receiving such a notice be essentially breaking the architecture and design of their system. The added capability is likely to result in unintended consequences which may create additional vulnerabilities in the system.

Ultimately, provisions seeking to foil criminal activity, including those in the Bill, will spawn new ways of hiding such activity to work around the scheme—ultimately reducing or negating the effectiveness of the Bill. For example, several the commonly used encrypted messaging applications are open source. In these instances, the targets of the Bill can just as easily download and compile applications for their devices making it impossible for interception agencies to target them anyway. The problem with this is that the price will be paid for by society at large, in having a weakened information security infrastructure on which contemporary service delivery, including government service delivery, depends.

The government has not yet made the case that the assistance and access provided for in the Bill is necessary, reasonable, or proportionate, relying instead on mere assertion. In light of the importance of encryption in contemporary government, economy, and society more broadly, the premise of decryption is unacceptable and the scheme as it is articulated in this Bill is fundamentally flawed and should not be passed.

We address below the question of constitutionality as well as the following specific aspects of the Bill:

- Its purpose
- Who is covered
- What is covered
- Decision making
- Compliance and enforcement

Constitutional Power

The Constitutional power under which this Bill is to be enacted is unclear. It is uncertain that regular heads of power, such as the corporations power,⁵ would be sufficient to support such an extensive scheme. The post and

³ *Assistance and Access Bill 2018 Explanatory Document* (August 2018) ('AAB Explanatory Document'), 10.

⁴ Chris Culnane, 'Assistance and Access Bill 2018' *State of IT* (30 August 2018) <https://stateofit.com/interception/>.

⁵ *Constitution*, s51(xx). In seeking to apply to individuals as well as corporations, the Bill would, in any event, need to come under an additional power.

telegraph power⁶ may cover the subject-matter of the Bill, but the applicability of the power to internet services is assumed rather than affirmed. It appears that Australia through its Five Eyes security network may have agreed to implement decryption provisions.⁷ This may bring the external affairs power⁸ into play. However, the status of this arrangement is yet to be determined.

In *Thomas v Mowbray*⁹ the High Court of Australia confirmed, by a majority of 5:2, that the defence power¹⁰ could support legislation dealing with threats other than an external threat, or war between nations. In this case, the power extended to enacting legislation to protect the public from terrorist acts. On this reasoning, the defence power may be invoked to support this Bill, but only to the extent that it provides protection against terrorist acts. The scope of the Bill concerning protecting revenue, or responding generally to criminal behaviour, for example, is beyond the remit of the defence power. Further, the power to mandate building capability is not proximate to the threat, being a longer term and less certain goal. This is in contrast to the nature of the laws upheld in *Thomas v Mowbray* calling into question whether these provisions have constitutional legitimacy.

This Bill appears to have a shaky constitutional basis, at best. At the very least, its scope should be considerably curtailed to bring it within the power of Parliament.

Purpose

The Bill's explanatory notes set the context for its purpose as dealing with terrorism.

...encrypted devices and applications are eroding the ability of our law enforcement and security agencies to access the intelligible data necessary to conduct investigations and gather evidence. 95 per cent of the Australian Security Intelligence Organisation's (ASIO) most dangerous counter-terrorism targets actively use encrypted messages to conceal their communications.¹¹

The contention is that modern life (notably through encryption) makes it difficult to gather intelligence and therefore intelligence services seek the power to interrupt modern life through mandating private sector decryption. Despite expressly prohibiting building 'systemic weaknesses' into products or services, this purpose fails to comprehend the enormous impact of vulnerabilities in encrypted communications on information security.

Further, and of significant concern, the Bill lists not only immediate and grave terrorist offences within the purpose of the scheme, but extends also to:

- enforcing the criminal law
- assisting the enforcement of the criminal laws in force in a foreign country¹²

Enforcing criminal law exceeds the purported imperative for national security or terrorism-related dangers.

⁶ *Constitution*, s51(v).

⁷ Ms Smith, 'Five Eyes Threatens to Force Encryption Backdoors, Says "Privacy is Not Absolute"' CSO (3 September 2018) <<https://www.csoonline.com/article/3301353/security/five-eyes-threaten-to-force-encryption-backdoors-privacy-is-not-absolute.htm>>.

⁸ *Constitution*, s51(xxix).

⁹ (2007) 233 CLR 307.

¹⁰ *Constitution*, s51(vi).

¹¹ *AAB Explanatory Document*, 7.

¹² See, eg, s317A.

There is no safeguard in relation to foreign law enforcement that other security agencies must adhere to any oversight mechanisms or human rights. This exemplifies the willingness of government to put at risk foundational principles of civil society in pursuit of surveillance mechanisms.

Even if national security could be a purpose that justified some kind of mandated decryption or access to endpoints, the remainder of the listed purposes should be removed.

Who is Covered by the Bill

Designated communications provider is defined in s317C to encompass ‘the full range of participants in the global communications supply chain, from carriers to over-the-top messaging service providers. This reflects the multi-layered nature of the communications environment and the types of entities that could meaningfully assist law enforcement and national security agencies.’¹³ Certainly, the list of those liable to participate is extensive.

Of note, a number of categories of ‘communications providers’ are so widely framed that their scope may—unwittingly or otherwise—encompass almost anyone using information communication technology. For example:

- ‘persons who provide an electronic service that has one or more end-users in Australia’ i.e. allowing end-users to access material using a carriage service: this is anyone who has a blog, or a website.
- ‘persons that develop, supply or update software used, for use, or likely to be used, in connection with a listed carriage service or an electronic service that has one or more end-users in Australia’ would capture anyone who uses open source software and develops an interoperable app or code, and students who are developing software. The example cited: ‘designing trust infrastructure used in encrypted communications or software utilised in secure messaging applications’ misleads as to the breadth of this category.
- ‘persons that manufacture, supply, install, maintain or operate a facility’ includes ‘any part of telecommunications infrastructure’. This would embrace most homes and businesses that connect to the internet.
- ‘persons that connect a facility to a telecommunications network in Australia...[including] mesh networks, private networks’: homes and businesses with private networks would be caught by this definition.

The rise of the internet of things—which connects potentially every commonly available device and appliance to the internet in a global web of information capture—will place almost every citizen within the ambit of the ‘global communications supply chain’ through the installation of hardware, downloading of software, and transfer of information. As interconnected contemporary and future information technologies become commonplace, the Bill’s scope will massively overreach in terms of its professed aims. Further, as discussed below, any backdoor capability puts the ‘internet of things’ system at risk.

The scope of ‘communications providers’ provided in the Bill bears no proportionality to the ostensible purpose of the Bill. While we acknowledge the challenge of comprehending those with the requisite role in the ‘information supply chain’ the framing of the Bill is unjustifiable and must be rejected. If the Bill is to proceed, the definition of ‘communications provider’ must be far more circumscribed.

¹³ AAB Explanatory Document, 24.

What is Covered by the Bill

The Bill permits law enforcement agencies to seek assistance to decrypt information in the execution of law enforcement functions. The types of assistance required is enumerated in s317E, but additional forms of assistance may be required for *technical assistance requests* and *technical assistance notices* (but not *technical capability notices*).

The Bill is framed, clearly, to address considerable concerns with creating 'backdoors' to encrypted data. To achieve this, there is a prohibition on a requirement to implement or build 'systemic weaknesses' (s317ZG). The Explanatory Document states that this ensures that 'a provider could not be required to install or utilise any agency software or equipment that weakens security across non-target devices or services.' (s317(1)(c)).

This ignores the reality that creating any backdoor weakens encryption generally.¹⁴ Coupled with the broad-ranging purposes these provisions create significant scope for weakening information security overall.

There is a further problem, namely that while any one notice or request may generate a single instance of decryption, multiple activities may collectively comprise a systemic weakness. The likelihood of this problem is exacerbated by the poor transparency and accountability provisions (discussed below). Without tracking each instance and understanding the relationship it bears to all others, it is impossible to know whether the scheme overall is creating structural backdoors.

There is also the possibility that the scope of the capability at the time it is requested will not be reflected in the end product: building any single capability may inadvertently generate a structural backdoor. However, by this time it will be too late. The legislation simply cannot prevent structural backdoors by prohibiting them. For the Bill to purport to provide an assurance of this to placate serious concerns with decryption is misleading at best.

A further concern with the scope of the scheme is the proximity of the likely information problem to the mandated activity. This is particularly the case with the *technical capability notice* which may require significant investment of privately-owned resources to build a *new* capability with the stated purpose of assisting law enforcement agencies. That this will take time and resources distances the effort from any immediate threat; the nature of the assistance is indirect relative to any law enforcement issue. This calls into question the proportionality of the scheme to address the professed problem.

Together, the activities covered by the Bill comprise a disastrous weakness of the scheme and justifies rejecting the Bill outright. Asserting that the scheme does not introduce backdoors is misleading in light of the explicit purpose of the legislation.

Decision-Making

This part addresses weaknesses in the way in which each of the three types of request or notice is made.

Voluntary Technical Assistance Request ('TAR')

¹⁴ See, eg, Tom Merritt, 'Top 5: Risks of Encryption Backdoors' *TechRepublic* (27 July 2017) <<https://www.techrepublic.com/article/top-5-risks-of-encryption-backdoors>>.

This requires a person to do a thing or to develop the capability to assist law enforcement to carry out its functions. TAR thus involves more than simply the supply of information—in requiring the ‘voluntary’ building of capability, it amounts to government co-opting private sector resources for the purpose of law enforcement.

It is stated to be ‘entirely voluntary but must be consistent with the powers and functions of the requesting agency.’ Immediately this raises the question of why there is a need for consistency with agency power if undertaking the work is in fact ‘voluntary’. This is a troubling aspect of the scheme in terms of authority. Under what authority is the relevant agency, or the government, making the request if it is to be undertaken on a voluntary basis?

In developing a new capability *for the government*, government is effectively commandeering private services as if under a war footing. The authority for government to usurp private property and business requires appropriate and constitutional authority and this seems to be eschewed in framing the work as ‘voluntary’. As to whether the government has sufficient power to require private enterprise to assist in this way is open to question.

Even if it could be argued that the ‘war’ against terror might justify commandeering private property, the scope of the purpose—including protection of public revenue for example—is so extensive that this power is unlikely to have sufficient legitimacy. Of note, public revenue in these provisions includes fines, charges, and debt collection. The ‘national economic well-being’ takes the purpose to another level entirely.¹⁵ This is an extremely broad remit that would not support what might be considered emergency powers.

‘The persons who can make technical assistance requests occupy the most senior position in their organisation and can exercise suitable judgment about the propriety of a request...’.¹⁶ Again this is mere assertion as to the capability of decision-makers and lacks principles of accountability, transparency, and oversight. Such decisions, if they are to be made, require extensive oversight. The provisions as they stand fail to provide suitable oversight mechanisms and should at the very least, be reconsidered.

The request might also be issued orally. This provides for no accountability and is entirely inappropriate given the nature of the request being put, and what is at stake for the subject of that request. The same can be said of an oral variation of a written request (s317JA).

Technical Assistance Notice (‘TAN’)

The Bill stipulates that in issuing a notice, the decision maker must be satisfied that:

- the requirements imposed by the notice are reasonable and proportionate; and
- (b) compliance with the notice is:
 - (i) practicable; and
 - (ii) technically feasible¹⁷

While the Bill itself does not identify anything further, the *AAB Explanatory Document* states that the issue of a TAN requires a subjective state of mind.¹⁸ This reflects the common law requirements of executive decision-

¹⁵ See s317E(j)(iv).

¹⁶ See s317G.

¹⁷ S317P.

¹⁸ *AAB Explanatory Document*, 34, citing *Minister for Immigration and Multicultural Affairs v Eshetu* (1999) 197 CLR 611 at 651-654; *Water Conservation and Irrigation Commission (NSW) v Browning* (1947) 74 CLR 492 at 505.

making. The *AAB Explanatory Document* further enumerates the weighing up of the interests of the agency and provider, the wider public interest, privacy, cyber-security and innocent third parties. Yet none of these weighing factors are incorporated into the text of the Bill itself. In light of the significant erosion of civil liberties attendant upon this Bill, it should provide more rigour in the decision-making process.

The TAN is not subject to merits review. While this is apparently consistent with recommendations of the Administrative Review Council,¹⁹ the *AAB Explanatory Document* says that there are ‘in-built safeguards to ensure that the scope of the powers do not go beyond what is reasonable and necessary to assist agencies’.²⁰ However, there appear to be few safeguards in the decision-making or oversight process. If this process is to come into force, there must be greater safeguards built into the Bill.

Technical Capability Notices (‘TCN’)

Decision-making on the issue of a TCN is ‘restricted to the highest levels of government’. Again, mere assertion of the capability of decision-makers does not make for good or transparent governance. More is required.

As with the capability-building purpose of a voluntary TAR, these notices effectively commandeer private resources for government purposes akin to a compulsory acquisition. These activities in particular contribute to construction of a government surveillance infrastructure in an economy thriving on data. It usurps business activity for the ends of a ‘war economy’ where the ‘war’ is on ‘terror’. Again, the breadth of purposes in the Bill is neither reasonable nor proportionate, and calls into question the legitimacy of these provisions.

These provisions should be rejected.

Compliance and Enforcement

The Explanatory Document is replete with the language of ‘cooperation’ and voluntariness. This is reflected also in the use of the term ‘enforcement remedies’ when what is provided for are penalties designed to compel and deter.²¹ Yet it contains coercive powers and harsh penalties for non-compliance with the regime, and a lack of clear protection for providers. The Explanatory Document thus misleads as to the true purpose of the Bill.

Penalties for disclosure of requisitioned services are harsh, including imprisonment for up to five years.²² There is no requirement for harm. The premise is therefore that the government may co-opt ordinary people to assist in top secret law enforcement activities, and may impose strict secrecy on those people at the risk of harsh penalties. The construct of the scheme is punitive and inappropriate given the breadth of scope and purpose.

At the very least, the penalties provisions should be reconsidered to reflect the breadth of the coercive powers available and those targeted by the powers.

In undertaking work pursuant to a *technical assistance request*, a provider has immunity from civil liability where the purpose is one of those enumerated, and the provider gives help to agencies in pursuit of their functions and powers furthering a ‘relevant objective’.²³ Yet there is no provision that the provider is to be told what the purpose

¹⁹ Administrative Review Council, ‘What Decisions Should be Subject to Merits Review’ (1999) 13.

²⁰ *AAB Explanatory Document*, 41.

²¹ *Ibid.*

²² S317ZF.

²³ S317G.

is. This leaves the provider in no position to assess whether the work they are ‘voluntarily’ undertaking complies with the legislation.

This is doubly problematic. First, the work undertaken is to be ‘voluntary’ rather than mandated which calls into question how a provider might assess the reasonableness or good faith involved in agreeing ‘voluntarily’ to undertake the work. Secondly, the mechanisms for protection of voluntary as opposed to mandated work is unclear as the work does not occur under a state delegation.

The indemnity provisions therefore leave providers exposed. At the very least, the ‘voluntary’ *technical assistance requests* should be omitted from the scheme.

Secondary Impacts of the Bill

Law enforcement arguments in favour of decryption seem to distil down to the primary justification that encrypted information should be readily available when there is a government desire for access to it.

If this is true and law enforcement agencies would only seek access to encrypted information on persons in whom they have a legitimate law enforcement interest, then the onus in an open and free democratic society must be on the law enforcement agencies to prove that they have this legitimate interest. The law enforcement agencies have not provided sufficient justification that, if access is required, it should be undertaken without a warrant, covertly as well as overtly, through the co-option of private resources, and by placing the foundation of information security at risk.

To the extent that legislation commands private sector or individuals to support enforcement capabilities in decryption, it generates significant inefficiency and loss of productivity, in that significant resources are required to meet law enforcement needs. This will also involve opportunity cost in building capability for obscure and secretive purposes at the expense of their own enterprise. Despite provisions for compensation for capability building, the government’s position seems to prefer private communications providers to bear the cost of that inefficiency. This is particularly problematic for small businesses where the opportunity cost is difficult, if impossible to gauge, and the loss of trust if the actions were made public would effectively decimate the business.

Conclusions

Future Wise’s position is that the government’s proposals for access and assistance as articulated in the Bill are neither necessary and proportionate²⁴ and that the Bill should be rejected.

We reject absolutely the assertion that any form of decryption or backdoor access to endpoints for government purposes (ie mandated or ‘voluntary’) is safe or proportionate to resolve ostensible challenges of law enforcement in dealing with information security.

²⁴ <https://en.necessaryandproportionate.org>.

Summary of Recommendations

- 1. The Bill be rejected by the Senate wholesale**
- 2. The period of consultation for the Bill be extended to allow more input from stakeholders but also the general public**

If the Department is not persuaded of this position, we urge it to at a strict minimum, accept the following recommendations:

- Purpose: Narrow the purpose of the legislation to embrace only national security threats
- Scope: Narrow the definition of communications provider to identify more specifically and realistically those who should be the subject of notices
- Oversight: record keeping requirements of the law enforcement agencies that have issued notices or requests needs to include the type of request, the purpose, how the capability was used, whether it altered the outcome of the investigation in a material way, a log of staff involved in the capability and confirmation that the capability was dealt with in a secure manner such that it would no longer be able to provide a backdoor. Remove any voluntary aspects of the Bill and require judicial oversight
- Sunset clause or mandatory review of the legislation