Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600
Via email: legcon.sen@aph.gov.au

7 November 2022

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

Dear Secretary

On behalf of the Australian Information Industry Association (**AIIA**), I am writing in relation to the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* ('**the Bill'**) on which the Legal and Constitutional Affairs Committee is reporting to government. The AIIA is pleased that parliamentary processes are applying to the Bill and subject to review by appropriate committee processes with the opportunity for consultation with stakeholders, notwithstanding the tight timeframes provided for industry input.

The AIIA notes that the government has introduced the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 which will seek bipartisan support to increase penalties for data breaches to the greater of $50 million, 30% of turnover or three times the value of any benefit obtained through the misuse of information.

In respect of recent high-profile data breaches, the AIIA has called on the Albanese Government to release its Final Report from the *Privacy Act Review* before the end of the year. The AIIA in its response to the Privacy Act review discussion paper in December 2021 also called on government to introduce the controller-processor distinction into the Australian privacy landscape. The AIIA appreciates the Government's commitment to seeing the *Privacy Act* review through to its completion, as the appropriate legislative vehicle to deal with current data and privacy concerns, and understands the deep level of community concern about data security, especially when it comes to sensitive personal information.

The AIIA has concerns about the quantum of the proposed increases in penalties and the disincentives to good corporate behaviour and transparency around data breaches that this may lead to, including cooperation with governments.

The AIIA has been supportive of the ambition of government to update cyber security policies and its members have been heavily engaged with co-design processes pertaining to the Critical Infrastructure Systems of National Significance reforms. In line with the calls of the then-Opposition, in recent years the AIIA has called on government to avoid unnecessary haste in moving legislation through the parliament and short consultation timeframes, especially where legislation is not referred for committee review. The AIIA notes that meaningful consultation with industry and parliamentary committees leads to the development of better policy and regulation.

In principle the AIIA supports the Government's aim, in the Bill, to strengthen the powers of the Australian Information Commissioner, reinforce the Notifiable Data Breaches scheme, and equip the Australian Information Commissioner and Australian Communications and Media Authority with greater information-sharing powers. However, allowing genuine consideration of the Bill, especially when it comes to timely data breach reporting and mechanisms for compliance, is important, and the tight reporting timeframes will make this challenging.

The Bill as introduced exceeds that of the strictest regimes found on the global stage, with the maximum penalties being increased by a factor of more than twenty. We note that under draft legislation *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* ('the Online Privacy Bill'), section 13G (2), penalties were to be increased to $10m, three times the value of the benefit obtained, or 10% of the relevant turnover.[1]

In respect of the rationalisation that has been provided for the quantum increase of damages, the AIIA notes the below from the Explanatory Memorandum:

> *10. These changes are consistent with the proposed maximum penalties under the Australian Consumer Law (ACL) in the Treasury Laws Amendment (More Competition, Better Prices) Bill 2022. The Australian Competition and Consumer Commission's Digital Platforms Inquiry July 2019 report recommended that the maximum penalties of the Privacy Act should be increased* ***to mirror the penalties for breaches of the ACL as the lack of effective deterrence has enabled problematic data practices.*** [emphasis added][2]

The relevant 2019 ACCC report at recommendation 16(f) recommended the following:

> *16(f) Higher penalties for breach of the Privacy Act:*
>
> *Increase the penalties for an interference with privacy under the Privacy Act* ***to mirror the increased penalties*** *for breaches of the Australian Consumer Law.*[3] [emphasis added]

However, the AIIA further notes that the *Treasury Laws Amendment (More Competition, Better Prices) Bill 2022* was only introduced in recent weeks. The effect of this is that when the ACCC report made the recommendation to mirror the ACL penalties, those penalties were the greater of $10m, three times the value of the benefit derived, or 10% of turnover.[4] Therefore, the rationale that tethering to the 2022 quantum of maximum penalties under the ACL was a recommendation of the ACCC three years ago in 2019 is questionable. The AIIA also makes the point that anti-competitive conduct and being the subject of a data breach are quite different behaviours.

The AIIA joins with other associations in calling for a safe harbour mechanism to be embedded in the legislation.

Help-seeking and reporting behaviours by entities acting in good faith must not be disincentivised by a blunt instrument approach with disproportionately severe penalties, which could be a perverse and unintended outcome of the proposed approach.

If businesses engage in timely reporting and act in good faith in implementing data and cyber security frameworks with due diligence, there should be a legislative mechanism to quarantine such organisations from these penalties. Safe harbour would provide certainty for businesses and is particularly important given the need for clearer security requirements as identified in the *Privacy Act Review* Discussion Paper, with several submitters noting that under the current law entities 'can find it difficult to determine what security controls are reasonable in their circumstances, or what security

---

[1] https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-exposure-draft.pdf

[2] https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6940_ems_715c9651-94ce-4b91-9912-a4023d8c7f61/upload_pdf/22113%20EM.pdf;fileType=application%2Fpdf

[3] https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report

[4] https://jws.com.au/en/insights/articles/2022-articles/esg-and-consumer-law

measures are expected of them'.[5] Safe harbour provisions that have been applied in the US States of Ohio, Utah and Connecticut could form a useful model for the government.[6] In those States, legislation was passed to stipulate that a safe harbour mechanism would be enlivened if the organisation subject to a data breach could demonstrate that their data security policies followed one of several possible cyber security frameworks. The concepts of due diligence and good faith are essential; government must ensure that privacy penalties and legislation are sensitive, not blunt, to these factors, especially where actors are sophisticated and circumstances are out of all reasonable control of the subjects of breaches. These good faith and industry government cooperation are the basis of the Critical Infrastructure and Systems of National Significance (**SoNS**) legislation.

Given the penalties the Government is proposing are three to five times higher than the previously-drafted maximum, the AIIA believes there should also be appropriate justification for such a high penalty by global standards and sufficient clarity in the law as to the steps entities must take to avoid triggering the penalty.

The AIIA supports the comments by Telstra Chair in the media on 25 October 2022 that the relationship between government and business ought to remain constructive and characterised by goodwill in the context of data breaches, and reaffirms the intent of the technology industry to build a genuine cybersecurity culture at every level, mindful of the serious responsibilities data stewardship impose on business. It should be noted that increasing penalties, while appropriate, is a necessary but not sufficient step for government to take and must be accompanied by meaningful cooperation towards a common goal on part of government and business. Our sector understands the critical importance of data security and wishes to work with government to this end. Defaulting to an overly punitive approach will not serve constructive purposes in addressing an already complex problem.

The AIIA would welcome the opportunity to engage with the Committee on these matters further.

Yours sincerely

Simon Bush
CEO
AIIA

[5] *Privacy Act Review* Discussion Paper, p144.
[6] https://www.cshub.com/security-strategy/articles/three-us-state-laws-are-providing-safe-harbor-against-breaches