10 September 2018

Australian Government
Department of Home Affairs
By email to: [redacted]

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

A. Statement of Interest

BSA | The Software Alliance (**BSA**) is the leading advocate for the global software industry before governments and in the international marketplace. BSA members are at the forefront of data-driven innovation, including cutting-edge advancements in data analytics, machine learning, and the Internet of Things.[1]

Our members 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**), which we understand is designed to enhance assistance from the communications industry and better enable law enforcement authorities to investigate criminal and terrorist activities in the digital era.

B. Introduction

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. At the same time, we must note that the debate over this legislation should not devolve into a false choice between privacy and security. Strong encryption is a powerful enabler of not only personal liberty and privacy, but also for security and safety of communications and transmissions relied upon the delivery of critical functions, e.g., water filtration, electricity distribution, transportation systems, and financial services. They all rely on the power of software developed and secured by our members further underscoring the interest of BSA in ensuring that this legislation is successful in improving law enforcement capacity to investigate serious crimes without compromising cybersecurity and other priorities.

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

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.

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 agencies in Australia and 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.

In our experience, the needs of law enforcement, technology providers, and the consumers whose privacy interests are at stake, are best met by governments that have a robust mechanism for judicial oversight, transparency of activities, privacy protections, and clearly defined processes for bidirectional communication on law enforcement needs. In addition, as data is stored by global organizations subject to privacy laws in different countries, it is increasingly important that laws for government access be interoperable.

Deepening collaboration between private industry and law enforcement based on these principles can generate practical and impactful solutions to the challenges facing law enforcement. BSA therefore welcomes the opportunity to bring an industry perspective on the Bill and strongly urges continued engagement 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.

Addressing challenges associated with law enforcement's access to digital evidence is not an issue that is unique to Australia. BSA has been involved in discussions with governments, policy-makers, and industry bodies around the world for several years on efforts to facilitate law enforcement access to communications in a way that balances the associated concerns. Building on these discussions, BSA is pleased to offer the recommendations below in response to the draft Bill.

C. Summary of 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 I to request or compel assistance from technology organizations in accessing electronic communications information; namely, the authorities to issue voluntary technical assistance requests (**TARs**) and mandatory technical assistance notices (**TANs**) or technical capability notices (**TCNs**). These extraordinary new authorities are of unprecedented scope and application.

While BSA recognizes that the Australian Government has sought to build certain safeguards into the Bill, such as ensuring that providers are not required to implement "back doors" or to build systemic weaknesses

into forms of electronic protection, BSA is concerned that the safeguards do not go far enough to protect principles such as privacy, cybersecurity, and trust in the digital economy.

BSA's comments and recommendations are set out in further detail in Section D of this submission. Here is a summary of these comments and recommendations:

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 limited judicial oversight, based on evidence that may be unknown to the designated communications provider (**Provider**), and a subjective assessment of reasonableness and proportionality. 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 was appropriate for the notice to be issued in the first place.

   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. The regime should also allow the Provider to challenge the issuing of the notice, as well as its scope and terms. While we have significant concerns with 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*". In line with this, it would be essential that a robust judicial oversight and challenge mechanism that provides for full and transparent due process be incorporated into the Bill.

   Additionally, recognizing that once legislation is passed in Australia, similar legislation could be reasonably expected to be enacted by all governments worldwide, whether based on democratic values or not, BSA urges Australia to make all efforts to encourage the adoption of requirements for judicial authorization and other safeguards through appropriate global bodies and communities.

2. ***The "acts or things" that can be required from a Provider should be narrowed and any list should be exhaustive; 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. 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. For example, the "acts or things" envisioned in the Bill could force the removal of electronic protections applied for cybersecurity purposes, mandate the installation of untested software that could inadvertently introduce new systemic vulnerabilities, undermine trust in processes for automatic security updates, or compel the disclosure of vulnerabilities that are unknown to the technology vendor and have therefore not yet been patched, and which could be exploited by bad actors having access to such information. 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.

   BSA therefore 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 vulnerability handling and disclosure for 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) protecting the public revenue; or (d) safeguarding national security." 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. The principle that organizations could be required to engage in these "acts or things" to support purposes that go far beyond preventing or detecting serious crime or protecting against identified threats to national security under certain narrowly defined circumstances sets a troubling precedent, and BSA recommends that the scope of circumstances be narrowed substantially.

Two objectives are especially concerning, both because they extend far beyond law enforcement purposes and because they remain vague and undefined: "protecting the public revenue" and "safeguarding national security." Particularly in light of the absence of robust judicial oversight, these authorities could empower Government decision-makers to require Providers to take actions beyond addressing potential criminal or security threats to 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. In addition to the ramifications that participating in such activities may create for global businesses operating in markets outside of Australia, the authorities would set a troubling precedent that other governments, including non-democratic or authoritarian governments, may look to in establishing counterpart laws.

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 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. Further, BSA recommends that the principle, called out in the Explanatory Document but not addressed in the Bill – 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. Finally, BSA recommends that the Bill include a new section to address the conflict of laws issues that arise from requiring organizations to comply with TANs and/or

TCNs that would put them in breach of laws and regulations in other jurisdictions to which they are subject.

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.

BSA therefore recommends that the Bill 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. Further, 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 regarding technical feasibility, reasonableness, and proportionality, should flow through into the computer access warrants regime. Further, 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.

D. Key Issues and Recommendations

Issue	Reference[2]	Description of issue	BSA Recommendations
1. Process, oversight and review	Sections 317L, 317P, 317T and 317V; Division 5; Section 317ZK Schedule 1 to 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.	• 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 Document, should be reflected within the Bill itself. This dialogue

[2] References are to the section in the amended *Telecommunications Act 1997*, unless otherwise specified.

Issue	Reference[2]	Description of issue	BSA Recommendations
		• While the Explanatory Document explains that agencies are expected to engage in a dialogue with the Provider before issuing a notice, the Bill itself 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. • 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. 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, 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.	should happen before the agency submits evidence to the independent judicial authority in order to issue a notice and should consider both the *necessity* of issuing the notice as well as the assistance to be provided under the notice. This should replace the limited consultation regime for TCNs in section 317W. • The Bill should expressly require that the independent judicial authority consider both the interests of the requesting agency and the interests of the Provider, including with regard to the factors set out in the Explanatory Document (such as the objectives of the agency, the availability of other means to achieve those objectives, the likely benefits of an investigation and the potential business impact on the organization). The judicial authority should also be required to consider whether the Provider is the most appropriate party to provide the assistance (see item 4 below) and wider public interests including the impact on privacy, cybersecurity, and any third parties. • The Bill should include a procedure to allow the Provider to challenge 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. • To address conflict of interest concerns, the arbitrator 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" are not limited to third party, out-of-pocket expenditure, but include 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.

Issue	Reference[2]	Description of issue	BSA Recommendations
2. Scope of "listed acts or things"	Sections 317E, 317L, 317P, 317T, 317V, 317ZG	• The "listed acts and things" that could be required of Providers through TANs and TCNs are overly broad and, amongst other things, could require them to: ○ decrypt communications; ○ install government spyware on their systems; ○ develop a new technology or capability; ○ modify any characteristic of a service; ○ replace portions of their service with a service provided by another party; or ○ 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. • The list is 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. • 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. While the Explanatory Document provides that a TAN may require a Provider to do something where they are "*capable*" of doing so, this is not reflected in the wording of the Bill itself. • 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	• 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 Document. The Provider should only be required to comply with a TAN *to the extent it is capable* of doing so. There should also be a further definition of "capability" to clarify that it must be reasonably practicable, taking into account, amongst other things, the resources reasonably available to the Provider. • 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 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,

Issue	Reference[2]	Description of issue	BSA Recommendations
		to install software provided by an agency (under section 317E(1)(e)), 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.	and guidance as to what is and is not required. In particular: ○ 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; ○ 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; ○ 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 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; ○ sub-section (1)(d): the requirement to provide information in a particular format should be subject to a qualification that the format is secure; ○ 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; ○ 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 ○ sub-section 1(j): the requirement to conceal certain actions should be removed as it is unclear how a Provider can comply without making false or

Issue	Reference[2]	Description of issue	BSA Recommendations
			misleading statements or engaging in dishonest conduct. • 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 "relevant objectives" for which a request or notice may be issued are overly broad. These objectives include enforcing criminal law and laws imposing pecuniary penalties, assisting the enforcement of criminal laws in force in a foreign country, protecting the public revenue, 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 relevant objectives, which further broadens the scope. • While these purposes are consistent with those for which agencies can seek assistance under section 313 of the Telecommunications Act, the application of the Telecommunications Act is limited to carriers and carriage service providers, and does not apply 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 go far beyond anything in the Telecommunications Act (see item 2 above). • 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	• The "relevant objectives" should be limited to the following matters: ○ 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 ○ the purpose of 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. • 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 BSA disagrees with 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

Issue	Reference[2]	Description of issue	BSA Recommendations
		perform the "listed acts or things" to achieve such broadly-defined objectives sets a troubling precedent and goes beyond even the UK Investigatory Powers Act. • Notices requiring that Providers assist elements of Australia's national security apparatus for any undefined national security purpose or any undefined purpose relating to Australia's public revenue, 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.	themselves be *necessary*.[3] The purposes should not simply be "objectives" of requesting or requiring the "listed act or thing".
4. Broad application to "designated communications providers" and extraterritorial effect	Section 317C Schedule 2 to the Bill (in relation to computer access warrants)	• 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: ○ electronic service providers with one or more end users in Australia (i.e., potentially those having any website that does not geoblock Australia); ○ 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 ○ 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	• 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: ○ item 8 (manufacturers / suppliers of components for use in telecommunications facilities); ○ item 10 (manufacturers / suppliers of customer equipment);

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

Issue	Reference[2]	Description of issue	BSA Recommendations
		whether they are used in Australia); and (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 in another jurisdiction, with virtually no link to Australia, to perform acts or things that are 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. For example: ○ A TAN could require a service provider to install software provided by an agency into its systems, which would enable covert access to unencrypted data. The service provider hosts its data in the EU. Complying with the TAN would put the provider in breach of the EU's General Data Protection Regulation (**GDPR**), as installing the software impacts the adequacy of protection of personal data which is processed using the system. This could potentially expose the service provider to the substantial penalties that exist under GDPR. ○ A TCN could require a mobile phone manufacturer to develop a capability which, subject to issue of a warrant, can be switched on remotely and used to covertly record conversations or capture images or videos. The manufacturer distributes the mobile phones globally. Building such capability would make the mobile phone a listening device and cause the manufacturer to breach privacy and telecommunications laws in various jurisdictions. • Similarly, compliance with a computer access warrant (see item 6 below) might also require organizations with operations or customers outside of Australia to take actions that violate laws in other jurisdictions.	○ item 11 (manufacturers / suppliers of components for use in customer equipment); ○ item 14 (manufacturers / suppliers / providers of data processing devices); and ○ item 15 (software developers / providers). • 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 Document (page 34) 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 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 notices have no effect to the extent that compliance (whether with the assistance and access regime or a warrant) would expose the organization to liability under any other laws or regulations to which it is subject.
5. Unauthorized disclosure of information	Section 317ZF Schedule 2 to the Bill: section 47A	• 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.	• 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, or TCN) can be used should be expressly limited

Issue	Reference[2]	Description of issue	BSA Recommendations
	of the *Surveillance Devices Act 2004* ("**SDA**")	• This exposes Providers to substantial risks and these are not adequately addressed by the Bill. For example: ○ the Bill does not limit the purposes for which the technical information can be used; ○ the Bill does not require that the technical information is protected by appropriate security measures; ○ 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); ○ the Bill does not impose any requirement to minimize the volume of technical information requested; ○ the Bill does not impose time limits on the duration for which the technical information can be retained; and ○ 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. • Similarly, when requesting information under a computer access warrant, 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.	to the purposes for which such information was obtained (see item 3 above regarding "relevant objectives"). • There should 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. • 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. • Information disclosed by a service provider or system administrator under a computer access warrant should always be kept confidential other than with consent from the relevant provider of the information. Similarly, such information should also be subject to the same purpose limitation, data minimization, retention, and destruction requirements as set out above.
6. Computer access warrants	Schedule 2 to the Bill: section 64A of the SDA	• The definition of "specified persons" who may be required to provide information and assistance is very broad and includes:	• This regime should be adjusted in line with the proposed amendments set out above in relation to Schedule 1 of the Bill. In particular:

Issue	Reference[2]	Description of issue	BSA Recommendations
	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"**)	○ a person engaged under a contract for services by the owner / lessee of the computer; and ○ 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.	○ 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); ○ assistance or information should only be provided to the extent it is it is practical and technically feasible, reasonable and proportionate; and ○ 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: ○ introduce an immunity that releases a specified person who is a service provider or a system administrator from any criminal or civil liability arising from the specified person providing assistance or information under section 64A; and ○ provide for reimbursement of *all costs* incurred by a specified person who is a service provider or system administrator associated with the provision of information and assistance under a computer access warrant (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 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.

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 [redacted] or [redacted].

Yours faithfully,

[redacted]

Darryn Lim
Director, Policy – APAC