#AABill in economic context

Part 1: key perceptions about the economic implications of the legislation

20 December 2018

AustCyber's mission focuses on the economic opportunity of Australia's cyber security sector.

Many in Australia's cyber security industry have raised economically oriented concerns about the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* as well as the amendments made immediately prior to the Bill's passage through the Australian Parliament in early December 2018. It is unlikely – and understandably so – that companies have read, or had the opportunity to understand, the detail of the legislation as passed.

There has also been a lot of public and political discourse on the pros and cons of the legislation, some of which is conflicting and has created further confusion among the sector and its broader stakeholders.

AustCyber will deliver a series of communication materials that inform stakeholders on the facts, and where we see the need for clarification or further industry consultation on economic related issues.

To underpin this, we sponsored the Australian Strategic Policy Institute (ASPI) to deliver a report on industry's views on any potential or perceived impediments to sector growth stemming from the Bill. The report, *Perceptions survey: Industry views of the economic implications of the Assistance and Access Bill 2018*, was published on 20 December 2018 and is available here.

This document, Part 1 of the series referred to, seeks to support the Australian cyber security industry to better understand the facts and context of areas of the legislation industry have told us are of most concern for their company at this time, including through the survey process.

Contact us

E: info@austcyber.com | P: 02 9239 3250

T: @AustCyber | @Cyber_Roo

Relevant findings from the Perceptions Survey

The *Perceptions survey: Industry views of the economic implications of the Assistance and Access Bill 2018* identified four key perceived economic impacts among those surveyed:

- Compliance with the three forms of requests or orders has direct costs.
    - The Bill makes provision for 'reasonable cost' recovery for companies that provide compulsory assistance, but there was a widespread perception among survey respondents that costs would not be recovered.
- Companies may be negatively affected if a perception exists that Australian encryption products, products with Australian encryption embedded in them, or both, are less secure than competitor products as a result of the Bill.
    - Given that a level playing field will exist within the Australian market, this is more likely to be a problem for Australian exporters or for multinational firms doing business in Australia, whose products may be perceived to have been affected.
- Australian market participants seek to manipulate their ability to comply with the law, which would have development costs.
    - Under the provisions of the Bill, technical assistance and technical capability notices have to be 'practicable' and 'technically feasible'. This could create an incentive for companies to design their products so that providing access is not practicable or technically feasible, which would carry a cost.
- Poor or poorly thought through implementation of a technical capability notice could have costs for individual companies, as well as the broader ecosystem.
    - For example, if a company was asked to design a capability to access its product, there is a risk that it might inadvertently create a wider vulnerability, beyond what the company and the requesting government agency had anticipated or required.

In preparing this material, we received both a verbal briefing from the Department of Home Affairs as well as responses to a series of questions that we posed.

Since we published our first statement on this issue, we have appreciated the level of engagement from the Government.

The table below outlines the first tranche of questions that we asked of the Government after the Bill was passed. It also includes the Government's response and AustCyber's thoughts on what this means to Australia's cyber security sector from a economic perspective.

There remains a number of areas of concern that have not yet been adequately addressed. Where we have raised further questions, these have been provided to the Government but responses were not available at the time of publishing.

We are continuing to engage with industry and Government on these matters and will publish responses in future iterations of our communication toolkit.

What we asked:	What Government said:	Our thoughts:
Staff protections/ employee 'lockdowns' – media reporting and some industry commentary has suggested that employees may be required to process requests under the legislation without notifying their employers or others within the organisation. How would this work in operation, noting best practices across many areas of product development involve peer review, assessment etc?	The corporate entity or '*designated communications provider'* is the recipient of a notice. The legislation won't require an employee to be operating under a notice that their employer is ignorant of.	Since we asked this question, there has been further industry and media analysis of this area of concern which has helped tease out the complexity of this aspect of the legislation. To manage the business impacts of a notice being served, further guidance is needed about the various types of 'person' and how these definitions apply to the notion of a 'designated communications provider'. Beyond what is currently in the legislation, it must be clear to everyone what information can be shared between an employee and their employer, as well as between employees and, further, what information can be provided to external parties where there are commercial arrangements in place. We have and will continue to advocate for this guidance to be tailored to different roles in organisations, such as executive managers, security / IT practitioners and those in unrelated job roles.
Technical Capability Notices – what are the kinds of circumstances in which organisations will be issued notices and required to comply, including how terms such as 'systemic weakness' will be interpreted? The legislation identifies organisations can't be compelled to 'break'	The Assistance and Access Act has very strict limitations on the type of assistance that can be compelled by a notice. Numerous limitations and safeguards within the Act ensure a provider cannot be asked to 'break' encryption. However, a provider may be asked	If you have the capability to decrypt information within your product or service already, then on receiving a notice you may be required to use this capability to assist law enforcement or other authorised agencies.

encryption or create a 'key' where there is not already a mechanism to access data. Can you provide some straightforward wording around the 'lateral' opportunities to get access to communications across the supply chain?	to decrypt information if they are themselves capable of doing so for their business functions. For example, if a provider routinely decrypts data on their service for their own purposes, an agency may request that they decrypt data for public safety and national security purposes. Importantly, if the provider cannot decrypt the information on their services or products, the Act contains very clear limitations that rule-out any form of decryption capability from being mandated. This is not about 'backdoors'. Given this strict limitation, the Act allows agencies to seek assistance from a broader range of provider who may be able to give targeted assistance at multiple points in the supply chain. This will bolster the ability of agencies to gather the requisite evidence and intelligence (still subject to an underlying warrant) without needing to 'break' encryption or undermine cyber security. Section 317ZG sets out the most important limitations in the legislation. It makes clear that a provider can't be required to do things that would: • make systemic methods of authentication or encryption *less* effective	You can't be asked to develop a decryption capability under the legislation. Law enforcement and other authorised agencies can request assistance to access communications from a broad range of organisations across the telecommunications supply chain. Essentially, they can seek out multiple points for interception of the communication across a range of vendors in the supply chain. One of the stated limitations in the legislation is that it can't require a provider to make systemic methods of authentication or encryption less effective. It also can't prevent a provider from rectifying a systemic weakness or vulnerability. Defining key terms such as 'systemic weakness or vulnerability' and the process under which this will be assessed would reduce uncertainty and give clarity to cyber security stakeholders within Australia and internationally. We understand this will be one of the areas examined in the coming months.

	• stop a provider from rectifying an identified systemic weakness or vulnerability • build a decryption capability – this means companies cannot be asked to decrypt data if there is no existing capability to do it • create a material risk that otherwise secure information can be accessed by unauthorised third parties. Further, the power which can require a provider to build capabilities (the technical capability notices), **cannot** compel a provider to be capable of removing a form of electronic protection, like encryption.	
No profit/ no loss – how will this be calculated? What sorts of activities can organisations be compensated for (e.g. can loss of IP be considered under a 'loss' for monetary purposes?)?	The costs for complying with a compulsory notice is determined on a case-by-case basis however providers are not expected to bear the reasonable costs of complying with a requirement. The 'reasonable costs' of compliance may be different from the actual costs of meeting the requirements in a notice. For example, if a provider's expenditure is higher than necessary to satisfy the requirements in a notice, they are entitled to recover costs equivalent to the expenditure that would have been reasonable to satisfy requirements.	It is not clear how providers will seek reimbursement of expenses related to compliance with notices, or who will determine what costs are considered 'reasonable'. Uncertainty around what costs might be incurred and which of these will be recoverable is concerning from an economic impact perspective. More detail on the cost recovery model will likely address industry concerns on this matter.

Process around the appointment of a 'former judge' and 'technical person – will this be case-by-case, or for a period of time? What is the transparency around the process? Would the names of the appointees be public, or some characteristics about their professional expertise and why/ how they were chosen?	The Department of Home Affairs is currently identifying suitable independent technical experts and retired judges to constitute an assessment panel.	The identification of a panel, rather than individual(s), suggests there is opportunity for some diversity and independence. This will positively impact sentiment regarding the ability of providers to seek a fair review of notice. Transparency in the appointment process and diversity within the panel, including ensuring the technical experts are drawn from a range of expertise and professional backgrounds, is essential to maintain trust among providers. Specifically, there should be representatives who have no prior government employment to boost the perception of integrity and impartiality.
Speed to action – what are the 'emergency' circumstances that would cause the nominated 28-day consultation period to be waived for a capability notice?	The mandatory 28 day consultation period for issuing or varying a technical capability notice may be shortened if the notice must be given as a matter of urgency. This is to be determined by the Attorney-General on a case-by-case basis. For example, a shorter timeframe may be required where a capability can be built to prevent imminent harm to the public or where there is a serious risk that material evidence will be lost without the assistance of a provider.	The 28 day consultation period is, presumably, when issues such as 'systemic weakness' and 'creation of material risk' would be considered. The circumstances when a consultation period may be reduced from the mandatory 28 days relate to the prevention of harm to the public or loss of material evidence. It is not clear how proper consultation and consideration would occur under the emergency circumstances, and whether reducing the consultation time could increase the risk of other harms. Additionally, it is not clear how costs incurred in responding to a notice at speed might be reimbursed, or whether these would be considered 'reasonable' as outlined above.

		Clear and effective guidance on this, including providing scenarios and case studies, will help alleviate concerns.
Right of reply – what safeguards/ support will be in place for companies (particularly SMEs) who are served with capability notices, including those under 'emergency' circumstances, so they can get appropriate legal and other advice on their rights and responsibilities? Is there ability to be compensated for the costs (if any) of seeking this advice?	The Act explicitly requires agencies to inform, and provide advice to a provider about their rights and obligations when issued with a request or notice. Importantly, decision-makers will be required to notify the provider of their right to make a complaint in relation to the notice to the appropriate oversight body – either the IGIS or Commonwealth Ombudsman. As noted above, a provider is able to be compensated for the reasonable costs of compliance. Further, in relation to a technical capability notice, the Act provides a substantive review mechanism. Following a decision by the Attorney-General to issue a TCN, a provider can request the Attorney-General to appoint a technical and legal expert to determine if the TCN should have been issued. These experts will also have carriage to assess whether: • Whether the notice creates a systemic weakness or vulnerability • the requirements imposed by the notice are reasonable and proportionate,	There are mechanisms in place for providers to be informed of their rights and obligations, including the avenues for complaint and review of notices. These avenues include: • oversight bodies such as the IGIS or Commonwealth Ombudsman • a technical expert and retired judge, appointed via a panel arrangement (outlined earlier) • judicial review. It appears that clearly conveying this information to providers that receive notices is part of the intended implementation. This should cover a range of issues, including (but not limited to): • timeframe for legal review • rights of the entity • rights of employees • how to engage with stakeholders, including supply chain and customers • entitlement for reimbursement of costs, including legal costs.

	• compliance with the notice is practicable and technically feasible, and • the notice is the least intrusive measure that would be effective in achieving the legitimate objective of the notice. Finally, providers are able to seek judicial review of any administrative decision to issue a notice. There are many grounds by which to challenge a notice, including where: • a compulsory notice creates broader vulnerabilities in networks, or • it is infeasible that the decision-maker could consider requirements to be reasonable or proportionate.	Communicating this broadly to stakeholders – not just those that are served with a notice – will help build trust in the review process. The impartiality of the assessment panel and transparency in its appointment, as outlined previously, is very important to the review process. The avenues for review should be accessible to providers who need them, and require no (or minimal) cost in their time and resources. An efficient review process will help providers to support the objectives of the legislation.
Pentesters/ researchers who identify a vulnerability that has been created to comply with a notice – how would you expect someone to responsibly report this information and how will the various equities be managed?	The non-disclosure provision of the Act only apply to those with knowledge of the notice. A third party who discovers a vulnerability can still report in the usual way. The Act does not allow systemic weakness or vulnerability to be created via a notice. Under this provision, even a notice to hold open such a weakness or vulnerability could not be issued. Providers are entitled to patch systemic weaknesses and vulnerabilities when they are discovered, or if they are informed about them by third parties.	Further clarification and guidance for people who identify vulnerabilities is still required. For example, would an employee of an entity who responded to a notice be considered a 'third party' if they were not privy to the notice itself?

About AustCyber

AustCyber was established in 2017 as an independent, not-for-profit organisation. We are funded by federal government grants and form a part of two national programs:

- We are part of the federal government's Industry Growth Centres Initiative which was established through the National Innovation and Science Agenda. AustCyber is one of six centres that have been set up in sectors of competitive strength and strategic priority to boost innovation and science in Australia.
- We are an important part of *Australia's Cyber Security Strategy* as a key enabler for cyber security research and development, as well as innovation.

Our program of activities is underpinned by evidence gained through extensive research and consultation. Our flagship *Cyber Security Sector Competitiveness Plan* and the *Cyber Security Industry Roadmap* outline the opportunity for Australia's cyber security sector to support growth across the whole economy.

We are guided by our Board of members who have significant industry experience. Our team come from a variety of backgrounds including academia, government and industry.

The