The Secretary
Parliamentary Joint Committee on Intelligence and Security
Parliament House
CANBERRA ACT 2600

SURVEILLANCE LEGISLATION AMENDMENT (IDENTIFY AND DISRUPT) BILL 2020 – PUBLIC SUBMISSION BY AMAZON WEB SERVICES

Dear Secretary

Amazon Web Services (**AWS**), provider of the world's most comprehensive and broadly adopted cloud computing platform, welcomes the opportunity to make the following submission to the Committee in respect of the draft *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* ('**the Bill**').

Relevance of the Bill to Cloud Computing and Customer Accounts

Cloud computing is the on-demand delivery of IT resources over the internet with pay-as-you-go pricing. For more than 14 years, AWS has provided, via cloud computing, the technology tools, services, and infrastructure required for customers to develop and build information technology products and solutions.

Our customers establish accounts with us that provide them with access to technologies developed by AWS and thousands of other entities across the world. With these technologies, our customers – commercial, not-for-profit, and governments – build and operate online services for both their own purposes and for the purpose of providing online services to end users.

An AWS account is created and activated by an account administrator, normally via the AWS Console (an online portal that provides access to all the AWS Cloud's features and functions). A customer can choose from over 200 fully featured AWS services to provision, manage and deploy their applications online. The services a customer chooses, and how those services are consumed, is decided by the customer. It is also the customer who selects where across AWS's global network they want their data stored. The AWS Cloud spans 24 geographic regions around the world including Australia (The Sydney Region has been operating since 2012 and a new Melbourne Region will be opened in 2022).

AWS recognises and acknowledges that the digitisation of much of our society's communications, commerce, retail, and critical infrastructure sectors, among others, has increased opportunities for the conduct of criminal activity online. In this context, law enforcement's need to access data to investigate or prevent criminal activities could in certain circumstances involve an AWS customer or their end user. AWS has approached consideration of the Bill with the aim of ensuring that the lawful interests of our customers in the security of the services they purchase from us, and in the protection of their information, should not be arbitrarily or unnecessarily compromised.

We have noted that two of the Bill's proposed warrants (data disruption and account takeover) are formulated for fundamentally different objectives for law enforcement, compared to warrants that law enforcement agencies can currently seek. These two warrants are intended not for the purpose of gathering evidence per se, but to allow law enforcement agents to effectively stand in the (online) shoes of persons suspected of engaging in potential criminal activity.

Though ancillary to existing warrants, both of these warrants are a significant departure from current provisions and their issue will involve an elevated risk to the liberty and privacy of citizens whose online accounts are impacted by law enforcement activities. The warrants will necessitate an increased responsibility on the relevant law enforcement agencies to act with care and propriety, and their use should be appropriately circumscribed by proportionate checks and balances, as well as supervised and monitored by an independent party.

This will be particularly the case if the computer that is the target of a data disruption warrant, or an online account that is the target of an account takeover warrant, is located in or provided from a cloud computing service as those computers and accounts could be servicing potentially thousands or millions of entities.

In considering the Bill we have noted the interplay between the changes proposed in the Bill and the operation of powers authorised by prior amendments to various pieces of legislation, including by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* ('**Assistance and Access Act'**). We note that the changes proposed in the Bill continue the Government's development of a comprehensive legislative framework for providing Australian law enforcement agencies with authority to investigate and prosecute serious criminal activity, including serious online criminal activity.

Understanding the above, we submit to the Committee for its consideration the following suggestions for improvements to the Bill.

Clarification of Assistance Provisions

Assistance to be Reasonable and Proportionate

To give effect to the stated purposes of the warrants proposed in the Bill, and to fulfill the objectives of the warrants, particularly where covert activity is required, it is likely that in many instances relevant law enforcement agencies will require the assistance of electronic service or designated communication providers.

As the Committee would be aware, AWS expressed reservations in 2018 that provisions of the Assistance and Access Act (introducing Part XV of the Telecommunications Act) could require actions that had the potential to make technology systems less secure. Chief among our concerns was the possibility that technology providers may be required to take actions that would defeat security protections provided to customers in a way that would systematically undermine the very purpose of those protections.

In response to these concerns, the Government included in the Assistance and Access Act provisions that listed matters that decision makers had to consider when determining whether notices seeking industry assistance under that Act were reasonable and proportionate.

Recommendation: AWS submits that similar considerations should be specified in the Bill and that technical feasibility should be an express consideration for those issuing warrants.

Additionally, AWS submits that the execution of the warrants proposed in the Bill should not result in the introduction of systemic weaknesses or vulnerabilities into any form of electronic protection of data implemented in a technology provider's systems. Such a warrant would be unreasonable in any circumstance as it would create significant and lasting risk to innocent third parties.

AWS submits that the Bill should be amended to include a specific prohibition against warrants being executed in a manner that would:

a) Require a person to implement or build a systemic weakness into a form of electronic protection; or
b) Prevent a person from rectifying a systemic weakness in a form of electronic protection.

Given the purpose of the warrants proposed in the Bill, AWS further submits that a relevant consideration for an issuing authority should be whether what is proposed by the law enforcement applicant is in all the circumstances technically feasible. This would require the applicant to make a case to the issuing authority as to how they propose, in particular, to disrupt data or takeover an online account. Warrants should not allow technical fishing expeditions that put at risk third parties.

Individual Assistance or Provider Assistance

As presently drafted, the Bill enables a law enforcement officer of the AFP or the ACIC to apply for an order requiring a specific person to provide information or assistance to enable the execution of warrants. These provisions mirror already existing provisions in the *Surveillance Devices Act 2004* and the *Crimes Act 1917*. In the circumstances of a cloud service, the ability of any one individual to support such warrants directed to a single account or target computer is highly problematic and most unlikely.

AWS notes that the government has legislated powers under the Assistance and Access Act framework to deal with circumstances where assistance is required from a provider. That regime requires that seeking the assistance must be both reasonable and proportionate. Relevant considerations are listed in the Act.

As drafted, the Bill does not provide, in our view, sufficient protection for individual employees of technology providers such as cloud services, and creates an assistance regime that is different from that specified for technology providers under the Assistance and Access Act. The Bill enables law enforcement to seek an assistance order requiring a specified person to provide any information or assistance that is reasonable and necessary to execute the warrant. A specified person includes an employee of the owner or lessee of the computer, or a person engaged under a contract for services by the owner or lessee of the computer, or a person who is or was a system administrator for the system including the computer. These definitions could include employees of a cloud service provider.

Recommendation: Given the potential cross-over of legislative provisions in relation to seeking assistance, AWS submits that the Bill should be amended to make clear that where assistance is sought from an individual the assistance request should be both reasonable and proportionate using the criteria specified in the Assistance and Access Act.

We have included possible language in Appendix A to this submission to demonstrate what this would mean in the case of an assistance order for a data disruption warrant.

Jurisdiction and Foreign Parent entities

AWS is also concerned employees who might be ordered to do an act or thing, or omit to do an act or thing, under an assistance order may be required to breach a foreign law, or cause another person to breach a foreign law. It would be appropriate to either make clear in the Bill that any such requirement would be unreasonable or provide a defence for an individual who refuses to do the act or make the omission. This is important for employees of technology providers who deliver services from computers located outside of Australia.

Recommendation: AWS submits that an appropriate defence would involve the introduction of a modified version of the exemption in section 317ZB (5) of the *Telecommunications Act 1997* in respect of the laws of foreign countries.

Immunity for related actions taken in good faith

The execution of warrants by law enforcement, or providing assistance in good faith to law enforcement officers executing a warrant, should not result in civil liability to a person (for example, a civil claim for breach of contract by a user where a technology industry participant is affected by a warrant or provides lawful assistance).

AWS recognises that there are difficulties in framing an appropriately narrow immunity for warrants where a technology industry participant may not necessarily be involved, but for account takeover warrants, and for assistance provided under assistance orders relating to account takeover warrants, there should be provision protecting third parties from liability.

Recommendation: AWS submits that the Bill should be amended to introduce a new immunity for online account providers in relation to the execution of account takeover warrants. This may be included, for example, at the proposed section 3ZZUR of the *Crimes Act*. The immunity should extend to criminal and civil liability, or an action or other form of proceeding for damages, in relation to an act or omission done in good faith in purported compliance with, or in the furtherance of a requirement under, an account takeover warrant.

Cost Recovery

The Bill acknowledges the need to provide for cost recovery and compensation relating to the execution of account takeover warrants. In AWS's view the same compensation provisions should apply to the execution of the other new warrants where loss or damage is innocently incurred.

It is not possible to predict all the potential outcomes from the execution of data disruption and network activity warrants. They are novel warrants. How they will be executed and to what effect cannot be known at this time. However as a data disruption warrant, like an account takeover warrant, will likely require the potential manipulation of technology systems and data, it is appropriate that the Commonwealth be willing to pay reasonable compensation if a person suffers loss of or serious damage to their property, or personal injury, as a result of the execution or as a direct result of the execution of any of the new warrants proposed in the Bill.

Recommendation: AWS submits that the terms of proposed clause 3ZZWA of the *Crimes Act 1917* be replicated in relevant sections of the *Surveillance Devices Act 2004*.

Judicial Authorisation of Warrants that involve coercive power

The Bill replicates the authorisation provisions of the *Surveillance Devices Act 2004* for two of the new warrants - data disruption and network activity. This means that these warrants can be issued by an eligible judge or a nominated member of the Australian Appeals Tribunal (AAT).

AWS maintains and repeats the views it expressed during the Parliament's consideration of previous legislation, namely the *Assistance and Access Act,* and the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020*, that independent judicial oversight and authorisation of warrants should be required where warrants involve interference in or the compromise of private property of not only technology providers but potentially millions of innocent citizens.

Recommendation: AWS supports the long-standing preference of the Senate Standing Committee for the Scrutiny of Bills that the power to issue warrants authorising the use of coercive or intrusive powers should only be conferred on judicial officers. AWS would fully support an amendment to the *Surveillance Devices Act 2004* and to the *Telecommunications Act 1997* to simplify and harmonise the issuance of warrants that involve the use of coercive or intrusive powers, by requiring that such warrants be issued and authorised by judicial officers.

AWS thanks the Committee for the opportunity to make this submission and is prepared to provide further support to the Committee in its consideration of the Bill.

Appendix A

Amending Clause 47 of Schedule 1 Section 64B of Surveillance Devices Act 2004[1] to introduce a modified versions of the exemption in Section 317ZH, and proportionality factors in section 317JC, 317RA, and 317ZAA of the *Telecommunications Act 1997*.

(2) The eligible Judge or nominated AAT member may grant the assistance order if the eligible Judge or nominated AAT member is satisfied that:

…

(vii) a person who is or was a system administrator for the system including the computer;

(f) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms or formed a part; or

(ii) measures applied to protect data held in the computer; and

(g) the information or assistance is reasonable and proportionate in all the circumstances.

Whether information or assistance is reasonable and proportionate

(3) In considering whether an assistance order is reasonable and proportionate, the eligible Judge or nominated AAT member must have regard to the following matters:

(a) the interests of law enforcement;

(b) the legitimate interests of the person to whom the order relates;

(c) the objectives of the order;

(d) the availability of other means to achieve the objectives of the order, including the availability of assistance under another law of the Commonwealth;

(e) whether the order is the least intrusive form of industry assistance, when compared to other forms of industry assistance known to the eligible Judge or nominated AAT member;

(f) whether the request is necessary;

(g) the legitimate expectations of the Australian community relating to privacy and cybersecurity;

(h) such other matters (if any) as the eligible Judge or nominated AAT member considers relevant.

General limits on assistance orders

(4) An assistance order has no effect to the extent (if any) to which it would require a specified person to do an act or thing for which the Australian Federal Police or the Australian Crime Commission, or a law enforcement officer of the Australian Federal Police or the Australian Crime Commission, would otherwise be entitled to request or obtain assistance from the specified person to do under Part 15 of the Telecommunications Act 1997.

[1] An equivalent proposed change would also need to be made to Schedule 3 of the Bill (in proposed section 3ZZVG of the Crimes Act).