



Atlassian's Submission to the INSLM review of the *Telecommunications and other Legislation Amendments (Assistance and Access) Act 2018*

Independent National Security Legislation Monitor (INSLM)
Dr James Renwick CSC, SC

September 13, 2019

Dear Dr Renwick:

Atlassian appreciates the opportunity to participate in the INSLM's review into the Assistance and Access Act (**Review**).

As one of Australia's most successful homegrown technology companies, Atlassian is in a unique position to present not only our concerns with this hastily passed legislation, but to also reflect the concerns of our employees, customers and others in the Australian technology sector who do not have the resources to engage in such advocacy. In short, those concerns relate to the disproportionate implications for individuals and companies given the reach of the powers, the lack of oversight and objective assessment of the issuance of a TAN and TCN, a lack of clarity as to what is required of companies, and the overall impact on the Australian technology sector. Atlassian acknowledges that the Review has been afforded by the Government's amendments to the Assistance and Access Bill in its passage through Parliament to enable the [Parliamentary Joint Committee on Intelligence & Security \(PJCIS\) to refer the Act](#) for review by the INSLM. Atlassian notes that this is the first referral made under s7A of the INSLM Act and is therefore a significant step.

Atlassian makes this submission for consideration by the INSLM. This submission is made in addition to the submission made by StartupAUS to the PJCIS dated 31 January 2019 which Atlassian joined in. This previous submission can be found here on Atlassian's blog: <https://www.atlassian.com/blog/announcements/atlassian-urges-changes-to-australian-assistance-and-access-act>

Atlassian recognises the serious threats to national security which governments and the public face today. It fully supports the Government's law enforcement and national security work to ensure the public's safety. The technology industry has an important role to play in working with the Government to support this work. However, the legislation as currently drafted gives the government unprecedented power to impact the operations of technology companies and access their customers' data, with little oversight of government action or recourse against potential abuse. As such, the effect of the Assistance and Access Act has been to erode trust in Australian

technology companies and their ability to protect customer and individual customer data from arbitrary access and from being compromised by weakened security. It is already damaging the reputation and perception of the Australian technology industry globally.

Our intention is to work with the Government to improve the operation of Assistance and Access Act, while ensuring it maintains its stated aims. We appreciate the INSLM's quotation of Lord Anderson in his call for public comment regarding "the importance of clear law, fair procedures, rights compliance and transparency" in today's age. We believe the Assistance and Access Act fails these values in many ways. As presently drafted, we do not believe that the Assistance and Access Act contains appropriate safeguards for protecting the rights of individuals, whether they be customers or employees in technology companies, and is not a proportionate means of achieving its stated goals of improving technical assistance for law enforcement.

Atlassian's specific concerns and recommendations

Atlassian understands that the Review will specifically consider whether the Assistance and Access Act achieves an appropriate balance of:

1. providing sufficient safeguards for protecting the rights of individuals; and
2. remaining proportionate and necessary.

The focus of this submission is on Schedule 1 of the Assistance and Access Act, namely the industry assistance measures in Schedule 1.

Atlassian notes that there have been many submissions made by and on behalf of industry and other interested parties to the reviews undertaken by PJCIS of the Assistance and Access Bill and the Act once passed. It agrees with many of the amendments made by the Government to the Bill to limit the application of the laws and to further strengthen the oversight of the exercise of powers.

Atlassian submits that the extent to which cloud computing services are now used should be considered, as the interconnectedness of the digital supply chain mean that the powers in the Access and Assistance Act have potentially far-reaching consequences beyond Australia. For example, an Australian based technology company may host or have access to the data of customers located worldwide and may be compelled under the Assistance and Access Act to enable access to the same. The INSLM should consider both the specific statutory powers and their overall breadth and effect together when considering whether the powers and procedures are proportionate and necessary and include only the least intrusive measures to achieve the stated objectives in order to safeguard individual rights.

The Review should also consider and take into account what alternative measures to a TAN or TCN may be available to agencies.

Set out below are the key concerns in relation to which Atlassian wishes to highlight -

1. Clarification of the uncertainty about the ability to issue Technical Compliance Notices (TCNs) against individual employees of a DCP:

The uncertainty about the ability for individual employees to be compelled to give assistance and the prohibition on disclosing TCN information has caused much anxiety among Australian technology workers and global companies with employees in Australia. It has led to certain American technology companies characterising their Australian staff as potential “insider threats”. This has undermined Atlassian’s efforts to recruit talent to Australia and is likely to discourage global technology firms from investing in Australian personnel. Atlassian submits that this should be addressed by amending the definition of DCP to clarify that while an individual may be a DCP, individuals who are employees of a DCP can never be.

2. Need for robust and credible authorisation, oversight and avenue for review/complaint:

Atlassian submits that, given the impact which the exercise of assistance powers will have on the privacy and freedoms of individuals and the onerous penalties on DCPs for non-compliance, there should be further statutory limitations on and increased oversight of the exercise of agency powers to issue, vary or renew industry assistance notices. This will also help address the risk of agencies resorting to issuing a notice instead of obtaining a warrant. The particular measures Atlassian submits should be introduced to ensure a statutory framework that can further control the exercise of agencies’ powers and ensure appropriate safeguards are as follows:

a) Atlassian strongly believes that the legality of TAN and TCN should be the subject of judicial oversight. There is currently no requirement for agencies to obtain judicial approval to issue notices and affected individuals cannot be informed of the exercise of powers which may compromise the privacy and security of their information and cannot challenge a notice. It is critical that the exercise of the power to do so is subject to independent judicial oversight before a notice can be issued.

b) Alternatively or in addition, DCPs should be able to complain about the issuing of any TAN or TCN or a variation or extension of them.

c) The regime in relation to obtaining independent assessment of the effect of the requirements of a TCN should be extended: DCPs should be able to request them in relation to both TCNs and TANs and any variation or extension of them. If requested by a DCP, an independent assessor’s report should be binding rather than merely informative.

d) Oversight should also be further strengthened by giving the Office of the Australian Information Commissioner and the Commonwealth Ombudsman additional oversight in relation to the exercise of powers - to receive information about and have oversight of assistance requests.

3. Definitions of ‘systemic vulnerability’ and ‘systemic weakness’:

Atlassian submits that key legal definitions that underpin the statutory framework should be carefully reviewed in consultation with stakeholders, including the technology industry, and further clarified or limited. In particular, the disclosure prohibitions and the definitions in relation to building a ‘systemic vulnerability’ or a ‘systemic weakness’.

Clarification of the definition states that industry assistance cannot be requested or required if it would be likely to "jeopardise the security of any information held by a person other than a person connected with a target technology, including if the act or thing or requested or required would create a material risk that otherwise secure information can be accessed by an unauthorised third party."

However, this clarification appears to contradict the Act’s assertion that an assistance notice can require the selective introduction of a weakness or vulnerability in a particular service, device or item or software. It is unclear how a vulnerability or weakness could be introduced into a particular application targeted at a specific person which would not ‘be likely to’ compromise the entire application or class of devices (and therefore compromise it in respect of all users rather than a specific user). The definitions and concepts need to be clarified to ensure that the terms of a TAN or TCN cannot require any assistance or the building of any capability or functionality to have this effect. Independent assessment and judicial oversight would provide additional opportunities for redress and clarification.

4. Threshold for ‘serious Australian offence’:

The definition of a serious offence is one that is against a law of the Commonwealth, a State or a Territory that is punishable by a maximum term of imprisonment of 3 years or more or for life. This makes the threshold for offences in relation to which an interception agency can issue an assistance request for enforcement purposes very low. Atlassian submits that this is inconsistent with the stated objectives of the Act in relation to serious crime and is a further example of how the combined effect of provisions in the statutory framework can operate to broaden agencies’ powers without judicial oversight. This definition also extends to serious foreign offences. Atlassian submits that the definition should at least be consistent with the definition in the *Telecommunications Interception Act* which establishes a higher threshold of seven years or more.

5. Assistance in relation to foreign offences:

Atlassian remains concerned that the industry assistance powers will offer a back door for foreign agencies to exercise powers they may otherwise not have under their local laws. The absence of judicial oversight detailed above heightens this risk, as does the Act’s failure to clearly treat situations involving a conflict of laws, discussed below.



6. Extra-territorial effect of the Act:

The Assistance and Access Act now provides a defence to a DCP in a foreign country for failing to comply with a TCN or TAN if doing so would breach a foreign law in the country where they are located.

However, this amendment does not take into account the global operations of technology companies and the global digital supply chain which means Australian based DCPs may also be custodians for the data of individuals located outside of Australia and be subject to laws in foreign countries where they operate and do business (such as the European *General Data Protection Regulation*). This amendment does not protect those DCPs from breaching foreign laws, nor does it protect the rights of foreign individuals under their local laws. Atlassian submits that the extra-territorial effect of the Act should be reviewed and clarified.

Conclusion

We know there will be many voices which the INSLM will hear from and consult in its Review. We look forward to the consultation process with the INSLM and the further exchange of views on these and other important areas for improvement of the Assistance and Access Act to achieve a balanced and proportionate framework of laws that both protects individual rights and achieves the important objectives of protecting national security and combatting serious crime.

Yours sincerely

Scott Farquhar and Mike Cannon-Brookes
Co-Founders & Co-CEOs
Atlassian