Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 – Critical Weaknesses

The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the **Bill**) has been the subject of extensive review and analysis by numerous parties over the last two months. This includes hundreds of detailed submissions to the Department of Home Affairs commenting on the draft Bill, and more recently to the Joint Committee on Intelligence and Security as a consequence of its review of this proposed legislation. These submissions cover the gamut - from leading industry organisations, academics, telecommunications providers as well as from local SMEs to large international vendors. This paper leverages the key observations and points made by those parties, and others, in order to identify some specific failings in the bill. There is no attempt made here to consider in detail all aspects of the bill, merely to identify some of the worst examples of where the Bill is so fundamentally flawed that it will very likely result in serious and/or damaging consequences should it be passed into law.

The key aspects of the bill that are of most concern are:

1. The Bill will damage Australian developers' and manufacturers' reputations in international markets, resulting in loss of trust and confidence in Australian cyber security R&D and products. This will result in a decline in the current value of exports in this category (which exceeds $3b) and the loss of jobs and technical expertise in this industry as companies look to relocate offshore.
2. Rather than protecting the interests of citizens, this bill compromises their security and privacy as a consequence of weaker cyber security practices and easier access to new tools for cyber criminals.
3. The implications of poor integration testing of capabilities could lead to unforeseen consequences, including the potential for large scale network outages impacting internet service in Australia and throughout the world.
4. Despite the Government's claims to the contrary, the reality is that the proposed legislation will compromise critical encryption systems and introduce "systemic weaknesses" into products and the internet as a whole.
5. Notwithstanding the minor changes made to the Exposure draft, the Bill may force Providers to breach foreign laws (e.g. "substitution of services"). In such cases the Bill's immunity and defence provisions provide no effective protection in foreign courts. Even within Australia, the immunity clause provides no protection to other parties in the supply chain and no capacity to seek redress or compensation.
6. Based on dozens of media reports, together with submissions by hundreds of multinational, local vendors and technology experts, it is clear that the consultation undertaken over the last year has not succeeded in building even modest support for this legislation. The details of the proposed structure and scope for the legislation outlined in discussions held with industry participants would seem not to be consistent with the Bill as tabled. Many Australian corporations and particularly SMEs have not been consulted in any way.

In summary, even this limited analysis has identified major defects in the Bill that would see any of the potential benefits achieved by this proposed legislation far outweighed by the damage it would do to the nation's security, economy and internet-based services in addition to International reputation and trade. The Bill is so demonstrably flawed that the only practical option is to see it withdrawn. The Government should then review its primary objectives and commence genuine engagement and consultation with all stakeholders – including consumers, business, industry representatives, Technology & Communications Organisations (including Australian SMEs), Internet Standards bodies and academia in order to achieve a workable way forward.

1. The Bill will damage Australian developers' and manufacturers' reputations in international markets and result in a significant reduction in local R&D and manufacturing as a consequence of declining employment and export revenue.

Foreign Governments and competitors will use the existence of this legislation to claim that Australian cyber security products are required to use, or collaborate in, creating encryption "back-doors" or key escrows. With export values exceeding $3b we face the real prospect of sales being lost, exports declining, local companies failing or leaving Australia, jobs in this industry disappearing and related technical skills deteriorating.

Examples of Evidence supporting this position

Put simply, the proposed legislation is able to force Australian based technology and telecommunication companies to compromise the hardware and software they create – the majority of which is exported. This undermines earning of billions of dollars in revenue for the nation and the employment of thousands of people. This contribution to the national economy, and the jobs that go along with it, are clearly threatened. This is effectively analogous to Australia's treatment of Huawei. However, in this case, Australian companies can't deny it as the draft legislation is explicit. And if the customer suspects that they might have been targeted, the legislation also requires that the company must deny it - regardless of the truth. Any guarantee of security from an Australian technology company is therefore meaningless.

The Communications Alliance is the primary industry body representing telecommunications related providers in Australia. In its submission (#43) it noted that *"The attempted extraterritorial reach of the legislation is unprecedented and has the potential to generate anti-competitive outcomes and to create disincentives for providers to offer leading edge products and services to Australians."* The submission went on to state that *"The proposed legislation, through its mere existence, will make Australian exports of IT and communications products and services, or even every Australian website, subject to the same concerns by overseas Governments and organisations that recently moved the Australian Government to ban certain vendors from supplying hardware for Australia's future 5G networks. Therefore, the draft Bill poses a real risk for the IT/communications export industry which Austrade values at AUD 3.2 billion (2016/17) and this figure does not even include the value of other exports enabled by Australian websites, IT and communications products."*

No less authority than The Internet Architecture Board (IAB) confirms the validity of this concern. The IAB is chartered both as a committee of the Internet Engineering Task Force (IETF) and an advisory body of the Internet Society. The IETF is the global body that is responsible for all Internet standards. In its submission (#23), the IAB notes that *"Any method used to compel an infrastructure provider to break encryption or provide false trust arrangements introduces a systemic weakness, as it erodes trust in the Internet itself. In other words, the mere ability to compel Internet infrastructure providers' compliance introduces that vulnerability to the entire system, because it weakens that same trust."* It goes on to state that *"The IETF, in RFC 2804, has rejected the development of any system designed to aid state actors in compromise of the security of Internet communications. Compelling individual participants to act contrary to that consensus introduces doubts about the motivations of and influences upon a participant's actions, and therefore may disadvantage Australian participants in these processes."*

2. The Bill compromises good cyber security practices and risks increasing cyber crime

The proposed legislation has the perverse effect of encouraging poor cyber security practices for individuals, enterprises and even government agencies. It will also very likely lead to improving access to better and more capable tools for cyber criminals.

Examples of Evidence supporting this position

In the enterprise and government context, the increased possibility of internal or external actors becoming aware of weaknesses introduced into systems as a result of requests made by government agencies under the legislation could lead to increased security risks. For example, the Bill creates a disincentive for parties discovering a weakness, or possible zero-day exploit in a system, to alert the user, relevant authorities and/or the technology or network provider as they may perceive a risk of being in breach of the legislation and subject to a fine and/or imprisonment. Conversely but importantly, the very existence of these weaknesses and exploits increases the risk of discovery and disclosure. From the perspective of an internal or external 'bad actor', becoming aware of a "systemic weakness" may act as an incentive to misuse that information, make it known to others and/or sell the information discreetly.

There have been numerous reliable reports of the NSA having its "hacking tools" stolen and used or repurposed for use by cyber criminals or others. There is some speculation that up to 75% of the NSA's tools have found their way into the wild[i]. In the wrong hands, these tools enable bad actors to remotely access and control various Windows, Unix and other platforms. There is very strong evidence to suggest that cyber criminals have used weaknesses found/created by the NSA to access the SWIFT interbank financial transfer system. Cyber Criminals have now successfully used these tools to target a number of banks. One of the most damaging attacks ever inflicted on internet users worldwide, using the WannaCry Ransomware tool, is now widely believed to have been derived, in part, from an NSA exploit.

This is not an attack on the NSA. The intention is to demonstrate that even highly secure government operations are not able to keep these capabilities safe/secret. This Bill almost guarantees that capabilities created as a consequence of a TCN will come to be misused - given that they are necessarily known by several parties and staff within the commercial entity(s) involved. In the absence of any clearance process for these personnel, the threat of prosecution is unlikely to always be sufficient as to outweigh the financial opportunity presented. Worse, for foreign corporations, the development effort will likely take place offshore. In the context of some software communities, code transparency is core and attempts to modify code will be identified by the support community. This will lead to either compromising the capability, identifying the target or to its misuse. Independent Software Auditors have full access to source code and when based in a separate jurisdiction, provide no prospect of the reporting of any compromise being kept secret.

In addition, the issues noted in item 1 above with respect to the perception of the Bill and its effect could lead to broader impacts on, and consequences for, the security hygiene of individuals and organisations. The ASD has stated that one of the most critical and fundamental aspects of Cyber Security is the need to ensure that computer systems' software is constantly kept up-to-date (ASD Essential 8, regarding Patch Management of Applications and Operating Systems). Should this Bill become law, many individuals and organisations will very likely adopt more cautious approaches to security patch management and systems updates out of concerns that such updates may have arisen from (and implement certain capabilities and features pursuant to) a request under the legislation. In particular, Firmware updates, Anti-Virus and Malware tools are highly likely to be viewed with suspicion by users given the system access they provide.

In essence, working with commercial organisations to develop and deploy these types of capabilities (as envisaged by this Bill), will result in high risks combined with extreme consequences – for all parties. The Government will be held accountable regardless.

3. Poor integration testing of capabilities could lead to unforeseen consequences, including the potential for large scale network outages impacting internet service in Australia and throughout the world.

Changes to communications systems and to any devices or technologies forming part of the supply chain of such systems (without undertaking extensive and expensive regression and integration testing) could lead to any number of unforeseen consequences resulting from an inability to follow standard software development and testing procedures, including the potential to compromise the wider security of those systems and potentially make them unstable.

Examples of Evidence supporting this position

Today's telecommunication networks are highly complex systems typically consisting of tightly coupled software and hardware products provided by dozens of different vendors and manufacturers. The fact that they work at all is a result of adherence to detailed specifications, rigorous compliance to standards, extensive integration efforts and thorough testing. In the context of the provisions of this Bill, a Provider implementing changes under a TCN (for example) seriously compromises normal practices. The short timeframes and limited ability to consult other participants in the network ecosystem may make the ability to conduct such integration and testing procedures challenging if not impossible. Changes that are then made unilaterally to hardware and/or software without integration and regression testing across these types of multi-vendor systems creates a real risk of degrading network performance or causing the network and/or individual components to fail entirely. In the context of core telecommunications systems, this could cause catastrophic outages across a wide scale.

In its submission to the Draft (Exposure) Bill, Telstra noted that the Bill *"covers the entire communications services supply chain, making it possible a TA Notice or TC Notice could require 'modification' to a piece of network equipment or its operating software without the knowledge or awareness of other communications providers. For example, if a telecommunications provider (such as a carrier or carriage service provider) uses equipment or software supplied by a third party, that third party may have been separately required to provide technical assistance to an agency (potentially including the installation of software or equipment supplied by the agency) or to introduce new technical capability into their products. Given the secrecy provisions of the Bill, this could occur without the knowledge of the telecommunications provider and could result in an adverse impact to its network and/or customers' use of the network. Such adverse effects could include service degradation, network faults, or other impacts on its business, or on non-target customers."*

In its submission to the Draft (Exposure) Bill, Optus expressed similar concerns though focused primarily on the degree to which requests of it should be subject to a period of consultation to ensure that the request is practical, technically feasible and that the consequent commercial risks are understood.

The potential for a small, and otherwise insignificant, change to a component of the network resulting in catastrophic failure cannot be discounted. For example, in May 2018, Telstra suffered an Australia wide outage of its 4G network. This failure was apparently caused by a single element of software provided by one of its many "technology vendors". In the same month the Triple Zero outage resulted in over 1,400 emergency calls not being answered. As a result of ACMA's six month investigation, we now know that this was caused by a hardware failure in just one controller card in Melbourne. In both cases Telstra's redundant systems also failed to respond.

In the context of the proposed legislation, there is no easy way for a party affected to track down the source of the problem since the change would likely have been made in an undocumented fashion. Even if they were able to identify it, there is also no legal capacity for the affected party to direct the Provider to clarify why it occurred or even rectify the problem. The obvious response by a telecommunication company to this situation would be to remove the offending product or restore it to a previous working state. Either of these actions could put the Provider and telecommunications company in a legally uncertain situation in terms of both criminal provisions in the Bill or civil action between the parties and/or by customers.

4. Despite claims to the contrary the proposed legislation does allow for encryption to be compromised and other systemic weaknesses to be introduced.

The Government's claims that the proposed legislation will not compromise critical encryption systems or introduce any "systemic weaknesses" into products do not stand up to scrutiny. While the Bill includes words (at Clause 317ZG) to the effect that the "communications provider must not be required to implement or build a systemic weakness or systemic vulnerability" or to "render systemic methods of authentication or encryption less effective" the analysis undertaken by numerous parties demonstrates that this clause does not, and almost certainly, cannot achieve this aim.

Examples of Evidence supporting this position

Cisco is the world leader in building global internet infrastructure and with 85% of internet traffic passing through Cisco products has arguably more experience in networking than any other company in the world. In its submission (#42), Cisco considers the issue of "backdoors" in great detail and states categorically that "*…the Bill would require via a TCN the creation of a capability while simultaneously preventing the DCP from documenting the existence of that capability, the law would result in the creation of backdoors.*".

The Massachusetts Institute of Technology (MIT) has established the Internet Policy Research Initiative (IPRI) "*to work with policy makers and technologists to increase the trustworthiness and effectiveness of interconnected digital systems*". The IPRI is generally regarded as the pre-eminent institution undertaking research and advising industry and government in this field. In its submission (#32), it has stated that they *"have yet to identify a system design that would allow law enforcement the requested access without introducing systemic weaknesses or vulnerabilities."* And this Bill is no exception.

The MIT submission also noted that "*failed cryptographic protocols can cause outsized damage in unexpected ways that last far beyond when they were discovered to be faulty. For example, the FREAK and DROWN exploits were only possible because earlier regulatory mandates to weaken encryption on products exported from the United States left critical systems perpetually vulnerable as Internet servers continued to support out-of-date software exported under the regulation."* And that as a consequence of this *"At one point, roughly 12% of the top million most visited websites were completely interceptable, allowing attackers to gain user credentials, passwords, and other private data."*

In its submission(#52), the Inspector-General of Intelligence and Security (IGIS) noted "*The potential for intelligence agencies to make technical assistance requests for the voluntary creation of 'backdoors'* " and that "*the amendments in Schedule 1 do not limit the power of any agency to request communications providers to introduce, or omit rectify, a systemic weakness or vulnerability into a form of electronic protection."* Presumably tongue-in-cheek, the IGIS noted that it was "*unclear if this result is intended".*

5. Providers are exposed to legal, financial and reputational risk with little or no protection available to them in foreign courts.

The Bill creates a high risk of Providers with international operations being in breach of foreign laws – simply by acting in accordance with provisions in the Bill (e.g. "substitution of services"). In such cases the Bill's immunity and defence provisions provide no effective protection in foreign courts. Even within Australia, the immunity clause provides no protection to other parties in the supply chain.

Examples of Evidence supporting this position

In its submission (#76), the Law Council of Australia noted that the issuing of a TCN to organisations with operations outside Australia and "*subject to foreign laws which preclude response to exercise of these measures are not afforded any defence in compliance with notices issued under this Bill. The safe harbour under proposed subsection 317ZB(5) is only in relation to legal proceedings for imposition of a civil penalty order: that is, the safe harbour is only in respect of the imposition of a financial penalty for committing an offence, not a safe harbour from being found to have committed an offence. This creates potential reputational and financial risk and jeopardy for many organisations that are required to report as to their compliance with laws."*

This is not a theoretical issue and foreign companies with subsidiary operations in Australia are particularly exposed here.

Apple Inc noted in its submission (#53) that "*Like Australia, many foreign countries have laws that prevent (in some cases in the form of criminal penalties) a party from accessing, altering, or providing access to a communications system or data storage device. Accordingly, a TAN or TCN may require an act or omission which, if carried out, would breach the law of a foreign country. In addition to suffering potential criminal liability for complying with a TAN or TCN in a foreign country, a provider may also suffer severe civil liability.*

Even though this bill grants immunity for compliance with a TAN or TCN, it does not and cannot extend that immunity to cover liability in foreign jurisdictions." The submission went on to note, as an example, that "*If Australian authorities were to issue a TAN or TCN that required access to data of European Union citizens, Apple could face stiff penalties of up to 4% of its annual turnover under the General Data Protection Regulation, were it to comply.* " Based on its current revenue, that would amount to a penalty of approximately $10 billion, a figure that easily exceeds Apple's total annual revenue from its Australian operations.

In its submission to the Draft (Exposure) Bill, Telstra note that the Bill *"covers the entire communications services supply chain, making it possible a TA Notice or TC Notice could require 'modification' to a piece of network equipment or its operating software without the knowledge or awareness of other communications providers."* It went on to give the example of a carriage service provider, suffering service degradation or failure as a consequence of a third party in its supply chain being the subject of the provisions of the Bill. In such cases this may affect the carrier's services to many customers and significantly impact its business. Not only would the immunity clause provide no protection to it and other parties in the supply chain, the secrecy provisions in the Bill would prevent all parties from even explaining the cause of the failure. The reputational and financial risks are severe.

6. The consultation undertaken has been misleading. Consequently, the Government cannot claim to have the broad support necessary for such radical legislation.

Based on dozens of media reports, together with the number and content of the actual submissions by hundreds of multinationals, local vendors and technology experts, it is clear that the consultation undertaken over the last year has not succeeded in building even modest support for this legislation. That consultation, such as it was, has been limited in number and content. The details of the proposed structure and scope for the legislation outlined in those discussions would seem not to be consistent with the Bill as tabled. Submissions and feedback provided in response to the Exposure (Draft) Bill have largely been ignored. Many Australian corporations, and particularly SMEs, have not been consulted in any way.

Examples of Evidence supporting this position

The original scope proposed for this legislation, when it was first raised in 2017, was to address national security issues, including terrorism and cybercrime, money laundering, general criminal activity, illegal transmission of sexually explicit material and the activities of pedophiles. Up until the release of the Exposure (Draft) Bill, statements by current and former Ministers consistently identified this as the target group.

In its submission (#76), the Law Council of Australia notes that the Explanatory Memorandum states that the Bill "*has been developed to address threats by terrorists, child sex offenders and criminal organisations who use encryption and other forms of electronic protection to mask illegal conduct.*" However, the Law Council goes on to observe that the actual legislation appears to be at significant odds with this and with the statements made in the Explanatory Memorandum. In particular that:

- "*the measures proposed go far beyond these threats, to include lesser unlawful acts…*"
- The "*exercise of power in relation to a particular set of facts or allegations is not required to take into account the wider context of maintaining citizen trust…*"
- The Bill "*confers an unstructured discretion*" on decision makers who are not required to assess the degree to which a measure is 'reasonable and proportionate'.

There are numerous inconsistencies elsewhere in the Bill. Apple, in its submission (#53) notes that "*On its face, the bill seems to forbid the government from requiring a provider to maintain an interception capability. Yet, like the bill's other purported limitations, the exceptions swallow the rule. Here, the limitation does not apply to ASIO computer access warrants, which can authorise access to a targeted computer to gather intelligence. This bill would allow ASIO to issue an order to a provider to build a capability to intercept encrypted communications to and from a particular device.* "

As outlined by numerous submissions, claims by Ministers and Officials that the Bill will not allow for the creation or retention of data, access to content, establish system weaknesses or vulnerabilities, or to compromise encryption systems, have all been shown to be false.

As it stands, the Bill is entirely consistent with that which might be proposed by an authoritarian regime. It is simply unacceptable for a democracy. The Government needs to undertake proper consultation, propose legislation that is proportionate to the nature of the problem/threat and build consensus with industry (including local SMEs), the community and other stakeholders.

[i] https://www.washingtonpost.com/world/national-security/prosecutors-to-seek-indictment-against-former-nsa-contractor-as-early-as-this-week/2017/02/06/362a22ca-ec83-11e6-9662-6eedf1627882_story.html?noredirect=on&utm_term=.2a808553b5eb