June 26, 2019

Parliamentary Joint Committee on Intelligence and Security
By online submission

REVIEW OF THE AMENDMENTS MADE BY THE TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018 – BSA COMMENTS

BSA | The Software Alliance (**BSA**)[1] refers to the review[2] by the Parliamentary Joint Committee on Intelligence and Security (**Committee**) of the amendments made to Commonwealth legislation by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (**Assistance and Access Act**).

BSA re-affirms our interest in the issues being discussed in relation to the Assistance and Access Act, and thanks the Committee for this further comment opportunity.

In this submission, we address the interaction of the Assistance and Access Act with the United States' *Clarifying Lawful Overseas Use of Data Act* (**CLOUD Act**).[3]

Our previous submissions to the Committee on the Assistance and Access Act (including when it was only a bill) also remain relevant to the Committee's present review.[4] We commend these previous submissions to the Committee for the Committee's re-consideration.

---

[1] BSA (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members are at the forefront of data-driven innovation, including cutting-edge advancements in data analytics, machine learning, and the Internet of Things. They earn users' confidence by providing essential security technologies, such as encryption, to protect customers from cyber threats.

BSA's members include: Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Baseplan Software, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] As notified on this review home page: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018.

[3] *CLOUD Act*, S. 2383 - 115th Congress, enacted March 23, 2018, available at: https://www.govtrack.us/congress/bills/115/s2383.

[4] Please refer to our submissions of October 12, 2018 and October 31, 2018, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Submissions (as Submission 48 and Supplementary to Submission 48, respectively).

Please also refer to our submission of February 12, 2019, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/ReviewofTOLAAct/Submissions (as Submission 36).

300 Beach Road
#25-08 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

Overview of the CLOUD Act

The CLOUD Act was enacted to, among other things, update the legal framework for US law enforcement to access data stored by specified communications service providers[5] (**CSPs**) who are subject to US jurisdiction, regardless of where the data is stored and pursuant to specific legal processes.

Of particular relevance to this submission, the CLOUD Act also empowers the US Government to enter into executive agreements with other eligible governments to enable law enforcement agencies to access data across each other's borders to investigate and prosecute serious crimes,[6] subject to an agreed-upon set of processes and controls negotiated between the two governments. As described in a US Department of Justice white paper[7] (**DOJ White Paper**), under such agreements, "*each country would remove any legal barriers that may otherwise prohibit compliance with qualifying court orders issued by the other country. Both nations would be able to submit orders for electronic evidence needed to combat serious crime directly to CSPs, without involving the other government and without fear of conflict with U.S. or the other nation's law.*" [8] Such agreements would thus provide a potentially more expedited means, as compared to the current Mutual Legal Assistance Treaty (**MLAT**) regime, for law enforcement agencies to obtain electronic evidence stored abroad in criminal investigations.

As pre-conditions to the US Government entering into an executive agreement with a foreign government, the CLOUD Act (in §105) requires, among other things, that:

(1) "*the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and liberties…*", which would include "*protection from arbitrary and unlawful interference with privacy*" and "*sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data by the foreign government*"; and

(2) with respect to any law enforcement order subject to the executive agreement and to be issued by the foreign government, the order must "*be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order*".

Potential Conflict between the Assistance and Access Act and the CLOUD Act

In its current form, the Assistance and Access Act could undermine Australia's qualification to enter into an executive agreement because of concerns the Assistance and Access Act creates about Australia's compliance with the above standards in the CLOUD Act.

---

[5] The CLOUD Act applies to two types of service providers:

(1) providers of "electronic communications services", which are defined as "services that provide users with "the ability to send or receive wire or electronic communications." (18 U.S.C. § 2510(15)); and

(2) providers of "remote computing services", which are defined as "services that provide "to the public" "computer storage or processing services" using an electronic communications system. (18 U.S.C. § 2711(2))

[6] The CLOUD Act does not define "serious crime" other than that it includes "terrorism".

[7] US Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, April 2019, available at: https://www.justice.gov/opa/press-release/file/1153446.

[8] DOJ White Paper, at page 4.

In particular, the Assistance and Access Act authorizes the Australian government to issue technical assistance notices (**TANs**) and technical capability notices (**TCNs**) to compel private companies to build or implement certain surveillance capabilities, without any recourse to a merits review by an independent judicial authority before or after a TAN or TCN is issued, and limited recourse to judicial review of the administrative decision to issue the TAN or TCN after the fact. Further, while TCNs can only be issued by the Attorney-General with prior approval from the Minister of Communications (and Cybersafety), no such safeguard exists in respect of TANs, which can be issued by the heads of the relevant enforcement agencies with no pre-issuance review by any independent authority.

The Assistance and Access Act also provides broad authority to the Australian Security Intelligence Organisation to issue TANs or TCNs for the purpose of "safeguarding national security", with little specific guidance as to the circumstances in which such purpose would apply, safeguards against abuse, and implementation oversight.

The above shortfalls in the overall TAN/TCN regime (among others) could result in the potentially arbitrary and non-transparent issuance of TANs and TCNs, in turn resulting in an arbitrary impact on privacy and liberties. This, coupled with the general lack of review or oversight by independent authorities in the TAN/TCN issuance process, would pose serious concerns as to whether the pre-conditions for entering into an executive agreement under the CLOUD Act are met.

To address these concerns and improve the prospects that Australia could be appropriately deemed to have met the standards in the CLOUD Act for entry into an executive agreement, the Assistance and Access Act should be amended to:

- make available a merits review by an independent judicial authority of any decision to issue a TAN or TCN, both before and after the issuance of the TAN or TCN;
- create a clear pathway for independent judicial review of any administrative decision to issue a TAN or TCN, such as by re-including Part 15 of the *Telecommunications Act 1997* (i.e., the provisions introduced by the Assistance and Access Act) in the scope of the *Administrative Decisions (Judicial Review) Act 1977*; and
- define how the authorities in the Assistance and Access Act may be used for the purpose of "safeguarding national security", including by detailing the circumstances in which such purpose would apply, safeguards against abuse, and implementation oversight mechanisms.

Conclusion

As we noted in our earlier submissions to the Committee, the issues concerning the assistance and access regime are complex and sensitive. BSA and our members remain at the disposal of the Committee and the Australian Government and Opposition stakeholders to help develop and deliver other enduring solutions to address the challenges of accessing evidence in the digital age.

BSA | THE SOFTWARE ALLIANCE