12 October 2018

Parliamentary Joint Committee on Intelligence and Security
By online submission

TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) BILL 2018 – BSA COMMENTS

A. Statement of Interest and Summary

BSA | The Software Alliance (**BSA**) is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members[1] earn users' confidence by providing essential security technologies, such as encryption, to protect customers from cyber threats. These threats are posed by a broad range of malicious actors, including those who would steal citizens' identities, harm their loved ones, steal commercially valuable secrets, or pose immediate danger to national security.

BSA and our members thus have a significant interest in the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (**Bill**) introduced into the House of Representatives on 20 September 2018, which we understand is designed to enhance assistance from the communications industry and better enable law enforcement to investigate criminal and terrorist activities in the digital era.

BSA had earlier submitted comments to Australia's Department of Home Affairs (**DHA**) [2] on the exposure draft of the Bill, and our interest in the Bill remains undiminished. We commend the Australian Government on having made various positive changes in the Bill since the exposure draft, and offer these updated comments and recommendations for consideration by the Parliamentary Committee on Intelligence and Security (**Committee**) in its review of the Bill.

In summary, we recommend that:

1. the assistance and access regime should be underpinned by judicial authorization and a review process, wherein decisions to issue mandatory notices are made only by an independent judicial authority, and a robust and transparent review mechanism is available to the subjects of such notices;

[1] BSA's members include: Adobe, Akamai, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Baseplan Software, Bentley Systems, Box, CA Technologies, Cad Pacific/Power Space, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, and Workday.

[2] A copy of BSA's comments to the DHA is available at: https://www.bsa.org/~/media/Files/Policy/Data/09102018BSACommentsAssistanceandAccessBill2018.pdf

2. the "acts or things" that can be required from a service provider should be narrowed and made exhaustive, and the carve-out for "systemic weaknesses" should be expanded to include any weakness or vulnerability in any system, product, service or component;

3. the scope of the circumstances in which the powers under the Bill can be exercised should be limited to preventing or detecting serious crime and protecting against identified threats to national security in narrowly defined circumstances;

4. the application of the Bill to "designated communications providers" should be limited, both in terms of extraterritorial effect and the types of organizations that are subject to the Bill;

5. technical information disclosed by service providers should be protected by the relevant agencies; and

6. the new computer access warrants regime should include the same limitations and safeguards as the assistance and access regime.

B. General Comments

We acknowledge and support the Australian Government's desire to have more powerful tools to aid in the fight against criminal and terrorist activity and to ensure that the rule of law applies equally to online and offline activity. As the Government considers new legislation to expand surveillance powers, one key area of focus is the ability of Australian law enforcement to access digital evidence. BSA supports this objective, and encourages close collaboration between the Government, Australian law enforcement, and the technology community to improve processes and methodologies enabling law enforcement access to digital evidence in a timely manner. At the same time, the debate over this legislation should not seek improvements to law enforcement access at the expense of privacy and security.

Given the complexity and sensitivity of the subject matter, we strongly encourage the Australian Government not to rush legislation, and instead take the time to thoroughly consider the broader issues at play and the implications (and possible unintended consequences) of the draft legislation.

The importance of security, privacy, and trust in the digital economy

Modern technology is giving us the potential to improve almost every aspect of our lives. BSA members are at the forefront of these data-driven innovations, including cutting-edge advancements in artificial intelligence, machine learning, cloud-based analytics, and the Internet of Things. These innovations are helping to make our devices smarter, our businesses more competitive, and the delivery of government services more efficient. Economists estimate that these technologies can grow Australia's GDP by an incredible 1.2% per year, adding $250 billion to the economy by 2025.[3] Australia's forthcoming Digital Economy Strategy also recognizes the importance of modern technology to Australia's long-term strategic interests.[4]

Such technology, which is now an integral part of every sector (including, manufacturing, logistics, transport, financial, legal, retail, and public services, to name a few), rely on a range of capabilities – including strong encryption, robust identity and authentication management, regular security patching,

[3] Simon Blackburn, Michaela Freeland, and Dorian Gärtner, Digital Australia: Seizing Opportunities From the Fourth Industrial Revolution, McKinsey & Company (May 2017), available at https://www.mckinsey.com/featured-insights/asia-pacific/digital-australia-seizing-opportunity-from-the-fourth-industrial-revolution.

[4] *Australian Government Response to Innovation and Science Australia 2030 Plan* (May 2018), available at https://www.industry.gov.au/innovation/InnovationPolicy/Documents/Government-Response-ISA-2030-Plan.pdf.

and secure configurations – to safeguard not only privacy, but also the security and safety of communications and transmissions.

In the delivery of critical services such as electricity, for example, encryption is used to protect data in transit across the electricity grid, including communications to and from operations centers, power generation systems, distribution stations, and home "smart grid" networks. The potential disruption that cyber attacks could have on critical services has already been demonstrated when, on two separate occasions, hackers shut off power for hundreds of thousands of citizens in Ukraine.[5] This dependence underscores how critical it is to ensure that this legislation is successful in improving law enforcement capacity to investigate serious crimes without compromising the technologies and tools that underpin security, privacy, and trust in the digital economy.

Access to Digital Evidence

A number of factors bear on law enforcement's ability to access digital evidence in an ever-changing technological landscape. As communications, business processes, and routine daily activities are increasingly digitalized, more data – and more different types of data sets – are available to law enforcement than ever before. The rapidly increasing volume of data presents diverse new opportunities for law enforcement. Millions of Australians have transitioned in recent years from relying strictly on difficult-to-access telephone and written communications to digitally transmitted and stored emails, text messages, phone calls, instant messages, social media postings, and other communications. Other data, such as information about individuals' banking transactions, purchases, Internet browsing histories, and geolocation, is also increasingly digitalized and available to law enforcement with appropriate process. Yet, this increasing volume of information also presents new challenges. Law enforcement's ability to access such data can be challenged by factors such as limitations in technical training and capabilities for accessing diverse data types, continually evolving technologies, and insufficient forensic laboratory capacity.

BSA's members have worked closely with law enforcement in Australia, the United States, the United Kingdom, and elsewhere around the world to ensure that law enforcement can access digital evidence in support of lawful criminal investigations in a timely manner pursuant to appropriate safeguards. For law enforcement to take advantage of the opportunities new technologies bring, and to overcome the array of associated challenges, digital evidence access must be approached collaboratively. In this regard, the Bill must serve as a platform to facilitate and deepen collaboration between the technology and law enforcement communities by establishing the foundation of a constructive partnership that takes into account the priorities, needs, and sensitivities of all relevant stakeholders.

The needs of law enforcement, technology providers, and the consumers whose privacy interests are at stake, are best met by policies and laws that provide for robust mechanisms for judicial oversight, transparency of activities, privacy protections, and clearly defined processes for bi-directional communication on law enforcement needs. In addition, as data is stored by global organizations subject to laws in different countries, it is increasingly important that laws for government access be interoperable.

BSA strongly urges continued dialogue between the Australian Government, policy-makers, and industry to find a solution that balances the legitimate rights, needs, and responsibilities of the Government, citizens, providers of critical infrastructure, third party stewards of data, and innovators. We would also welcome the opportunity to speak with the Committee at any hearing it holds.

[5] *How an Entire Nation Became Russia's Test Lab for Cyberwar*, Wired (June 20, 2017), available at https://www.wired.com/story/russian-hackers-attack-ukraine/.

C. Specific Comments and Recommendations

While the Bill addresses a range of issues associated with law enforcement assistance and access, BSA is chiefly concerned with the authorities outlined in Schedule 1 of the Bill for law enforcement to request or compel assistance from technology organizations in accessing electronic communications information; namely, the authorities to issue voluntary technical assistance requests (**TARs**), mandatory technical assistance notices (**TANs**), and technical capability notices (**TCNs**). The proposed TAN and TCN provisions, in particular, represent extraordinary new authorities of unprecedented scope and application.

BSA appreciates that the Australian Government has sought to build certain safeguards into the Bill, including laudable provisions ensuring that technology organizations are not required to implement "back doors" or to build systemic weaknesses into forms of electronic protection. However, BSA is concerned that the safeguards do not go far enough to protect principles such as security, privacy, and trust in the digital economy.

Accordingly, in addition to our general comments in Section B above on the policy and global regulatory environment, BSA offers in this Section C our specific comments and recommendations on the Bill (which we elaborate upon in Section D below):

1. ***The assistance and access regime should be underpinned by judicial authorization and a review process***

   The current Bill lacks a sufficient role for independent judicial authorities to oversee the issuance of mandatory TANs and TCNs. Decision-makers under the Bill can issue notices with very limited judicial oversight, based on evidence that may be unknown to the designated communications provider (**Provider**), and a subjective assessment of reasonableness and proportionality.[6] While the Bill includes a negotiation process that can culminate in arbitration, this is focused on the *terms and conditions* of compliance, not whether it is appropriate for the notice to be issued in the first place.

   BSA applauds the inclusion of new provisions in the Bill requiring the decision-maker to consider various matters before issuing a TAN or TCN, such as the legitimate interests of the Provider and the legitimate expectations of Australian citizens relating to cybersecurity and privacy.[7] However, while these considerations are important, they should be considered by an independent, objective judicial authority rather

   Example of issue that could arise under the current Bill:

   A law enforcement agency suspects that information stored in an encrypted form on a Provider's hosting service, by a customer of the Provider, is relevant to the agency's criminal investigation. The agency secures a warrant to compel the Provider to disclose the information. The agency then takes the view that the Provider can decrypt and hand over the information, based on misinformation that the Provider has a 'master decryption key'. The agency issues a TAN without consulting the Provider. The Provider does not have such a key but is unable to convince the agency to change its assessment because the Provider does not have any insight into the factors considered by the agency. The Provider is subsequently found to be in breach of the TAN requirement.

   Judicial review may be precluded as the agency in this case could be acting within its scope of authority, as it has secured the underlying warrant, and the Bill does not require the agency to go through a further consultation process with the Provider. The Provider could therefore be left without remedy or recourse.

[6] See the following paragraphs from the explanatory memorandum accompanying the Bill:
- Paragraphs 46 and 47 of the Statement of Compatibility with Human Rights (page 16);
- Paragraph 8 of the Notes on Clauses (page 29);
- Paragraph 130 of the Notes on Clauses (page 49); and
- Paragraph 174 of the Notes on Clauses (page 55).

[7] See, in particular, new sections 317RA and 317ZAA of the *Telecommunications Act 1997* proposed to be inserted by the Bill.

than by the agency seeking to issue the TAN or TCN.

The regime should also allow the Provider to challenge the issuing of the TAN or TCN, as well as its scope and terms, before an independent judicial authority. In this regard, although we have significant concerns with some elements of the recent *Statement of Principles on Access to Evidence and Encryption*, issued in August 2018 by the governments of the United States, the United Kingdom, Canada, Australia and New Zealand, we agree with its statement that: "*The principle that access by authorities to the information of private citizens occurs only pursuant to the rule of law and due process is fundamental to maintaining the values of our democratic society in all circumstances – whether in their homes, personal effects, devices, or communications*".

BSA recommends that:

- the decision to issue a TAN or TCN should be made by an independent judicial authority based on evidence from the requesting agency regarding the necessity of issuing a notice, as well as the reasonableness, proportionality, practicability, and feasibility of the proposed requirements; and

- the Bill should incorporate a robust judicial oversight and challenge mechanism that provides for full and transparent due process.

BSA also urges the Australian Parliament, as it considers the Bill and the issues it raises, to consider the precedent that the Bill – and its treatment of the question of independent judicial oversight – will set for other democratic and non-democratic governments, as they look to Australia's model in considering similar legislation.

2. ***The "acts or things" that can be required from a Provider should be narrowed and made exhaustive, and the carve-out for "systemic weaknesses" should be expanded***

The Bill sets forth a non-exhaustive list of "acts or things" that Australian Government agencies would be authorized to require of Providers through TANs or TCNs.[8] As currently framed, this would effectively allow Government decision-makers to require a Provider to do *anything* they deem appropriate, leaving such decision-makers broad discretion in determining such measures. The breadth of this scope not only creates potential technical and legal challenges for Providers, but also presents risks to cybersecurity.

BSA is also concerned that the carve-out in relation to "systemic weaknesses" in respect of "a form of electronic protection" is too narrow because the Provider could still be required to: (a) take actions that impact system security in a non-systemic way; or (b) implement a systemic weakness into something other than electronic protection.

Example of issue that could arise under the current Bill:

The "acts or things" envisioned in the Bill could compel Providers to compromise system security by:

- removing electronic protections applied for cybersecurity purposes;

- installing untested or uncertified software that could inadvertently introduce new systemic vulnerabilities; and

- disclosing vulnerabilities that have not yet been patched.

These vulnerabilities can all be exploited by bad actors, including nation state bad actors, who learn of these vulnerabilities.

[8] See, in particular, new sections 317L(3) and 317T(7) of the *Telecommunications Act 1997* proposed to be inserted by the Bill.

BSA recommends that:

- each of the "acts or things" should be further clarified (our specific recommendations are set out in Section D of this submission), and that the list itself should be exhaustive and subject to an overarching condition that the requirements imposed on designated communications providers are the minimum necessary required for the relevant objective;

- Providers should not be compelled to reveal details of vulnerabilities which have not yet been patched, and a transparent policy for handling and disclosing vulnerabilities the Government discovers and that are unknown to the Provider should be included in the Bill;

- the "systemic weakness" carve-out should be broadened to include *any weakness or vulnerability* in *any system, product, service, or component*; and

- all of the "acts or things" should be subject to a requirement that they are practical and technically feasible.

3. ***The scope of the circumstances in which the powers can be exercised should be limited to preventing or detecting serious crime and protecting against identified threats to national security in narrowly defined circumstances***

The Bill authorizes the issuance of TANs and TCNs for the purposes of "(a) enforcing the criminal law and laws imposing pecuniary penalties; or (b) assisting the enforcement of the criminal laws in force in a foreign country; or (c) safeguarding national security."[9] TARs can be issued for an even broader set of purposes, adding "the interests of Australia's foreign relations or the interests of Australia's national economic well-being" to the list.

Given the breadth of "acts or things" that can be required of Providers, BSA is concerned that the scope of circumstances in which the powers can be exercised is likewise unduly broad. BSA appreciates that the authors of the Bill have sought to narrow this scope by omitting "protecting the public revenue" from the list of purposes for which TARs, TANs, and TCNs can be issued. However, the remaining purposes – particularly the broad national security objective – remain broad and vague.

The principle that organizations could be required to engage in "acts or things" that go far beyond preventing or detecting serious crime or protecting against identified threats to national security under certain narrowly defined circumstances is troubling. Particularly in light of the absence of robust judicial oversight, this could empower Government decision-makers to require Providers to take actions beyond addressing

Example of issues that could arise under the current Bill:

Example 1: The Attorney-General, following a request from a law enforcement agency, issues a TCN requiring an international mobile device provider to develop and implant chips on mobile communications devices sold in Australia. The chips are intended to allow the agency to, when circumstances dictate, turn the device into a geolocation beacon to gather intelligence on foreign officials in Australia. After the devices are deployed into the market, the existence of the chip in the device is leaked. The mobile device provider's global reputation suffers as customers doubt the integrity of their devices and the privacy of their communications, and the provider's market share plummets, destroying its business.

Example 2: Country X, seeking to also have greater legislative powers to obtain access to information, could copy the current Bill wholesale and enact it. An agency in Country X uses the very broad powers under the law to compel a service provider operating in Country X and also in Australia to collect intelligence on Australian citizens. It would be difficult for Australia to make a principled request to Country X's agency to cease and desist with such activity, given the presence of similar powers within Australia.

[9] We note that the purpose of "protecting the public revenue", which was present in the exposure draft of the Bill, has been omitted in the version of the Bill that was introduced to the House of Representatives on 20 September 2018.

potential criminal or security threats within Australia, including activities in relation to intelligence collection, national defense, or foreign relations that could make private sector entities complicit in adversarial actions against another nation-state. By seeking to force Providers to assist in such activities, the Government could undermine Providers' hard-won reputations for integrity and neutrality in the global marketplace, ultimately compromising the integrity of the digital economy.

Moreover, and as mentioned earlier, the Bill, and the unprecedented authorities it confers, would set a worrying precedent that other governments, including non-democratic or authoritarian governments, may look to in establishing counterpart laws.

BSA recommends that the scope of circumstances be narrowed substantially. This would include limiting the list of purposes for which TARs, TANs, and TCNs can be issued to:

- preventing or detecting serious crime; and
- protecting against an identified threat to national security under a narrowly defined set of circumstances, such as preventing an imminent national security threat to Australia and its citizens.

4. ***The application to "designated communications providers" should be limited, both in terms of extraterritorial effect and in terms of the types of organizations that are subject to the Bill***

The Bill, as currently drafted, outlines a list of "designated communications providers" that would impact not only those Providers directly providing communications services in Australia, but also organizations operating outside of Australia and/or occupying roles in the supply chain that may be separated by several degrees from the direct Providers themselves. BSA notes that this could include organizations with virtually no control over the final product or service and virtually no link to Australia. This also raises concerns of conflicts of laws as foreign organizations may be required under a TAN or TCN to perform acts or things that are inconsistent with laws to which they are subject.

BSA recommends that the extraterritorial application of the Bill should be limited by reference to an active targeting of Australia, and that supply chain implications should be addressed by expressly carving out organizations that do not exercise control over the final product or service.

Example of issue that could arise under the current Bill:

An agency may require a Provider, under Schedule 5 of the Bill (which attracts criminal penalties for non-compliance), to provide assistance to access sensitive personal data of EU citizens that the Provider stores in its servers in Australia. Providing access to such data may result in the breach of the Provider's obligations under the EU's General Data Protection Regulation (**GDPR**), especially with respect to those special categories of personal data under Article 9 of the EU GDPR, where no clear exception exists for the disclosure of such personal data on account of a legal obligation imposed on the Provider in another jurisdiction. However, the Provider does not have a defense under the Bill for not complying with the requirement of the Agency, leaving the Provider in a position of conflict of having to choose between being in breach of the GDPR, and exposed to significant fines in EU, or face criminal penalties under the provisions of the Bill.

BSA also recommends that the principle, called out in the explanatory memorandum accompanying the Bill (**Explanatory Memorandum**)[10] but remaining unaddressed in the Bill itself – that the organization must be the most appropriate organization to provide the assistance – should be an explicit requirement for issuing a notice under the Bill.

[10] See paragraphs 131 and 175 of the Notes to Clauses of the Explanatory Memorandum (on pages 49 and 56, respectively).

Finally, BSA notes that there are new provisions in the Bill that provide Providers a defense against *civil* penalties for non-compliance with a TAN or TCN, where compliance with the TAN or TCN in a foreign jurisdiction will result in the Provider breaching the laws of that jurisdiction. **BSA recommends** that this defense should be extended to:

- non-compliance with a TAN or TCN in respect of activities *within Australia* that will result in a similar breach of the foreign jurisdiction's laws;

- non-compliance with a provision contemplated under Schedules 2 through 5 of the Bill, in respect of activities in foreign jurisdictions as well as within Australia; and

- *criminal* penalties that the Provider may be exposed to in Australia due to non-compliance with any provision of the Bill where compliance will result in a breach of another jurisdiction's laws.

5. ***Any technical information disclosed by Providers should be protected by the relevant agencies***

The technical information, such as source code, held by BSA's members constitutes one of their most valuable assets. Although the Bill includes limited non-disclosure responsibilities, it does very little to address concerns about the way in which the technical information will be protected and used. This exposes organizations to a risk of misuse or inadvertent disclosure, as well as having the potential to introduce a systemic weakness merely because the information is not properly protected.

Additionally, other jurisdictions who may decide to implement similar measures, but who do not have similarly robust or effective protection mechanisms against disclosure of sensitive technical information, could make similar requests for disclosure, putting those organizations at significant risk.

Example of issue that could arise under the current Bill:

An agency may issue a TAN to compel a Provider to hand over sensitive technical information for examination by the agency. The technical information is proprietary and sensitive as it relates to an innovative aspect of the Provider's service that provides the Provider a competitive edge. Minimal security measures are taken in respect of the information obtained, resulting in a bad actor obtaining access to the information. The bad actor releases the information publicly.

Leaving aside the issue of whether the agency in question might have breached its non-disclosure obligations under the Bill, the public disclosure of the sensitive technical information could cause significant losses to the Provider.

BSA recommends that:

- the Bill should include additional protections in respect of the use and protection of technical information, such as a purpose limitation, obligations to impose appropriate security measures, and limitations on retention periods; and

- technical information that Providers may be compelled to disclose should be limited to information that is public or commonly shared under commercial NDA arrangements, and Providers should not be forced to reveal their sensitive intellectual property, including source code.

6. ***The new computer access warrants regime should include the same limitations and safeguards as the assistance and access regime***

BSA notes that the definition of "specified persons" is very broad, with very few safeguards.

BSA recommends that:

- the concerns and recommendations on the assistance and access regime, such as those regarding technical feasibility, reasonableness, and proportionality, should flow through into the computer access warrants regime; and
- law enforcement should be required to minimize interference with data or equipment and, to the extent this is unavoidable, to reimburse organizations for all losses suffered as a result of damage or destruction.

Example of issue that could arise under the current Bill:

An agency suspects that a person has information on his personal device that connects to a corporate network. Due to the broad definition of "specified persons", the agency chooses to ask a system administrator of the corporate network to help in accessing the information instead of requesting the information directly from the person in question. The system administrator is inexperienced and unable to help, but is unable to convince the agency of this. The agency considers the system administrator to be in breach of the warrant and initiates criminal prosecution.

D. Further Details on Specific Comments and Recommendations

Issue	Reference[11]	Description of issue	BSA Recommendations
1. Process, oversight and review	Sections 317L, 317P, 317RA, 317T, 317V, 317W, 317ZAA, and 317ZK Schedule 1 of the Bill, section 1 (Amendment to the *Administrative Decisions (Judicial Review) Act 1977*)	• A large number of decision-makers can issue notices under the Bill. They can do so with limited judicial oversight and based on evidence that may be unknown to the Provider who receives the notice. • The decision-maker must not give a notice unless he/she is satisfied that the requirements are reasonable and proportionate, and that compliance is practicable and technically feasible. However, this assessment is based on the decision-maker's *subjective* satisfaction rather than any *objective* measures. The decision-maker may not understand, or be best placed to assess, the impact of a notice on the recipient organization, including the costs of compliance, impact on customers, and broader issues of security, privacy, and intellectual property. • While the Explanatory Memorandum explains that agencies are expected to engage in a dialogue with the Provider before issuing a notice,[12] the Bill itself	• The decision to issue a notice should be made by an independent judicial authority (for example, the categories of eligible judges and nominated Administrative Appeals Tribunal members who have authority to issue interception warrants under the *Telecommunications (Interception and Access) Act 1979*), based on evidence submitted by the requesting agency regarding the *necessity* of issuing a notice, in addition to the reasonableness, proportionality, practicality, and feasibility of the proposed "acts or things" and the consistency of the proposed notice with the underlying warrant. • The requirement for "dialogue" prior to issuing notices, as referred to in the Explanatory Memorandum, should be reflected within the Bill itself. This dialogue should happen before the agency submits evidence to the (recommended) independent judicial authority in order to issue a notice, and should consider both the *necessity* of

[11] References are to the sections in the *Telecommunications Act 1997* proposed to be inserted or amended by the Bill, unless otherwise specified.

[12] See paragraphs 132 and 176 of the Notes to Clauses of the Explanatory Memorandum (on pages 49 and 56, respectively).

Issue	Reference[11]	Description of issue	BSA Recommendations
		does not mandate any dialogue but, in relation to TCNs only, simply requires the Attorney-General to provide a notice and *consider* any submission made by the Provider and an optional assessment report jointly commissioned (under section 317W(7)) by the Attorney-General and the Provider at the cost of the Provider (unless the Attorney-General agrees to reimburse part or all of the cost). • In relation to the optional assessment mentioned above, the Bill requires the assessment to be completed and submitted to the Attorney-General within a consultation period specified by the Attorney-General. It may not be practicable for the assessment to be completed (or possibly even commenced) within this period if the Attorney-General keeps to the minimum specified period of 28 days, especially if the Attorney-General and the Provider are unable to arrive at a decision over the appointment of the joint assessor. • Further, a decision to issue a TAN or TCN is not subject to merits review or any other mechanism that allows Providers to challenge the issuing of such a notice. There is also very limited recourse that Provides will have to judicial review. While this is consistent with other legislation in Australia governing national security and law enforcement, the purposes for which TANs and TCNs can be issued, and the "listed acts or things" that may be required, are much broader than any legislative precedent (see items 2 and 3 below). • While the Bill allows the parties to agree on the *terms and conditions* on which the Provider must comply with a TAN or TCN as part of a process that can culminate in arbitration, this does not formally extend to whether the decision-maker should have issued the notice in the first place, or whether the Provider should be required to comply with it. Further, the arbitrator him/herself is to be appointed by the Attorney-General,	issuing the notice as well as the assistance to be provided under the notice. Further, the assessment report should be commissioned by default and through a fair and transparent process to address the appointment of the assessor without undue delay, unless both parties agree to waive the requirement for an assessment report, with the costs of the assessment borne by the Australian Government on the principle of cost-causality. All the foregoing should supplement the existing proposed regime for issuing TANs, as well as replace the limited consultation regime for TCNs in the currently-drafted section 317W. • Sections 317RA and 317ZAA[13] now require the decision-maker to consider both the interests of the requesting agency and the interests of the Provider, as well as various other factors, prior to issuing a TAN or TCN. However these sections should also expressly require the consideration of other factors that were called out in the previous Explanatory Document,[14] such as: the likely benefits of an investigation; the potential business impact on the Provider; whether the Provider to whom the notice is to be issued is the most appropriate party to provide the assistance (see also item 4 below); and the potential impact on third parties. • The Bill should include a procedure to allow the Provider to challenge a notice on its merits, including the necessity, reasonableness, proportionality, practicality, and feasibility of complying with the notice. This would also include the ability to request a review of the decision to issue the notice based on any new evidence that arises after the decision is made. At the minimum, the Bill should not exclude proposed Part 15 of the *Telecommunications Act 1997* (i.e., the proposed provisions governing the issuance of TARs, TANs, and TCNs) from the scope of the *Administrative Decisions (Judicial Review) Act* so as to afford affected Providers full and proper recourse to judicial review in respect of executive decisions taken under the

[13] Sections 317RA and 317ZAA were previously not included in the exposure draft of the Bill.

[14] The Explanatory Document issued in August 2018 and accompanying the exposure draft of the Bill; at pages 34 and 37.

Issue	Reference[11]	Description of issue	BSA Recommendations
		giving rise to a potential conflict of interest. • The "no cost, no profit" rule only applies to reasonable out-of-pocket costs and is likely to leave Providers bearing substantial costs themselves.	proposed Part 15 of the *Telecommunications Act 1997*. • To address conflict of interest concerns, the arbitrator under section 317ZK should be appointed by one or more independent third parties, not the Attorney-General. • Providers should be entitled to recover the *actual costs of compliance* with a notice. In particular, the Bill should make clear that "costs" include not only third-party out-of-pocket expenditure, but also other costs, such as costs arising from the termination of customer relationships that result from compliance with a notice, and overhead costs. For example, if a Provider is required to comply with a TCN to develop a new functionality, this will likely require a reallocation of internal technical resources and this carries an overhead cost that should be reimbursed.
2. Scope of "listed acts or things"	Sections 317E, 317L, 317P, 317T, 317V, 317ZF, 317ZG	• The "listed acts and things" that could be required of Providers through TANs and TCNs are overly broad, non-exhaustive, and, amongst other things, could require them to: o decrypt communications; o install government spyware on their systems; o develop a new technology or capability; o modify any characteristic of a service; o replace portions of their service with a service provided by another party; and o conceal any such acts or things. • This list goes far beyond any set of prescriptive requirements under any Australian law and, to our knowledge, any other law internationally. It effectively requires the Provider to do virtually anything that the requesting agency requires, including measures that could undermine trust in a business or adversely impact cybersecurity. • This list is also not exhaustive in relation to TARs and TANs. A non-exhaustive list creates an untenable grey area because Providers cannot reasonably plan or resource for the acts or things they may be required to perform.	• A Provider to whom a notice is issued should only be required to comply to the extent that it is objectively practical, technically feasible, reasonable, and proportionate. This should not be a subjective assessment made by the decision-maker (as set out in sections 317P and 317V). • The distinction between when a TAN or a TCN is used should be clarified within the wording of the Bill itself and not just in the Explanatory Memorandum. The acts and things that can be specified in a TAN (and the Provider's obligation to comply with the TAN) should be limited to those forms of assistance that the relevant Provider is *capable* of giving. There should also be a further definition of "capability" to clarify that it must be reasonably practicable, taking into account, amongst other things, the Provider's existing system configuration and the resources reasonably available to the Provider. Further, the Bill should include provisions stipulating when law enforcement must rely on a TCN instead of a TAN. • The listed acts and things should be an exhaustive list, not just in relation to the "listed help" required under a TCN. It is not appropriate to request Providers to

Issue	Reference[11]	Description of issue	BSA Recommendations
		• The decision-making criteria that the requirements must be "reasonable and proportionate" and that compliance with the notice must be "practicable and technically feasible" is not adequately clear and consequently gives the decision-maker very broad discretion, which is inappropriate given that the decision-maker may not have all the information, knowledge, and experience necessary to make an informed decision. • The distinction between a TAN and a TCN is unclear. The Explanatory Memorandum provides that the "acts or things specified in a [TAN] will be limited to forms of assistance a [P]rovider is already capable of giving", and gives the example that a TAN "may require a [P]rovider to assist with the decryption of material lawfully intercepted under a warrant if their systems enable them to decrypt this material" and could not "require a provider to build a new decryption capability".[15] However, this is not reflected in the wording of the Bill itself. Without diminishing concerns regarding the compromise to privacy and security, a Provider may, for example, be technically capable of building a decryption capability which does not currently exist in its systems, but does not have the resources to do so and significant compromise to its systems; and as drafted, there is nothing in the Bill proscribing the ability of the decision-maker to use a TAN to require the Provider to build such a capability. • There are also no provisions in the Bill specifying when law enforcement *must* rely on a TCN instead of a TAN to compel a Provider to do an act or thing. As the Bill is currently drafted, a Provider could be required to do the same acts and things whether under a TAN or a TCN. In fact, the list of acts of things that a Provider can be required to do under a TAN is potentially *broader* (as section 317T(4)(c) purports to exclude acts or things under section 317E(1)(a) from the scope of TCNs), whereas there is no similar limitation in respect of TANs). This is especially concerning when considering the relatively fewer checks and balances that currently exist in the	perform acts or things that go beyond this already very broad list. Additionally, the requirement to "conceal any such acts or things" should be confined to concealing that a particular law enforcement activity is in process, rather than the fact that a technical capability or thing exists as a result of a TAN or TCN. As with lawful interception capabilities today, capabilities developed as a result of a TAN or TCN should be publicly documented; any other approach represents creating undocumented backdoors. Further, Providers should not be compelled to reveal details of vulnerabilities which have not yet been patched and a transparent policy for vulnerability handling, and we encourage the Government to develop and include in the Bill a clearly articulated policy describing how it will handle vulnerabilities and what processes it will use to govern timely disclosure of that information to actors capable of fixing them. Finally, and most importantly, there should be an overarching condition that any requirements imposed on Providers are the *minimum necessary* required for the relevant objective. • The Bill should provide more clarity in relation to what is required under each listed act or thing. This should consist of a narrower scope in relation to each item, and guidance as to what is and is not required. In particular: o sub-section (1)(a): the requirement to remove electronic protection should be qualified to the extent that it would not create a risk of destroying, corrupting, or disrupting any hardware, software, or data; o sub-section (1)(b): the requirement to provide "technical information" should define the types of information to be provided and expressly carve out certain types of information such as source code and network diagrams; o sub-section (1)(c): the requirement to install, maintain, test, or use software or equipment (including installing software or hardware provided by an agency) is too broad and could have a serious impact on security – this should be limited to software or hardware that has been

[15] See paragraph 117 of the Notes to Clauses of the Explanatory Memorandum (on page 47).

Issue	Reference[11]	Description of issue	BSA Recommendations
		Bill in respect of TANs as compared to TCN, and the correspondingly natural disincentive for law enforcement to use TCNs. • Providers are prevented under section 317ZF from disclosing information relating to TARs, TANs, and TCNs, including the issuance or existence of such notices or requests, with section 317ZF(13) permitting a Provider to disclose only aggregated numbers on the total number of TARs, TANs, or TANs received during a reporting period that is not less than 6 months. The lack of greater information available to the public could undermine consumer trust in not only the Providers' services, but also in the use of modern technology in general. While a new section 317ZFA has been introduced which allow the courts greater powers over, among other things, the disclosure of information, are no provisions which confer authority on the issuer of the TAR, TAN, or TCN, in the first instance, to permit more transparent reporting by the Provider. • The prohibition against building backdoors is very limited. It only prohibits building in *systemic* weaknesses or vulnerabilities into forms of *electronic protection* (i.e., encryption). The likelihood is that carrying out any of the listed acts or things has the potential, in some circumstances, to introduce a systemic weakness, not only in the context of electronic protection. For example, a notice could require a Provider to install software provided by an agency (under section 317E(1)(c)), which allows the agency to access data hosted on the Provider's technology platform – this would not be prevented by section 317ZG as it does not require the provider to implement a systemic weakness into a form of electronic protection; however, it may nonetheless create serious security weaknesses by enabling access to data.	independently certified to meet at least the same levels of security that the host system meets and should not impact the system's performance or availability; o sub-section (1)(d): the requirement to provide information in a particular format should be subject to a qualification that the format is secure; o sub-section (1)(f): the requirement to assist with testing, modification, development, or maintenance of a technology or capability is extremely broad and potentially very onerous – if law enforcement wishes to develop technology, it should not be entitled to lean on technology organizations to perform the development for them; and this requirement should accordingly be limited to integration rather than developing entirely new functionality; o sub-section (1)(g): the requirement to notify relevant updates to the Provider's services or activities should be further clarified and narrowed to take into account products increasingly being delivered over the cloud (including software-as-a-service) where potentially relevant product improvements and updates (including patches to close security vulnerabilities) are delivered frequently and sometimes urgently, and where a notification requirement, in light of these practices, would be unduly burdensome and could significantly slow product development and time-to-market, and also compromise security; o sub-sections (1)(h) and (1)(i): the requirements to modify the characteristics of a service or substitute a service are too broad and unclear, and could potentially compel a Provider to modify or substitute a service to store a secret, unencrypted copy of data, or enable authorities to sight what the end user sees on a screen; and in absence of clear guiding criteria on what modifications or substitutions the authorities may require, these sub-sections should be removed; and o sub-section (1)(j): the requirement to conceal certain actions should be removed (along with the related sub-section (2)) as it is unclear when there would be a situation where a Provider

Issue	Reference[11]	Description of issue	BSA Recommendations
			can comply without making false or misleading statements or engaging in dishonest conduct. • The Bill should require that each time a TAR, TAN, or TCN is issued, the issuer will need to carefully evaluate, in consultation with the relevant Provider, the need for secrecy, and (if secrecy is required) the duration of secrecy that would need to be applied; and the Bill should accordingly grant the issuer of the TAR, TAN, or TCN, the authority to determine the appropriate level and duration of secrecy to be required for each case, including dispensing with the need for secrecy in appropriate cases. The Bill should also include a review process to allow Providers the ability to request the issuer of the TAR, TAN, or TCN for reconsideration of the need for secrecy (e.g., due to a change in circumstances). • A notice should have no effect to the extent it requires a Provider to implement *any weakness or vulnerability* (i.e., not just systemic weaknesses or vulnerabilities) in *any system, product, service, or component,* including devices, facilities, hardware, and equipment (i.e., not just a weakness in forms of electronic protection, such as encryption). • Alternatively, if the reference to "systemic" is to remain, the Bill should include a clear definition of "systemic" which not only includes wholesale weakening of security on a range of services, devices, or software, but extends to *any* weakening or vulnerability (even on a single system) which *could* cause weakening or vulnerability to security on a larger scale.
3. Circumstances in which powers can be exercised	Sections 317G, 317L, 317T	• The purposes for which a request or notice can be issued are overly broad. These purposes include enforcing criminal law and laws imposing pecuniary penalties, assisting the enforcement of criminal laws in force in a foreign country, safeguarding national security and, for TARs, the interests of Australia's foreign relations or national economic well-being. They can also include "a matter that facilitates, or is ancillary or incidental to", any of the	• The purposes for which a request or notice can be issued should be limited to the following matters: o the purpose of preventing or detecting *serious* crime (i.e., the Bill should include qualifiers for "seriousness" and "preventing or detecting", consistent with, for example, the requirements under the UK Investigatory Powers Act); and o the purpose of protecting against an identified threat to national security

Issue	Reference[11]	Description of issue	BSA Recommendations
		relevant objectives, which further broadens the scope. • It is unclear why the exceptional authorities to issue TANs or TCNs should extend to the enforcement of laws imposing pecuniary penalties, which would include laws imposing fines in respect of minor offences such as vehicle parking violations. • Additionally, TANs and TCNs requiring that Providers assist elements of Australia's national security apparatus for an undefined national security purpose, without limitation on the set of circumstances for seeking such assistance, could lead to requiring private sector organizations to act – or be perceived as acting – in complicity with adversarial security actions taken by the Australian Government in relation to foreign nations, or in actions impacting bilateral trade relations. Such perceptions could pose severe risks to such organizations' ability to compete in foreign markets. • While these purposes are consistent with those for which agencies can seek assistance under section 313 of the *Telecommunications Act 1997*, the application of the *Telecommunications Act 1997* is limited to carriers and carriage service providers, and does not extend to the broad range of "designated communications providers" to which the Bill applies (see item 4 below). Furthermore, the "listed acts or things" under the Bill (see item 2 above) go far beyond anything in the *Telecommunications Act 1997*. • While this is tempered somewhat by a provision that limits applicability in cases where the required act or thing would require a warrant or authorization under certain listed statutes, the principle that organizations should be required to perform the "listed acts or things" to achieve such broadly-defined and vague objectives sets a troubling precedent and goes beyond even the UK Investigatory Powers Act.	under a narrowly defined set of circumstances, such as preventing an imminent national security threat to Australia and its citizens. • All other "relevant objectives" should be removed, even in the case of voluntary TARs, as including them within such requests suggests that it is reasonable for the government to request support (even on a voluntary basis) in the context of these broadly-defined objectives, which is objectionable as a principle. • The broad catch-all for "a matter that facilitates, or is ancillary to, or incidental to" should also be removed as this could potentially present a justification in a range of very loosely-related scenarios, as determined by the decision-maker. • In addition to the decision-maker being satisfied that issuing a notice is necessary in the first place (see item 1 above), the "listed acts or things" in the notice should themselves be *necessary.*[16] The purposes should not simply be "objectives" of requesting or requiring the "listed act or thing".

[16] This would be consistent with, for example, the UK Investigatory Powers Act provisions.

Issue	Reference[11]	Description of issue	BSA Recommendations
4. Broad application to "designated communications providers" and extraterritorial effect	Section 317C Schedules 2 through 5 of the Bill (in relation to assistance that that Providers may be required to provide under the provisions contemplated in these Schedules)	• The definition of "designated communications provider" is so broad as to have the potential to capture most of the global technology supply chain, including organizations that have virtually no link to Australia. These could include, amongst others: o electronic service providers with one or more end users in Australia (i.e., potentially those having any website that does not geoblock Australia); o manufacturers of components that are "likely to be used in Australia" (even if the manufacturer does not control where those components are ultimately used); and o organizations that develop, supply, or update software that can be installed on equipment that is "likely to be connected to a telecommunications network in Australia" (again, even if the software developer does not specifically target Australia). • The Bill applies to the full range of participants in the supply chain, including hardware manufacturers, over-the-top messaging service providers, and cloud services providers, even where those participants may have little or no control over: (a) how their components or services are ultimately used (including whether they are used in Australia); or (b) the data that is processed using their components or systems (which may be owned and controlled by the organization's customer or other parties much further down the supply chain). • The Bill gives rise to a conflict of laws issue because it is so broad as to require an organization with operations or customers in one or more foreign jurisdictions to perform acts or things that may be inconsistent with laws to which the organization is subject. In those situations, the organization would have to choose which law to comply with, and which law to breach. While there is a new section 317ZB(5) which provides Providers a defense against *civil* penalties for non-compliance with a TAN or TCN, where compliance with the TAN or TCN in a foreign jurisdiction will result in the Provider breaching the laws of that jurisdiction, this defense does not	• The extraterritorial application of the Bill to "designated communications providers" should be limited to organizations that actively and directly target or offer their goods or services to persons or organizations in Australia. Mere availability (or likelihood of availability) of a product or service in Australia in the absence of active targeting should be expressly carved out. The approach taken by the EU's GDPR, albeit in the context of a different subject matter, is a useful benchmark, because (via the wording of the regulation and the associated recitals) the GDPR is clear that there has to be some level of *targeting* – simply being available in a country does not mean that the organization is actively doing business in that country. • The following items should be removed from the definition of "designated communications providers" because the focus should be on the primary service provider or manufacturer, not the entire supply chain: o item 8 (manufacturers / suppliers of components for use in telecommunications facilities); o item 10 (manufacturers / suppliers of customer equipment); o item 11 (manufacturers / suppliers of components for use in customer equipment); o item 14 (manufacturers / suppliers / installers / maintenance providers of data processing devices); and o item 15 (software developers / suppliers / updaters). • There should be an express requirement that the organization that is the subject of the notice is the *most appropriate* organization to provide the assistance sought. This principle is referenced in the Explanatory Memorandum[17] but does not appear in the Bill. This should be captured within the Bill itself and should be a requirement for issuing a notice and not only a consideration. Further, as part of the recipient's right to challenge, as proposed in item 1 above, the recipient should be entitled to challenge whether it is indeed the most appropriate organization to provide the

[17] See paragraphs 131 and 175 of the Notes to Clauses of the Explanatory Memorandum (on pages 49 and 56, respectively).

Issue	Reference[11]	Description of issue	BSA Recommendations
		extend to the situation where the Provider's compliance with: (a) a TAN or TCN in respect of activities *within Australia*; or (b) a requirement imposed under a provision in Schedules 2 through 5 of the Bill, in respect of activities in foreign jurisdictions and/or within Australia, will result in a similar breach of the foreign jurisdiction's laws; or to *criminal* penalties to which the Provider may be exposed under the Bill.	requested assistance and to refer to the agency to another organization who may be better placed to provide the assistance. • The Bill should address the conflict of laws issue by stating that Providers will have a defense against both civil and criminal penalties for non-compliance with a requirement imposed under the Bill, where compliance with that requirement (whether within or outside Australia) would expose the Provider to liability under any other laws or regulations to which it is subject.
5. Unauthorized disclosure of information	Section 317ZF Schedules 2 through 5 of the Bill (in relation to assistance that that Providers may be required to provide under the provisions contemplated in these Schedules)	• The requirement under section 317E(1)(b) to "provide technical information" is broad and may require Providers to hand over commercially-sensitive information, even if the categories of information required are limited as recommended at item 2 above. • This exposes Providers to substantial risks and these are not adequately addressed by the Bill. For example: o the Bill does not limit the purposes for which the technical information can be used; o the Bill does not require that the technical information be protected by appropriate security measures; o the exceptions to the offence for disclosing information in relation to a TAR, TAN, or TCN are too broad (e.g., in connection with the performance of functions or exercise of powers by certain government agencies, which could cover virtually any disclosure by the relevant government agencies); o the Bill does not impose any requirement to minimize the volume of technical information requested; o the Bill does not impose time limits on the duration for which the technical information can be retained; and o the Bill does not include safeguards to prevent indirect sharing of commercially-sensitive information with the Provider's competitors. • Further, if the information is not properly protected, simply handing over this information has the potential to create a systemic weakness.	• The Bill should include a purpose limitation on the use of information – i.e., the purpose for which technical information (or other information disclosed in accordance with a TAR, TAN, TCN, or any other provision of the Bill) can be used should be expressly limited to the purposes for which such information was obtained (see item 3 above regarding "relevant objectives"). • Information disclosed under the Bill should always be kept confidential other than with consent from the relevant provider of the information. There should also be a commitment to protect the information using appropriate security measures. • Only information which is public or commonly shared under non-disclosure agreements should be requested. Other more sensitive organizational information should be excluded from this requirement. • The exceptions to the disclosure offence should be substantially narrowed and should be subject to the original purpose limitation. • Any disclosure, even within an agency, should be on a strict need-to-know basis linked to the relevant purpose limitation. • There should be a data minimization requirement – i.e., the Provider should only need to provide the minimum information required for the relevant purpose.

Issue	Reference[11]	Description of issue	BSA Recommendations
		• Similarly, when requesting information under the other provisions in the Bill, there are only limited circumstances in which an order can be obtained in a proceeding to restrict the disclosure of information about computer access technologies or other commercially-sensitive information.	• Information should only be retained for so long as is necessary for the relevant purpose and there should be an express requirement for secure deletion or destruction of the information when that time period expires. • In line with the "no cost" principle, there should be dollar for dollar recovery if the Provider suffers any loss in connection with it providing the technical information, including loss suffered as a result of a breach of the obligations on use and disclosure of the information.
6. Assistance relating to computer access warrants	Schedule 2 to the Bill: section 64A of the SDA See also Schedules 3 to 5 to the Bill, setting out amendments to the *Australian Security Intelligence Organisation Act 1979* ("**ASIO Act**"), *Crimes Act 1914* ("**Crimes Act**") and *Customs Act 1901* ("**Customs Act**")	• The definition of "specified persons" who may be required to provide information and assistance is very broad and includes: o a person engaged under a contract for services by the owner / lessee of the computer; and o a person who is or was a system administrator for the system including the computer or device, and who has relevant knowledge of the computer or network that the computer forms part of, or the measures applied to protect data held in the computer. This is so broad that it could potentially apply to all app and software developers and platforms simply because the owner of a computer has downloaded an app or software. • Further, law enforcement officers are not required to minimize interference with data or equipment when executing a warrant. Executing officers are allowed to damage or destroy data or equipment to conceal actions taken under a warrant.	• This regime should be adjusted in line with the proposed amendments set out above in relation to Schedule 1 of the Bill. In particular: o there should be an express requirement that the specified person is the most appropriate person to provide the information or assistance sought (e.g., a system administrator should not be asked for passwords to unlock a computer); o assistance or information should only need to be provided to the extent it is it is practical and technically feasible, reasonable and proportionate; and o the specified person should only be asked to provide assistance or information if the specified person is *capable* of doing so (rather than having "relevant knowledge"). • Further, the Bill should, in relation to any requirement imposed on a specified person to provide assistance or information: o introduce an immunity that releases a specified person from any criminal or civil liability for, or in relation to, any act or thing the specified person does in compliance (or in good faith in purported compliance) in providing such assistance or information; and o provide for reimbursement of *all costs* incurred by a specified person associated with providing such assistance or information (in line with recommendation relating to costs as set out in item 1 above). • Law enforcement officers should be under an express obligation to minimize interference with data or equipment when executing a warrant and, to the

Issue	Reference[11]	Description of issue	BSA Recommendations
			extent such interference is unavoidable, the Australian Government should reimburse the organization (and any affected individuals) for all losses the organization suffers as a result. • Associated amendments should also be made to the computer access warrant regime under the ASIO Act, Crimes Act and the Customs Act, where relevant.

E. Conclusion and Next Steps

Given the complexity of the Bill, the sensitivity of the subject matter, and the limited consultation period, the summary above is not an exhaustive list of BSA's concerns and recommendations in respect of the Bill. There are other aspects of the Bill that require further consideration in order to find the right balance between the legitimate rights, needs, and responsibilities of the Australian Government, citizens, providers of critical infrastructure, third party stewards of data, and innovators.

As such, we respectfully encourage the Australian Government to engage in further dialogue with industry to consider the broader issues at play and the implications (and possible unintended consequences) of the Bill.

BSA and our members remain at the disposal of the Australian Government to participate in any industry and stakeholder groups, not only to assess the impact of the Bill, but also to help develop and deliver other enduring solutions to address the challenges of accessing evidence in the digital age.

If you require any clarification or further information in respect of this submission, please contact the undersigned at darrynl@bsa.org or +65 6292 0680.

Yours faithfully,

Darryn Lim
Director, Policy – APAC