Friday 13 September 2019

Dr James Renwick CSC SC
Independent National Security Legislation Monitor
3-5 National Cct,
BARTON ACT 2600

Dear Dr Renwick,

Independent National Security Legislation Monitor Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Submitted via Online Submission Form

Please find attached a submission from Amazon Web Services ("**AWS**") in respect of your review of the abovementioned Act.

The content of this submission was made previously to the Parliamentary Joint Committee on Intelligence and Security ("**PJCIS**") in July 2019. In the opinion of AWS the substantive issues raised in our submission to the PJCIS remain relevant to the terms of reference for this Inquiry.

AWS would welcome the opportunity to discuss further this submission.

Yours sincerely,

[redacted]
Simon Edwards
Head of Public Policy, Australia & New Zealand
Amazon Web Services

[redacted]

SUMMARY POSITION

Trust in the security of information is fundamental to business innovation and economic growth – it is crucial in a digital economy. Information security tools, processes and protocols are deployed to protect the personal data of Australian citizens, and the commercial or sensitive information of businesses and governments. We recognise that any technology can, in the wrong hands, be used for criminal and other illegal purposes. Consequently, AWS takes seriously our obligations to law enforcement.

We recognise the complex dilemma facing law enforcement and security agencies with advances in information security and the widespread adoption of encryption technologies. The *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (the "**Act**") however alters the balance between law enforcement needs to access readable data and the right of technology users to expect that the products and services they use are free from interference. The Act has the capacity to reduce consumer trust in technology.

The Act has provided new powers for law enforcement and security agencies that could be used to order technology providers to create or install new ways to access secure systems and data. Each of these ways of access would constitute a security vulnerability. The underlying assumption of the Act, that a security vulnerability can be created for a targeted technology without creating a systemic weakness or vulnerability, is technically flawed. Data cannot be made more secure by introducing any security vulnerability into a technology system.

Deliberately creating for one party a means of access to otherwise secure data will create weaknesses and vulnerabilities that, regardless of any good intentions, creates the opportunity for other actors - including malicious ones - to access that same data. Simply stated, if anyone creates a vulnerability in a technology that allows access to otherwise secure data then that vulnerability is capable of being exploited by another party with the knowledge and means to do so.

The extraordinary powers provided by the Act need to be balanced by specific measures that establish public confidence and trust in the use of those powers. AWS acknowledges that there is no simple solution to the security of data dilemma faced by law enforcement and security agencies in an age of ubiquitous encryption. Nevertheless, any law that puts the data of Australians at greater risk and reduces trust in technology is not the answer.

CONCERNS WITH THE ACT

In addition to the Act's fundamental flaw that we outline above, the following specific concerns are raised for consideration.

(i) Creation of Weaknesses and Vulnerabilities. Notices cannot require a technology provider to implement or build a systemic weakness or a systemic vulnerability *into a form of electronic protection*. However, a technology provider can be required to install or maintain any software or equipment, or to implement or build systemic weaknesses or vulnerabilities into any other component of a network, system, product or service.

(ii) Lack of Judicial Authorisation and Review. Notices are issued based on the judgment of decision-makers at agencies or the Attorney-General, without prior judicial authorisation. These Notices can be issued based on facts or criteria that may not be made known to the recipient of the Notice. The validity of a Notice is dependent upon the issuer's interpretation of the law, their analysis of the facts, and their weighting of the various factors to which the Act requires them to give consideration. There is no requirement for this assessment to be documented to help ensure consistent application of the Act. Once a decision to issue a Notice has been made, that decision cannot be reviewed by a judge on its merits.

(iii) Extraterritorial Jurisdiction and Conflicts of Law. Notices can require technology providers to do acts in Australia that violate the laws of other countries in which they operate.

(iv) Expansion of interception and data retention capabilities. The Act's Explanatory Memorandum states that interception and data retention obligations remain subject to; "existing legislative arrangements," which apply only to carriers or carriage service providers, who are only a subset of technology providers captured by the scope of the Act. The language of the Act, however, does not make clear that only carriers or carriage providers are subject to these obligations, potentially expanding obligations to other entities. This anomaly needs to be corrected.

RECOMMENDATIONS TO INCREASE TRUST

(i) Creation of Weaknesses and Vulnerabilities. We recommend that clause 317ZG of Schedule 1 of the Act be amended by deleting the term "systemic". The clause should also be amended to apply this limitation to all "listed act or things" in clause 317ZE (consistent with Recommendation 10 in the Committee's Advisory Report on the Act in December 2018). So that a Notice cannot require a technology provider to implement or build a weakness or vulnerability into a network, system, product or service.

(ii) Judicial Authorisation and Review. We recommend that Division 3 and Division 4 of Schedule 1 of the Act be amended so that a Notice can only be issued or varied based on a determination of an independent judicial officer. We also recommend that the amendment to the *Administrative Decisions (Judicial Review) Act 1977* in Schedule 1 of the Act be deleted so that the decision to issue a Notice can be reviewable by a judge.

(iii) Extraterritorial Jurisdiction and Conflicts of Law. We recommend that clause 317ZB(5) of Schedule 1 of the Act be amended so that a technology provider has a defence for failing to comply with the requirement of a Notice if they can prove that compliance with the requirement - either in Australia or in a foreign country - would contravene the law of a foreign country.

(iv) Expansion of interception and data retention capabilities. We recommend that clause 317ZH of Schedule 1 of the Act be amended so that Notices cannot be used to impose data retention or interception capabilities on technology providers that are not a carrier or carriage service provider, as defined in the *Telecommunications Act 1997*.

We also consider there are opportunities to improve the ability of law enforcement and security agencies to work with overseas technology providers within existing international legal assistance frameworks. For example, the United States is looking to enter into Executive Agreements under the CLOUD Act with nations that can meet their bar on privacy and human rights. AWS recommends that signing an Executive Agreement should be a priority for both Australia and the United States.

About Amazon and AWS

Founded in 1994, Amazon is a retail and technology company with principal offices in Seattle, Washington. Amazon is guided by four principles: customer obsession rather than competitor focus, passion for invention, commitment to operational excellence, and long-term thinking. Customer reviews, 1-Click shopping, personalised recommendations, Prime, Fulfilment by Amazon, Amazon Web Services, Kindle Direct Publishing, and Amazon Devices are some of the products and services pioneered by Amazon.

Amazon serves Australian customers through its global websites, including www.amazon.com.au. Thousands of small and medium-sized Australian businesses currently sell their products to Amazon customers around the world via Amazon Marketplaces and thousands of independent Australian authors have published books via our Kindle Direct Publishing service.

AWS offers 165 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality, media, and application development, deployment, and management. These are available from 66 Availability Zones (AZs) within 21 geographic regions and one Local Region around the world, spanning the U.S., Australia, Brazil, Canada, China, France, Germany, India, Ireland, Japan, Korea, Singapore, and the UK. The global network of AWS Edge locations now consists of 169 Points of Presence (158 Edge Locations and 11 Regional Edge Caches) in 68 cities across 29 countries.