ATLASSIAN

Atlassian's submission to the PJCIS review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth)

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security (**PJCIS**)
PO Box 6021
Parliament House
Canberra ACT 2600
Australia

22 June 2020

Dear Committee Secretary,

Atlassian appreciates the opportunity to participate in the PJCIS' review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the **Act**).

Atlassian appreciates that the private sector has an important role to play in working with the Government to address and minimise threats to national security and to combat serious crime. However, the scope and impact of measures introduced by the Act represents a fundamental shift in Australia. It is therefore critical to ensure that the operation of the Act achieves its stated aims, while retaining appropriate safeguards and implementing proportionate measures. In our view, this is not currently the case.

We believe that Atlassian is in a unique position to inform the PJCIS' review of the Act.

As one of Australia's most successful home-grown technology companies, this submission presents not only Atlassian's own concerns with the Act, but also reflect those of our employees, customers and others in the Australian technology sector who do not have the resources to engage in such advocacy. In short, and as detailed further in this submission, these concerns relate to the disproportionate implications for individuals and companies given the reach of the powers, the lack of oversight and objective assessments of the issuance of industry assistance notices, a lack of clarity as to what is required of providers, and the overall impact on the Australian technology sector.

These concerns are motivated by four key factors:

- the need to balance national security concerns with the detrimental impact of the Act on Australia's growing technology sector, which is key to the future of economic growth;
- the potential impact on Atlassian's business, including our role as trusted custodians of our customers' private and commercially valuable data;
- the reputation of Australia's technology sector internationally; and
- the impact on the interconnected global technology and national security ecosystem.

With these considerations and concerns in mind, it is critical to note the significance of the technology sector to Australia's economy, both today and into the future. The technology sector

contributes $122 billion a year to the Australian economy — making it the sixth largest industry contributor to GDP — and employs at least half a million Australians. Atlassian believes that the sector can grow to become a backbone of Australia's economy, and our export capability. With the world economy fast-changing as a result of a major digital transformation (which has only been accelerated in light of recent global events), Australia needs to be ambitious and visionary, in order to grow and develop an economy which is innovative, creates jobs and maintains wealth in our country well into the future. To support the transition and growth of our economy, Australia needs to support the growth of the technology sector to become the basis of Australia's new manufacturing capability. To promote this successful transition, Australia needs to implement consistent legislation and administration across the broad matrix of technology policy to best position Australia for the future.

The continued viability and growth of technology innovation and manufacturing in Australia will in large part be based on the actual and perceived security of the technologies that underpin the digital economy and its ecosystem. In large part due to many of the issues outlined in this submission, Atlassian is concerned that the effect of the Act has been to erode trust in Australian technology providers and therefore limit the ability of Australian technology providers to compete internationally, through both their actual and perceived ability to protect their customers, data and systems from being compromised through weakened security.

Atlassian's specific concerns and recommendations

Atlassian understands that the PJCIS' review of the Act (the **Review**) will build on the findings of the review currently being conducted by the Independent National Security Legislation Monitor, and two previous Committee reviews.

Atlassian notes that there have been many submissions made by and on behalf of industry and other interested parties to these earlier reviews, including submissions made by Atlassian both in its own capacity and together with StartupAus. Further to those submissions, this submission focuses only on key concerns which Atlassian wishes to highlight in respect of the industry assistance measures in Schedule 1 of the Act, as set out below.

1. Systemic weaknesses and systemic vulnerabilities

Atlassian has significant concerns about the ambiguous nature of the prohibition on systemic weaknesses and systemic vulnerabilities, and the associated definitions, in the Act.

Atlassian believes the current definitions of 'systemic weakness' and 'systemic vulnerability', and the manner in which they operate as part of the corresponding prohibition on their introduction, are unworkable, and should be wholly re-framed to provide clarity for all parties involved. This is because:

- The current definitions of 'systemic weakness' and 'systemic vulnerability' as a weakness or vulnerability 'that affects a whole class of technology' but not 'that is selectively introduced to one or more target technologies that are connected with a particular person' can be selectively interpreted to allow a broad swath of actions that would have a systemic and detrimental impact on the security of a designated communications provider's (**DCP**) systems and products.
- As the associated defined terms used within those concepts (such as 'whole class of technology') do not have clear ordinary meanings or acknowledged industry understandings, the end result is that the relevant concepts could be widely interpreted, such that few weaknesses or vulnerabilities would meet the threshold required by the Act to fall within the prohibition in section 317ZG.

- While there are a number of specific prohibitions in the current definitions, for example, of acts that 'will, or is likely to, jeopardise the security of any information held by any other person', these prohibitions are themselves open to broad interpretation and appear to contradict what is authorised in the initial definition.

We believe that the amendments set forth in the Telecommunications Amendment (Repairing Assistance and Access) Bill 2019 (the **Bill**) provide an appropriate starting point for addressing these concerns, as it helpfully removes these unclear definitions and focuses on prohibited effects.

Atlassian would also add further protections to the prohibition, as drafted in the provisions of the Bill, to address the specific concerns that industry assistance notices should not be used to prevent improvements to a DCP's security capabilities or to create new points of access into a DCP's electronically protected systems or products that would expose otherwise secure data. These proposed protections are set out in Attachment 1 to this submission as suggested drafting changes to the version of section 317ZG included in the Bill. With respect to the building of points of access, Atlassian's primary concern is that — once created — a point of access into a DCP's systems and products can be exploited by unauthorised parties without the knowledge of law enforcement or the DCP, and without following the legal procedures required for notices under the Act. This specific example is also helpful to clarify the bounds of the 'material risk' prohibition that already exists in the Act, which is also repeated in the proposed Bill. Given the commercially valuable data entrusted to DCPs like Atlassian and the ongoing threats of intellectual property theft by state-sponsored and private actors alike, this is an important area for clarification.

In addition, Atlassian is also amenable to the proposal made in other submissions, to temporarily halt the exercise of the TCN power while industry and government co-operate on preparing a clear set of boundaries for the power.

Finally, Atlassian also believes that these amendments should be coupled with an explicit requirement in the legislation that TCNs should be identified as a measure of last resort, to be used only where access is not reasonably available through existing or other less intrusive means of co-operation.

2. Authorisation, oversight and review

The nature of the powers outlined in the Act are such that it is vital for transparency and public confidence in the Act that additional, independent approval and oversight mechanisms be adopted. Importantly, this must apply both from the perspective of pre-approval of industry assistance notices as well as subsequent disputes or objections as to their application, including in relation to whether systemic weaknesses or systemic vulnerabilities may arise.

From Atlassian's perspective, the form of approval and oversight must be independent, robust and able to increase public trust in the regime. In particular, the Act must feature approval and oversight mechanisms that are rigorous, as transparent as possible, provide DCPs with opportunities for objection and further review, and give access to the necessary guidance to allow all affected persons and entities to understand their rights under the Act.

Without seeking to limit these guiding principles, Atlassian believes that industry assistance notices should be the subject of independent judicial oversight and independent approval prior to their issuance. This approval mechanism must also be accompanied by appropriate, binding and independent review mechanisms to ensure that any disputes (including as to whether systemic weaknesses or systemic vulnerabilities may arise) that arise following issuance, variation and extension of such notices will be capable of independent review and assessment.

ATLASSIAN

3. Serious offences threshold under the Act

Atlassian believes that the current threshold for engaging the powers under the Act (which generally refers to offences punishable by 3 years of imprisonment or more) is too low. Given the nature and extent of these powers, and the stated objectives of the Act, the threshold should be raised to those crimes punishable by seven years or more of imprisonment.

4. Interaction with foreign laws

Atlassian is concerned about the interaction of the Act with foreign laws. In particular, the Act provides a limited defence to DCPs that is only available where the DCP is *located in* a foreign country, and compliance with a notice would breach the laws of that country.

This defence does not take into account the global operations of technology companies and the interconnected nature of the digital supply chain, which renders it increasingly difficult to determine *where* an act or thing must be done. The extra-territorial effect of the Act should be reviewed and clarified having regard to these principles.

5. Clarification of the application of the Act to a DCP's employees

Atlassian is also concerned about the perception that the Act may apply to individual employees of a DCP, particularly given the current 'war for talent' in the global technology industry. The Government has acknowledged that this is not the intent of the Act, and we reiterate that this should be clarified to remove all doubt. One such amendment might involve, for example, adding the following words after the table in section 317C of the Act: *'For the purposes of this Part, an individual who is an employee, contracted service provider or employee of a contracted service provider of a person that is a designated communications provider under this section 317C will not be deemed to be a designated communications provider by reason of the [above] table'*.

Finally, we understand that it is tempting to consider that much of the vocal opposition to the Act in the media is based only on perceptions or 'myths' of how the Act operates (including in respect of the issue outlined immediately above). However, we would urge caution in adopting this approach both on principle and in substance. To the extent that the Act or its effect are unclear, there is no disadvantage — and indeed considerable advantage — to using this opportunity to clarify the intent and operation of its provisions, as noted above. More importantly, in the context of the Australian technology sector and its reputation globally, the Act's reception has made it clear that perception matters.

Atlassian is committed to and intends to work further with the Government, industry and other stakeholders on these and other issues to ensure that the Act becomes an example of the clear law and fair procedure that will best position Australia for the future.

Yours sincerely

Patrick Zhang
Head of Policy & Government Affairs
Atlassian

ATLASSIAN

Attachment 1 – Proposed amendments to section 317ZG

317ZG Designated communications provider must not be requested or required to implement or build a systemic weakness or systemic vulnerability etc.

(1) A technical assistance request, technical assistance notice or technical capability notice must not have the effect of:

(a) requesting or requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability; or

(b) preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability or from improving its or its products' security, encryption or authentication capabilities or features.

(2) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, includes a reference to implement or build a new decryption capability, or to build or modify a point of access into any electronically protected products, services or systems with the intent to access, or which will or may result in access to, otherwise secure information.

(3) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, includes a reference to one or more actions that would render systemic methods of authentication or encryption less effective.

(4) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, includes a reference to any act or thing that would or may create a material risk that otherwise secure information would or may in the future be accessed, used, manipulated, disclosed or otherwise compromised by an unauthorised third party.

(5) The reference in subsection (2) and subsection (4) to otherwise secure information includes a reference to the information of, about or relating to any person who is not the subject, or is not communicating directly with the subject, of an investigation to which the relevant technical assistance request, technical assistance notice or technical capability notice relates.

(6) The reference in subsection (4) to an unauthorised third party includes a reference to any person other than:

(a) the person who is the subject of, or who is a person communicating directly with the subject of, an investigation to which the relevant technical assistance request, technical assistance notice or technical capability notice relates; or

(b) the person that issued, or asked the Attorney General to issue, the relevant technical assistance request, technical assistance notice or technical capability notice.

(7) *Subsections (2), (3) and (4) are enacted for the avoidance of doubt.*

(8) *A technical assistance request, technical assistance notice or technical capability notice has no effect to the extent (if any) to which it would have an effect covered by paragraph (1)(a) or (b).*