18 February 2022

Department of Home Affairs
Commonwealth of Australia

(Submission lodged via email)

Dear Sir/Madam,

Re: Reform of Australia's electronic surveillance framework Discussion Paper

AWS is pleased to provide comment on the *Reform of Australia's electronic surveillance framework Discussion Paper* (the Discussion Paper). This Discussion Paper raises fundamental questions on the scope and use of electronic surveillance, and we welcome ongoing engagement with the Department of Home Affairs (the Department) on the development of these important reforms.

As the Discussion Paper and the *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Richardson Review) comprehensively demonstrate, Australia's electronic surveillance laws are complex, inconsistent, outdated and inflexible. AWS agrees that it is necessary and appropriate that these laws are updated to reflect the continuously evolving technological landscape. Incremental changes introduced over decades, designed to address new and emerging issues, have ultimately resulted in a disaggregated and confusing framework.

AWS views these reforms as an opportunity to support the important work of law enforcement and the intelligence community, while protecting the privacy of individuals and security of information and data. In principle, we support reforms that are technology-neutral and adaptable, result in clear accountabilities, and create streamlined processes. It is also essential that a revised framework balance the legitimate needs of law enforcement and intelligence agencies with strong safeguards and oversight.

We are encouraged that the Discussion Paper acknowledges these issues as core considerations and recognises the deeply complex and technical nature of the questions it asks. Our hope is that this consultation is the beginning of a detailed, considered process that examines each of the issues outlined in the Discussion Paper with an appropriate level of depth. The sensitive and intrusive nature of surveillance powers requires nothing less, and we believe that confidence and public trust in the scope and use of surveillance powers should be a fundamental consideration as these reforms progress. We look forward to working closely with the Department throughout this process.

Guiding Principles for Reform

To meet these objectives, AWS suggests that the following core principles underpin the development of the proposed legislative framework.

1. Reasonable and Proportionate

Who should be able to access information and when?

A new framework needs to balance the public safety objectives of law enforcement and the intelligence community with protecting the privacy of individuals and security of information and data. To achieve

this, the new legislative framework should require that surveillance and data disclosure requests be reasonable in scope and proportionate to the nature of the offence under investigation. The following elements should be considered as part of achieving this balance:

Application of least privilege: In recognition of the sensitive and intrusive nature of surveillance activities, as a general rule we believe the principle of least privilege – an information security concept which requires that the minimum level of access be granted to allow a user, in this case whether a person or agency, to perform their job functions – should be a baseline expectation for warrants and data disclosure requests.

Clear thresholds: To reflect the seriousness of the use of surveillance powers, we recommend that a new framework adopts the definition of 'serious offences' from the *Telecommunications (Interception and Access) Act 1979*. This definition provides an appropriately comprehensive set of circumstances for the use of lawful interception and access powers, including references against relevant state and territory legislation.

On the question of thresholds, we also note that while the Discussion Paper extensively references national security justifications for surveillance activities, there is currently no standard legislative definition of 'national security'. We recommend that the definition of national security, for the purposes of meeting an appropriate legislative threshold for the provision of warrants and data disclosures, be given a clear meaning within a new electronic surveillance framework. Within the context of domestic surveillance, it is appropriate that this meaning reflect espionage, sabotage, foreign interference, and terrorism or violent extremism.

Recognition of non-content data sensitivity: Achieving a reasonable and proportionate balance should include a recognition that metadata and non-content data, particularly when combined across multiple sources, may be as sensitive as content or information. Indeed, the potentially sensitive nature of data aggregation in commercial settings was acknowledged by the Attorney-General's Department in its recent *Privacy Act Review Discussion Paper*. It would be a significant lacuna for reforms to protect the privacy of individuals to recognise a certain level of sensitivity in one setting and not in another – arguably more intrusive – setting.

Metadata and non-content data requests should be required to adhere to clear thresholds and be proportionate to the offence being investigated, as recommended by the Parliamentary Joint Committee for Intelligence and Security (PJCIS) in its 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*. In that review, the PJCIS recommended an examination of the proportionality test required under the TIA Act to "also consider the appropriateness of applying a consistent proportionality test across the interception, stored communications and access to telecommunications data powers". Similar issues were raised by the PJCIS in its 2020 *Review of the mandatory data retention regime*.

On consideration of these different reviews and the submissions of multiple entities highlighting the serious and intrusive nature of non-content data, it is clear that warrantless requests for metadata or non-content data are no longer fit for purpose and should be replaced by a more robust system under the new framework.

Specificity of requests: Warrants or data disclosure requests should be specific and time-bound. While we support the overall aim of creating a simplified warrant framework, this should not be achieved by the creation of a 'catch-all' warrant that emphasizes outcomes without proper regard for the methods used (as indicated on pages 34-36 of the Discussion Paper). The specificity of a request is crucial for both ensuring that activities are proportionate, and that the compliance burdens on impacted entities remain manageable.

Principle of proximity: The warrant should be directed to the entity or application owner closest to the intended target of surveillance activities. As well as being important for the timely and efficient servicing of requests, this requirement will prevent unnecessary access to third-party information and data. This approach also ensures that requests are technically feasible, more efficient and result in quicker servicing of law enforcement requests, and result in a less disruptive framework.

An embedded principle of proximity also engenders a clear line of contestability, should an entity believe it has received a warrant in error. AWS takes our responsibility to protect and secure our customers' information seriously, and where we need to act to protect customers, we do. We have repeatedly challenged government demands for customer information that we believed were overbroad. It is also our view that, unless exceptional circumstances apply, it is appropriate for our customers to be notified of the request. We believe these are essential elements to a transparent and accountable framework, addressed in more depth later in our submission.

2. Clear and Feasible

What information should be accessed?

The question of what information and data should be accessible to law enforcement and intelligence agencies is arguably the most consequential item in the Discussion Paper. AWS recognises that addressing these fundamental definitions and core concepts is necessary for the development of a framework that can readily adapt to technological change. In principle, these revised definitions and concepts should provide clarity for agencies, entities and society on the precise nature of information available under warrant and the circumstances in which it must be provided. The technical feasibility of a request should also form a strong part of the warrant decision making and include a balanced assessment of its reasonableness and proportionality.

Addressing this issue with any level of sufficiency will demand in-depth consultations between the Department, industry, academia, and civil society. We offer the following observations and suggestions as a precursor to a more detailed consultation process:

'Communication' or 'content': It is appropriate that the definition of a communication in this context be revised and clarified to reflect the evolution of technology since Australia's electronic surveillance laws were established in the late 1970s. Indeed, the question of the definition of 'communication' was posed to government by the PJCIS in its review of the mandatory data retention scheme.

It is reasonable for the definition of 'communication' or 'content' to continue to mean an exchange of information between one or more intended recipients. Per our earlier point on non-content sensitivity, we also propose that the volumes and breadth of non-content data may reach a level of sensitivity to deserve the same protections as content once aggregated.

Non-content data: Per the above, we believe it is appropriate for non-content data to mean the inverse of content – data that has *not* been input by a user for the consumption of an intended recipient. This can mean, for example, machine-to-machine communications, metadata (that is, data about the communication), locational data, or online activity (such as web browsing history).

Electronic objects: In addition to the above, a third category created for 'electronic objects' will provide clarity to the warrants process. For AWS, an object refers to a file and any metadata that describes that file; similar in scope, in essence, to a 'stored' communication, but recognising that not all objects are intended to be communicated. These objects should be considered separate to a communication (unless, of course, the object has been attached as part of a communication), but no less sensitive and with the same expectations for privacy and security as a communication and requiring an equally high threshold for warranted collection. The creation of this category will allow for the creation of something akin to an electronic search warrant, with requisite requirements for specificity, just as these warrants would exist in the physical world.

How should information be accessed?
As addressed in the Discussion Paper, the current framework is fragmented and complex, and imposes a significant regulated burden on impacted entities. Addressing the suggestions in the preceding sections of our submission will go a long way to alleviating these burdens by creating clarity for impacted entities and ensuring requests are technically feasible. To further embed these principles the following should also be considered:

Centralised authority and processes: In addition to consistent, proportionate thresholds for warrants and data requests, it is essential that a centralised statutory authority be established to oversee and administer the warrants process. Creating a 'single door' for these requests will ensure consistency for impacted entities, create a level of specialised knowledge within a clearly designated statutory authority for administering requests with appropriate consideration given to technical feasibility, and will have the overall result of strengthened oversight.

Prohibitions on systemic weaknesses or vulnerabilities: As AWS articulated in our submissions relating to the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*, the execution of warrants 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.

Conflicts of law: Government surveillance powers should not require companies to do an act or thing, or omit to do an act or thing, that would breach a foreign law, or cause another person to breach a foreign law. It would be appropriate to either make clear that any such requirement would be unreasonable and provide a defence for any company or individual who refuses to do the act or make the omission. This is important for employees of technology providers subject to laws of foreign countries.

3. Transparent and Accountable

Trust in the security of information is fundamental to business innovation and economic growth, and is crucial in a digital economy. AWS customers trust us to handle their data securely, and we are committed to maintaining that trust. Likewise, trust is fundamental for the maintenance of legitimacy in any democratic system and public institution, but particularly in the use of surveillance powers. Maintaining and building that trust should be a foremost consideration of these reforms.

As stated by Director-General for Security, Mike Burgess, in his 2022 annual threat assessment, transparency is a precursor for trust. It is also a precursor for the accountable use of intrusive powers, ensured through the presence of strong, independent, expert oversight.

In his *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, the Independent National Security Legislation Monitor, James Renwick CSC SC, made recommendations for the creation of an Investigatory Powers Commissioner. AWS wholeheartedly supports these recommendations. We believe it is essential that there is a dedicated, independent statutory authority with the focus and necessary technical expertise to oversee Australia's electronic surveillance framework as it continues to grapple with the challenges posed by technological change. In addition to providing oversight on the proper functioning and use of a new surveillance framework, this body should also provide for contestability of the warrants process – particularly on the question of technical feasibility.

AWS looks forward to working with the Department in a trusted and collaborative manner to modernise Australia's electronic surveillance framework.

Best regards,

Roger Somerville (somroger@amazon.com)
Head of Public Policy, Australia and New Zealand
Amazon Web Services.