7 November 2022

Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600
Legcon.sen@aph.gov.au

Re: Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022

Amazon Web Services (**AWS**) is pleased to provide comments to the Senate Legal and Constitutional Affairs Committee (**Committee**) on the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* (**Bill**). We continue to support the Australian Government's objective of creating a stronger, modernized and flexible privacy framework, suited to the needs of an increasingly digitized world. AWS is proud to play our part in building the technology infrastructure and services, to help Australian businesses and governments innovate, and deliver greater productivity, greater resilience and better services for their customers and citizens.

AWS is the world's most comprehensive and broadly adopted cloud platform. AWS launched in Australia in 2011 and opened its Sydney Region in 2012. In the past decade, Amazon including AWS has invested AUD $8 billion in local infrastructure and jobs across Australia. Our investment includes a workforce of more than 5,000, including 1,000 employees joining in the past year. These roles include high value AWS jobs such as machine learning scientists, sales and solutions architects, and data centre operators. In late 2020, we announced a second Australia AWS Region in Melbourne, which will offer our Australian customers a second onshore option when choosing where their data and workloads are hosted.

As we noted in our submission to the Attorney-General's *Privacy Act Discussion Paper* last year, major privacy reforms have been enacted internationally since the previous reforms to the Privacy Act 1998 (**the Act**), including the European Union's General Data Protection Regulation and the Californian Privacy Rights Act. Australia has the opportunity to learn from the development and implementation of these regimes to create a framework that raises the bar for privacy on a global scale.

We support the creation of comprehensive privacy laws that protect individuals' personal information, whilst balancing an organisation's legitimate need to process that information. We also recognize that an important objective of privacy laws is to encourage better internal data governance and improve information security hygiene-practices in organisations.

Security is our top priority. AWS is highly sensitive to the security needs of our customers in every location in which we operate. We know how important it is to Australian customers to mitigate security risks in data centre supply chains, and we understand that agencies need to identify and source technology from providers they trust. AWS has attained international security accreditations that are important to our customers. Like many multinational entities, AWS has deep experience in implementing and complying with international privacy regimes. We know our customers care deeply about privacy and data security, and so we support the highest privacy standards and compliance certifications to satisfy the requirements of our customers around the world. We are certified as a Strategic Hosting Provider in the Australian Government's Hosting Certification Framework. As of H1 2022, 132 AWS Cloud services available in the AWS Sydney Region have been assessed by the Information Security Registered Assessors Program (IRAP)

for operating workloads at the PROTECTED level, the highest Australian Government data classification attainable for public cloud services.

We would like to make some recommendations, based on our discussions and experience with governments globally, particularly where it relates to implementing and applying security and privacy frameworks and guidelines.

Key Recommendations:

1/ The Bill should allow for its penalties to be proportionate to the harm caused, and for mitigating or aggravating factors to be considered.

The Bill substantially increases the maximum penalty under section 13G of the Privacy Act for "serious or repeated interferences" with privacy to an amount not exceeding the greater of $50 million; three times the value of the benefit obtained; or, if the court cannot determine the value of the benefit, 30% of the offending entity's adjusted turnover in the relevant period. The Explanatory Memorandum states that this increase will signal Australia's "expectations that businesses undertake robust privacy and security practices".

While AWS agrees that penalties must be adequate to protect Australians' personal information and promote effective deterrence, civil penalties frameworks should not impose undue hardship on an otherwise responsible entity that already undertakes robust privacy and security practices. Entities should have the opportunity to demonstrate that they have taken appropriate security and organisational measures to protect personal information if an interference occurs, and these factors should be taken into consideration. If the Commissioner applies to the Federal Court or Federal Circuit Court for a penalty order in contravention of section 13G, the Bill should ensure due consideration is given to any aggravating or mitigating factors. Mitigating factors could include (a) how actively and promptly the entity has tried to resolve the matter with the individual(s); (b) whether the entity took reasonable steps to prevent or reduce the harm caused by the interference have been taken; and (c) whether the entity has provided the affected individual(s) with remedies. Aggravating factors could include (a) where the entity knew or should have reasonably known of the risk of the interference but continued with its operations without taking measures to minimize the risk or remedy the interference; or (b) if the entity is in the business of handling sensitive information (e.g. health data), but failed to put in place safeguards that were adequate or proportional to the harm that might be caused to the individual(s), should that information be disclosed.

Penalties under section 13G should also be proportionate to the harm caused to individuals by an interference with privacy. Per the Explanatory Memorandum, penalties should be a reasonable and proportionate response to the "behaviours the penalties are intended to deter and penalize". As such, due consideration should be given by the Court to an entities' existing privacy and security practices not only to assess whether appropriate security and organizational measures were in place, but also to what degree their actions caused harm to individuals. Otherwise, the penalties may not proportionately reflect the true extent of the harm caused to any individuals in the event of a privacy interference and, consequently, may not effectively address the behaviours of entities that they are intended to deter.

2/ The Bill must ensure that appropriate safeguards and scope be applied to proposed enhancements for the Commissioner to obtain and share information.

Section 33 of the Bill proposes to enhance the Commissioner's ability to obtain information relating to actual or suspected eligible data breaches of the Privacy Act, to share that information with other "receiving bodies", and to then publicly disclose "certain information" if deemed in the public interest. While we noted in our previous submission to the Attorney-General's *Privacy Act Discussion Paper* that we believe strengthening existing regulatory and enforcement mechanisms is fundamental for improving accountability and clarity under the Act – it is our view that the proposed enhancements to Section 33 do not put in place an appropriate and proportionate scope for obtaining and sharing information. This will have significant implications for privacy of individuals, and is also inconsistent with the broader legal tradition for well-scoped information sharing provisions in Australian legislation. We provide more details on our concerns and propose recommendations for your consideration:

A. *Section 33A is overly broad, lacks details around appropriate safeguards, creates significant risks for both the privacy of individuals as well as companies facing investigations, and is inconsistent with other Australian legislation.*

Under proposed section 33A, the Commissioner is empowered to share information or documents with a "receiving body" (specifically, an enforcement body, alternative complaint body, and a State or Territory authority or foreign authority with privacy functions) for the purpose of either entity or body exercising its power or performing its functions or duties. We are concerned that these powers are overly broad, not subject to appropriate safeguards, and may cause significant privacy concerns for both organisations and the wider Australian community.

We appreciate that the Commissioner is already empowered to share information with certain Australian authorities, but these are a narrow set of bodies and information that may only be shared for limited purposes such as the Consumer Data Right or a breach of the My Health Records Act. If section 33A is to remain in the Bill, we recommend that (1) the bodies to whom the Commissioner may disclose information be significantly narrowed to only Australian State or Territory authorities that have functions to protect the privacy of individuals; and (2) the purposes for which the information can be shared be narrowed to only purposes relating to the privacy of individuals. Disclosure of any information by the Commissioner to the receiving body should also not only be in the public interest, but there should be a proportionate and necessary justification for sharing the information between bodies, rather than the receiving body approaching the organisation directly to request the information under their own powers.

The effect of the powers under section 33A is such that an organisation could share information regarding an eligible data breach with the Commissioner, who may then share that information (including the personal information of Australians) with any "receiving body" for any purpose of the receiving body – including to pursue investigations or matters that are not related to the data breach in question. This could all occur without the consent or knowledge of the organisation, or any affected individuals.

It is also concerning that any of this information, especially personal information, may be given to a foreign authority without the consent or knowledge of the organisation or affected individuals. Beyond the Commissioner's satisfaction that "satisfactory arrangements" are in place to protect the information, there is no basis to ensure that the foreign authority has sufficient privacy and security frameworks in place to ensure that information – which may be highly sensitive – is adequately protected. In addition, as a jurisdictional matter, a foreign authority would not be directly subject to the restriction in subsection (5) of section 33A, and it could use the information for any purpose whatsoever.

Although the Explanatory Memorandum notes that the Commissioner's ability to share information is subject to certain safeguards, these safeguards also lack clarity and are overly broad. For example, the receiving body's requirement to use "the information only for the purposes for which it was shared" does not impose any limits on what those purposes might be. In particular, the purpose might be entirely unrelated to privacy or data protection. This provides little comfort or certainty that the information shared with the Commissioner will be used solely for an eligible data breach investigation, and may cause organisations to be reluctant to share information with the Commissioner, which is contrary to the goals of this section. At a minimum, the current drafting of section 33A will incentivize organisations to apply the narrowest possible approach to sharing information with the Commissioner.

B. *Section 33B should define the specific kinds of information that may be collected and disclosed by the Commissioner.*

Additionally, the proposed reforms under section 33B, which empower the Commissioner to disclose in the public interest "certain information" (including personal information) acquired in the course of their functions or duties, may have harmful and unintended consequences. While we note that the intention behind these provisions is "to ensure Australians are informed about privacy issues and to reassure the community that the OAIC is discharging its duties", allowing the Commissioner to disclose or otherwise publish personal information and extensive privacy-related information may actually be harmful to the individuals the Commissioner seeks to protect, and could also result in confidential or commercially sensitive information being published, such as customer lists, or details of an organisation's security posture.

We note that there is no definition of "certain information", beyond the broad interests the Commissioner must consider before disclosure in the public interest, as outlined in paragraph 33B(2). This in practice means organisations may have to share any information requested by the Commissioner, including but not limited to personal information, commercially sensitive information or otherwise protected information, and be prepared that such information may be made public even if no actual privacy interference has occurred. Without clear safeguards, and with such a broad and ill-defined scope, there is substantial risk that information provided by organisations to the Commissioner could create security and privacy risks, increase the cost of security for regulated organisations, and become ineffective, inefficient and even counterproductive to security outcomes.

We therefore recommend that the Commissioner specifies the types of information that can be collected by the Commissioner, and that may be disclosed in the public interest, safeguards and process should that information be published, and also provide clearer guidelines for when the information could be requested under section 26WU. It is important that such specificity and clarity be included in this legislation rather than subsidiary legislation, and be subject to public consultation, given the proportional risks to the privacy of individuals and the commercial confidentiality of organisations this poses. This is to avoid uncertainty in implementation and disproportionately increased compliance costs, and also so that the Commissioner only publicly discloses appropriate information suitable for the eyes of the wider Australian community.

Relatedly, under proposed section 26WU, the Commissioner is empowered to require an organisation to give information or produce a document relevant to the assessment of an eligible data breach. The list of "relevant matters" that these documents or information may relate to are overly broad and non-exhaustive. We appreciate that the Commissioner requires thorough and comprehensive knowledge of information compromised in an eligible data breach, in order to assess the risk of any harm to individuals,

and that this information may not otherwise be publicly available. However, we note that increased information-sharing powers may not, in practice, achieve the goal of bettering internal data governance and improving information security hygiene practices in organisations. An organisation retaining disproportionate amounts of information, on the chance they may have to disclose it to the Commissioner in the future, creates its own privacy and security risks that, again, may be counterproductive to the wider privacy and security outcomes that this Bill seeks to create.

Thank you for the opportunity to provide our comments. We look forward to continuing to engage with the Attorney-General's Department on this important issue.

Best regards,

Roger Somerville
Head of Public Policy, Australia and New Zealand Amazon Web Services.